DCAF Geneva Centre for Security Sector Governance

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

DCSD
PARTENAIRE POUR UNE SÉCURITÉ DURABLE

Guide to Good Governance in Cybersecurity

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of people and the states they live in within a framework of democratic governance, the rule of law, and respect for human rights. DCAF contributes to making peace and development more sustainable by assisting partner states, and international actors supporting them, 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. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality.

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

DCAF Geneva
P.O. Box 1360
CH-1211 Geneva 1
Switzerland

Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva

Cite as: DCAF, Guide to Good Governance in Cybersecurity (Geneva: DCAF, 2021).

Copy-editor: Alessandra Allen

Design & layout: DTP studio

Contents

Introduction

The increasing access of people to cyberspace and its resources affects our daily lives and has a considerable impact on our societies. It has already profoundly transformed how we live, work, and interact. Cyberspace offers countless opportunities for economic development, social interaction, and political exchanges. On the flip side, it has provided tools to conduct illegal surveillance, collect personal data, influence democratic processes, commit crimes, and change the means and methods of warfare.

These challenges require multiple responses, and governments, the private sector, and civil society must come together to address the challenges of cybersecurity governance. Legal and policy frameworks will also have to adapt to respect better and implement international human rights norms, while effectively combating cybercrime, malicious cyber activities, and cyber-attacks, as well as the use of the internet for terrorist purposes and the promotion of violent extremism. Only vigorous action to address these issues will promote a secure, stable, and open cyberspace.

It is in this context that, in 2018, the Directorate of Cooperation of Security and Defence (DCSD) of the French Ministry for Europe and Foreign Affairs and the DCAF - Geneva Centre for Security Sector Governance launched the drafting of this guide to good practices for the promotion of good governance in cyberspace. In 2020, the guide was translated into Albanian, English, Macedonian, and Serbian as part of DCAF's project 'Enhancing Cybersecurity Governance in the Western Balkans', with the support of the United Kingdom's Foreign, Commonwealth and Development Office (FCDO).

This guide was written for policy makers, technical experts, civil society, and all those interested in best practices for cybersecurity governance. It draws on DCAF's experience in promoting good governance in the security sector.

This book comprises six chapters that explain how to apply the principles of good governance to cybersecurity. The chapters focus on:

- applying the principles of good security sector governance to cyberspace;
- the link between cyberspace, cybersecurity, and security sector governance;
- international and regional legal frameworks applicable to cyberspace;
- applying international and regional standards;
- national cybersecurity strategies; and
- promoting effective cooperation between the public and private sectors in cyberspace.

CHAPTER 1
INTRODUCING GOOD SECURITY SECTOR GOVERNANCE

OBJECTIVES

This chapter aims to increase readers' knowledge and understanding of key terms related to good security sector governance, and how to apply them in the context of cyberspace. To this end, the chapter focuses on three essential components of good security sector governance in cyberspace:

- accountability;
- transparency; and
- the rule of law.

The chapter begins by introducing these concepts, and it goes on to highlight the challenges of promoting the principles of good governance in cyberspace, as well as identify recognized good practices.

THIS CHAPTER AIMS TO:

- increase awareness of the key terms and definitions that explain the differences between governance, security sector governance, and good security sector governance;
- increase understanding of the underlying principles of good governance, such as accountability, transparency, and the rule of law;
- increase knowledge of the underlying principles of good security sector governance; and
- increase understanding of the importance of promoting the principles of good governance in cyberspace.

1. Introduction

Governance, security sector governance, and good security sector governance

Governance is defined as the 'exercise of power and authority'. As a general concept, the term governance can be used to describe the set of rules by which an organization is run, including private, commercial, and non-profit entities. Within the security sector, the term 'governance' is used to describe all formal and informal decisions, processes, and actors that may influence the provision of public services, such as health, education, or security.

Security sector governance (SSG) is defined as the 'exercise of power and authority in the context of one particular national security sector'.[1] It is an analytical concept that is not based on a commitment to any specific norm or value.

> Good security sector governance focuses on applying the principles of good governance to security provision, management, and oversight in the national context.

Good SSG aims to make a state's security sector more effective and accountable within a framework of democratic civilian control, respect for human rights, and the rule of law.[2]

Moreover, good SSG is based on the idea that the security sector should be held to the same high standards of public service delivery as any other public sector service provider. Therefore, a security sector that fails to comply with these standards may challenge political, economic, and social stability in a national context (also referred to as 'poor SSG').

What is the security sector?

In general, a security sector includes all structures, institutions, and personnel responsible for security provision, management, and oversight at the national and local level.[3]

The state is therefore not the only provider of security and justice; individuals also provide security and justice in their homes and communities, regardless of whether the state takes steps to meet their security needs. Some communities organize themselves to ensure security through measures such as neighbourhood watches, women's groups, or commercial security provision.

Furthermore, the customary roles of important community figures in security and

1 DCAF, Security Sector Reform: Applying the Principles of Good Governance to the Security Sector, DCAF SSR Backgrounder series (Geneva: DCAF, 2015).

2 Ibid.

3 Ibid.

justice decision-making and alternative dispute-resolution mechanisms, as well as traditions and informal rules, can shape security and justice provision within a community. As a result, such community groups also constitute part of the security and justice sector in a wider sense.

Non-state security and justice providers form part of a broader definition of the security sector owing to their direct impact on SSG. In the last two decades, private security providers have been increasingly deployed to provide security and services protecting people and their property. Private military and security companies operating on a commercial basis have therefore become a major security actor.

The security sector is composed of all structures, institutions, and personnel responsible for security provision, management, and oversight at the national and local level, including both:

- security providers, such as armed forces, the police, border guards, intelligence services, penal and corrections institutions, and commercial and non-state security actors; and
- security management and oversight bodies, such as government ministries, parliaments, special statutory oversight institutions, parts of the justice sector, and civil society actors, who not only play an important role in ensuring that public security provision adheres to high standards, but who are also the ultimate beneficiaries, including women's organizations and the media.

Security sector reform (SSR) is based on a broader understanding of the security sector. The ultimate aim of SSR is to promote good governance in the security sector in order to improve human and state security.

Source: DCAF, Security Sector Reform: Applying the Principles of Good Governance to the Security Sector, DCAF SSR Backgrounder series (Geneva: DCAF 2015).

What is security sector reform?

A security sector that is neither effective nor accountable fails to deliver security for all. It is unable to fulfil its tasks in a credible manner, in areas such as national defence, law enforcement, or public assistance. An inefficient security sector is likely to waste public resources, diverting funding from other essential public services.[4]

SSR is a political and technical process that aims to improve human and state security by making security provision, management, and oversight more effective and accountable within a framework of democratic civilian control, the rule of law, and respect for human rights.[5]

4 Ibid.

5 DCAF, Security Sector Reform: Applying the Principles of Good Governance to the Security Sector, DCAF SSR Backgrounder series (Geneva: DCAF, 2015), p. 2.

Good practice: It is important to recognize that individuals and communities have different security needs, including actors in cyberspace.

In cyberspace, every individual has specific security needs; women and girls are disproportionately affected by bigotry, hate, and misogynist speech. Acknowledging this reality and providing effective mechanisms for reporting incidents and initiating criminal investigations can help to improve the security of affected vulnerable groups.

EXAMPLES OF GOOD PRACTICE

Benin has launched an annual cybersecurity campaign as part of efforts to raise awareness of the issue. The campaign targets the country's youth and is to be codified in the national cybersecurity strategy document.

As part of the No Hate Speech Movement, Council of Europe member states have launched national campaigns and established national reporting bodies to adopt national reporting procedures and mechanisms for hate speech, hate crime, and cyberbullying.

In Austria, the Ministry of Interior is piloting a reporting mechanism for violent extremist and radical videos in order to remove hate speech from social media platforms.

(Source: Federal Ministry for Interior of Austria, http://bvt.bmi.gv.at/601/)

The Ukrainian police established a point of contact for reporting cases of cyberbullying and hate speech, in order to allow victims to file complaints

(Source: Council of Europe, https://www.coe.int/en/web/no-hate-campaign/reporting-to-national-bodies#{%2237117314%22:[8]})

In Senegal, the National Cybersecurity School (École Nationale de Cybersécurité à Vocation Régionale – ENVR) was established, with French support, in November 2018 to strengthen West Africa's defences against cyber-attacks and the use of the internet for terrorism financing and propaganda. The school will provide training to security service providers, members of the judiciary, and private enterprises on combating cybercrime, and will have a 'regional vocational role' in helping other countries in West Africa.

(Source: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/le-cadre-institutionnel-de-l-action-de-la-france/la-cooperation-de-securite-et-de-defense/les-ecoles-nationales-a-vocation-regionale/article/senegal-inauguration-de-l-ecole-nationale-de-cybersecurite-a-vocation-regionale)

2. Good security sector governance in cyberspace

What is good security sector governance?

Good SSG is all about applying the principles of good governance to security provision, management, and oversight in a national setting. Good governance is based on seven main principles:

- **Accountability:** There are clear expectations from security providers, and independent authorities oversee whether these expectations are met and impose sanctions if not.
- **Transparency:** Information is freely available and accessible to those affected by decisions and their implementation.
- **Rule of law:** All persons and institutions, including the state, are subject to laws that are publicly known, enforced impartially, and consistent with international and national human rights norms and standards.
- **Participation:** Women and men of all backgrounds have the opportunity to participate in decision-making processes and service provision in a free, equal, and inclusive manner, either directly or through legitimate representative institutions.
- **Responsiveness:** Institutions are aware of the different security needs of all parts of the population and fulfil their mandates in the spirit of a service-oriented culture.
- **Effectiveness:** Institutions must fulfil their respective roles, responsibilities, and missions with the utmost professionalism.
- **Efficiency:** Institutions make the best possible use of public resources to fulfil their respective roles, responsibilities, and missions.

Applying good governance principles in cyberspace

If cyberspace were a country, it would be the biggest and most populous in the world. It would not, however, have a legislative or other representative decision-making body, nor would it have a designated law enforcement mechanism, or a mechanism to protect citizens' human rights – because no single entity exercises exclusive authority and control over the entire digital space.[6]

6 Anja Mihr 'Good Cyber Governance: The Human Rights and Multi-stakeholder Approach', Georgetown Journal of International Affairs (2014), https://www.jstor.org/stable/43773646.

Cyberspace governance is instead characterized by a multitude of diverse actors with different roles and responsibilities influencing policy decisions and regulatory processes.

Non-state actors in cyberspace include civil society, such as non-governmental organizations, academic research groups, the media, and the private sector, particularly private companies and industrial bodies, as well as international and regional organizations.

Owing to the vast number of actors involved in developing and implementing policies and regulatory frameworks in cyberspace, these processes are often burdensome, complex, and/or ineffective.

This, combined with a lack of knowledge on how to apply effectively the principles of good governance to cyberspace, can lead to poor governance and affect the security sector's ability to provide effective human and state security. The following sections take a closer look at three key principles of good SSG: accountability, transparency, and the rule of law.

CASE STUDY: THE UNITED STATES NATIONAL SECURITY AGENCY'S SURVEILLANCE PROGRAMME

In 2013, CIA employee Edward Snowden leaked top-secret documents revealing that US and UK intelligence agencies had been operating mass surveillance programmes around the world, including intercepting internet and telephone conversations transmitted via undersea fibre optic cables, collecting data from Google and Yahoo user accounts and mobile phone records, spying on foreign governments, and hacking and infecting computers with malware.

Notably, the US Foreign Intelligence Surveillance Court (FISA) ordered companies to hand over their customers' data. Vast intelligence-sharing practices between members of the 'Five-Eyes Alliance' and other countries were also uncovered. Although then President Obama responded by reforming the National Security Agency's surveillance programmes and the FISA Court to increase transparency, the US Congress has still not been able to agree on a system to ensure effective privacy protection, while preserving investigative capabilities.

(Source: American Civil Liberties Union (ACLU). Available at https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=nsa-surveillance and https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began?redirect=NSAreform)

2.1 Developing norms and institutions to apply the principle of security sector accountability to cyberspace

Effective accountability depends on democratic and civilian control. This can be exercised by national parliaments and, more broadly, by civil society. Such oversight is essential towards ensuring the accountability of the security sector. In cyberspace, however, democratic and civilian control of the security sector is often undermined for a number of reasons.

Democratic oversight frequently faces the following obstacles:[7]

- **The complexity of online networks**

The complexity of online networks is a significant challenge for democratic oversight. A large and diverse number of states, private international actors, and other non-state actors take part in cybersecurity provision. Similarly, a diverse group of actors participate in operations that are broadly defined as 'cyber-attacks'. Owing to the technical complexity of online networks, however, it is difficult for oversight bodies – such as parliamentary committees with often limited capacity – to identify the relevant actors, gain knowledge of their existence and activities, or even acquire the legal mandate to do so.

- **The technical knowledge required to develop and implement effective regulation**

The highly technical nature of cyberspace exacerbates oversight challenges. Oversight bodies, such as parliaments, often lack the expertise required to understand the technical aspects involved and, as a result, may find it difficult to draft legislation that can effectively regulate activities in cyberspace. Cooperation between public and private bodies is further complicated by the division between the highly paid and sophisticated technical experts involved in developing and implementing effective regulation and the often poorly paid and less well-informed government actors responsible for oversight.

- **Legal complexities of cyberspace, such as jurisdiction and attribution**

Oversight challenges are also compounded by legal complexities. The interconnected, 'borderless' nature of cyberspace poses significant challenges to traditional territorially bound legal frameworks. Data and cyber activities can shift from servers located in one jurisdiction to another at the speed of light. Furthermore, while it is often said that the same laws should apply for both offline and online activities, it is frequently unclear what this entails in practice. Cybersecurity poses complex legal questions related to, among other things, the right to privacy and freedom of expression. This complexity is further magnified by public-private cooperation in cyberspace, which in turn creates legal issues regarding the division of accountability and oversight.

7 See Buckland, B., F. Schreier, and Th. H. Winkler, op. cit., pp. 18-19, https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.

- **The diverse nature of actors involved, blurring the traditional boundaries between accountability and oversight**

Oversight challenges are exacerbated by the diverse nature of actors involved. In most instances, national oversight institutions are organized by agency or according to their function. For example, a parliamentary committee may oversee intelligence services, the armed forces, or justice institutions. Cooperation between public and private actors involved in cybersecurity, however, cuts across the boundaries of various agencies, areas of expertise, and oversight mandates. As a result, a large number of areas are left with inadequate or no oversight.

Cyberspace also results in a blurring of lines of responsibility and accountability. The actions of every government agency are intertwined in a chain of responsibility. For example, a Paris police officer is linked through his superiors to the police prefect (politically appointed head of the force) and, ultimately, to the Ministry of the Interior and the executive. The responsibilities and oversight functions of democratic governance institutions, such as the parliament, are therefore linked to individuals or agencies carrying out government directives. These ties can be severed by the involvement of private actors and the creation of public-private cooperation mechanisms. While an IT firm contracted by a public agency may seem to act as a simple agent of the state, the relationship is generally much more complex and clouded by numerous discrepancies, reducing transparency and preventing oversight mechanisms from operating effectively.

- **Understanding the oversight body's mandate**

In general, government oversight bodies are mandated to oversee the government agencies for which they are directly responsible. Private partners of these agencies may therefore evade their oversight, even in cases where they are directly funded by, or work in close collaboration with, those agencies.

CASE STUDY: AN ENQUIRY BY THE GERMAN BUNDESTAG INTO THE SALE OF SURVEILLANCE TECHNOLOGIES TO FOREIGN GOVERNMENTS

In 2014, members of the German parliament conducted an inquiry into the sale of surveillance technologies to foreign governments. In response, the German government stated that, over the past decade, it has provided German companies with licenses to export surveillance technologies to at least 25 countries, many of which have long histories of human rights abuses.

As a consequence of this inquiry, the German government stated that it will further pursue the regulation of surveillance technologies that encroach upon human rights.

(Source: European Digital Rights (EDRi) Protecting Digital Freedom. Available at: hhttps://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

The technical complexity of cyberspace further compounds the difficulties traditionally faced by parliamentarians in overseeing the security sector, which may undermine effective accountability. This factor, coupled with the difficulty of reliably identifying specific actors responsible for violations of law in cyberspace, can make it difficult, if not impossible, for civilian authorities to hold the security sector accountable, thereby contributing to a culture of impunity.

CASE STUDY: PARLIAMENTARY OVERSIGHT OF CYBERSECURITY IN SWEDEN: MAIN CHALLENGES AND GOOD PRACTICES

The Swedish parliament has 15 parliamentary committees, with varying roles and responsibilities. These committees can, for example, conduct public hearings to gain a better understanding of specific issues on which parliament needs to pass legislation. While it is unclear which parliamentary committee is tasked solely with overseeing cybersecurity governance, it is likely that various committees play an oversight role, depending on the thematic context. For instance, the Committee on Defence may be tasked with issues related to cybersecurity.

Sweden's national cybersecurity strategy, adopted in 2016, addresses a wide range of subjects, including the regulation of information and communication technology (ICT) providers and critical infrastructure protection. However, there does not appear to be a committee or sub-committee specifically tasked with cybersecurity. The complexity of this issue often requires a cross-government response, as appears to be the case in Sweden. Monitoring this sector is also complicated because an important part of cyber protection is provided by private actors, and parliamentary committees do not have an adequate mandate to monitor this type of activity. Nevertheless, unlike several national cybersecurity strategies, the Swedish strategy sets up strategic principles and an action plan, which may help the parliament to hold a variety of non-governmental actors accountable.

The justice sector plays a pivotal role in overseeing the activities of the security sector. For example, the justice sector may grant special powers to law enforcement and intelligence service agencies by issuing search warrants. This can play an important role in the context of communication interception, although judicial control is often circumvented or limited for reasons of national security or states of emergency.

Achieving good security sector governance is both a process and the goal of security sector reform.

Civil society plays a key role in security sector oversight, complementing the oversight functions of legislative and judicial authorities. Civil society can provide policy guidance and technical expertise. As a public watchdog, it can also facilitate dialogue and negotiations. Additionally, civil society also helps to raise awareness of various issues and can guide policy-making. The media, in particular, can investigate and support access to information by looking deeper into cross-cutting issues of concern.

CASE STUDY: THE ROLE OF PRIVATE COMPANIES IN SELLING SURVEILLANCE TECHNOLOGY TO GOVERNMENTS

Private companies, such as the Italian company Hacking Team, have sold remote intrusion systems to various countries, including Egypt, Nigeria, Uzbekistan, Turkey, Morocco, and Colombia. This growing trend has triggered discussions on the potential use of these technologies as a means of repression and as a tool to commit human rights violations.

Mass surveillance constitutes an emerging challenge, and private companies continue to sell surveillance tools and technologies to various countries. While civil society organizations are raising awareness about the risks posed by this business practise –including the launch of a searchable database on more than 520 surveillance companies that sell their tools to governments around the world – this issue remains poorly regulated.

2.2 Developing norms and institutions that promote and strengthen transparency, making information freely available and accessible

In general, transparency has a two-fold purpose: to promote information sharing, which can in turn improve the effectiveness of security sector institutions, and to play a key role in ensuring their accountability. Moreover, ICTs are also a tool to promote and strengthen transparency, making information publicly accessible to citizens.

While it is impossible to achieve absolute transparency in the security sector, it is also not necessarily appropriate in certain contexts.

It is important to understand this 'transparency dilemma' with regard to promoting a culture of trust and openness between public and private security providers. Limiting transparency must be an exception to the rule, however, and should be clearly defined by national legislation.[8]

Transparency also increases general understanding of cybersecurity risks and encourages governments, private companies, and civil society to coordinate and collaborate more effectively to prevent and respond to these risks.

Understanding cyber risks can help individuals who use these technologies to make informed decisions. This is essential as individual users of technologies are often considered to be the weakest link in the (cyber)security chain. Improved information channels can support better online behaviour, also referred to as good 'cyber hygiene', which in turn is likely to reduce the impact of most malicious activities.

8 Iulian F. Popa, Extensive Transparency as a Principle of Cyberspace Governance and Cyber Security Dilemma Prevention, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603326.

In this respect, a multi-stakeholder approach can also contribute to fostering transparency and may increase awareness of cybersecurity risks.

EXAMPLES OF GOOD PRACTICE

The Organization for Security and Co-operation in Europe (OSCE) adopted an agreement on confidence-building measures in 2014. These voluntary measures call for states to share their national viewpoints on cybersecurity, including their strategy and the challenges they face. OSCE Members further agreed to share information on national organizations, programmes, and strategies relevant to cybersecurity, in order to identify points of contact to facilitate communication and dialogue on ICT-related security matters.

El Salvador has enacted laws on data protection and access to public information, both of which establish norms for transparency and freedom of information.

(Source: https://publications.iadb.org/handle/11319/7449, p. 74)

The Organization of American States published a report on computer security incident response teams (CSIRTs), identifying different ways to enhance cooperation between CSIRTs for information-sharing purposes.

(Source: https://www.sites.oas.org/cyber/Documents/2016%20-%20Best%20Practices%20CSIRT.pdf)

Encouraging the establishment of public-private partnerships can contribute to an environment that is conducive to information exchange and access.

2.3. Strengthening the rule of law in cyberspace

Cyberspace may also represent a new realm for unlawful behaviour, for example through the dissemination of hate speech, child pornography, incitement to violence, copyright infringements, fraud, identity theft, money laundering, or denial-of-service attacks.[9] Such criminal acts are becoming increasingly transnational.

The Council on Europe has noted that 'the digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision-making.'[10] Consequently, the rule of law may be undermined by the erosion of privacy rights and other fundamental freedoms, such as the freedom of expression.

9 Council of Europe, The Rule of Law on the Internet and in the Wider Digital World, Issue paper published by the Council of Europe Commissioner for Human Rights, Executive summary and Commissioner's recommendations (2014), http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf.

10 Ibid., p. 6.

The United Nations Secretary-General explained the concept of the rule of law in the following way:

For the United Nations, the rule of law refers to 'a principle of governance in which all persons, institutions, and public and private entities, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance or arbitrariness and procedural and legal transparency'.

(Source: UN Secretary-General's report 'The rule of law and transitional justice in conflict and post-conflict societies', S/2004/616 (23 August 2004), para 6, https://www.un.org/ruleoflaw/files/2004%20report.pdf)

The principle of the rule of law has been further interpreted by international courts, such as the European Court of Human Rights (ECtHR). The ECtHR has developed a set of requirements for measuring compliance with the rule of law whereby 'all restrictions on fundamental rights must be based on clear, precise, accessible and foreseeable legal rules, and must serve clearly legitimate aims; they must be "necessary" and "proportionate" to the relevant legitimate aim [...] and there must be an "effective [preferably judicial] remedy"' available.[11]

Governments have called on private companies that own social media platforms to ensure their services are not misused to promote violent extremism and terrorism.

In order to meet such government requests, private companies, especially social media corporations such as Facebook, Google, and Twitter, have developed terms of service and codes of conduct to regulate content hosted on their social media platforms – thereby establishing norms for the internet. However, these terms of service and codes of conduct vary between platforms, creating ambiguity and legal uncertainty as to what kind of content is prohibited.

CASE STUDY: THE ROLE OF SOCIAL MEDIA COMPANIES IN POLICING THEIR PLATFORMS

While the right of social media companies to control their platforms and identify 'community standards' is uncontested, when it comes to terrorism, social media companies may de facto act as regulators, with the authority to restrict free speech on their platforms without being bound by international human rights law. Moreover, social media companies are under increasing pressure from states to keep their platforms free from any violent speech that incites, glorifies, or promotes terrorism.

Consequently, these social media companies have updated their community standards to address this pressing demand from states – often leading to ambiguous regulations on different platforms.

11 Ibíd., p. 8.

Facebook, for instance, does not allow any organizations or individuals engaged in terrorist activity to have a presence on Facebook. The terms 'terrorist activity' and 'terrorist organization' are thereby defined as 'any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate a civilian population, government, or international organization to achieve a political, religious or ideological aim'. A terrorist act is defined as 'a premediated act of violence against persons or property carried out by a non-state actor to intimidate a civilian population, government, or international organization to achieve a political, religious, or ideological aim'.

(Source: https://www.facebook.com/communitystandards/dangerous_individuals_organizations)

Twitter, on the other hand, does not refer to terrorism in its rules, but instead prohibits hateful content that incites violence or directly attacks or threatens others because of their race, ethnicity, origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease. In addition, Twitter prohibits the glorification of violence on its platforms as well as violent threats. Examples of glorification of violence include mass murder, terrorist attacks, rape, and sexual assault.

(Source: https://help.twitter.com/en/rules-and-policies/violent-threats-glorification)

Snowden's revelations demonstrated that intelligence agencies routinely tap into private communications and intercept these using so-called 'back-doors'. In other words, in relation to national security, there is no real cornerstone to uphold the rule of law. Existing fundamental principles, however, could provide a foundation for ensuring respect for this essential part of the universal framework for the protection of human rights. Given the increased number of partnerships between law enforcement, intelligence, and security agencies, this weakening of the rule of law may also affect the work of police officers and prosecutors. The absence of clear legal frameworks at the national and international levels is an additional threat to the rule of law online and in the wider global digital environment.

Certain developments in international law are also undermining the principle of the rule of law, including the move towards voluntary, non-binding, and ad-hoc rules and regulatory frameworks that govern security sector actors' behaviour in cyberspace. (For an overview of the existing international and regional legal framework, see Chapter 3.)

CASE STUDY: PRIVATIZED LAW ENFORCEMENT IN CYBERSPACE

The fact that the internet and the global digital environment is largely controlled by private entities – particularly, but not exclusively, US companies – also poses a threat to the rule of law. Such private entities can impose, and be 'encouraged' to impose, restrictions on access to information without being subject to the constitutional or international law constraints that apply to states when limiting the right to freedom of expression. These private

entities can also be ordered by national judicial systems, acting at the request of other private entities, to perform highly intrusive analyses of their data to detect probable (or merely possible) infringements of private property rights, which often concern intellectual property rights.

Private entities may be ordered to 'extract' data, including governmental, commercial, and personal data, from servers in other states for law enforcement or national security purposes. They can do this without obtaining the state's consent – or the consent of the companies or individuals in the other state – in violation of the other state's sovereignty, the commercial confidentiality to which companies are entitled, and the human rights of the individual concerned.

The liability of social media companies ('intermediary liability') should be interpreted more closely. In other words, a thorough assessment should evaluate whether companies such as Google, Facebook, or YouTube can be held liable for content posted on their platforms, as this can have a direct effect on freedom of expression and other human rights. However, governments around the world are putting increasing pressure on such companies to impose stricter content control, encouraging a climate of 'self-censorship'.

EXAMPLES OF GOOD PRACTICE

The Manila Principles on Intermediary Liability stipulate that 'intermediaries must not be required to restrict content unless an order has been issued by an independent and impartial judicial authority that has determined that the material at issue is unlawful'. The Manila Principles also state that any decision by an intermediary to restrict content must be supported by evidence sufficient to document the legal basis of the order. The Manila Principles stress the importance of integrating the principles of transparency and accountability into laws, noting that governments must not use extra-judicial measures to restrict content. Such extrajudicial measures may include collateral pressure to impose changes in the terms and conditions of service, to promote or enforce so-called 'voluntary' practices, and to establish agreements that restrict trade or the public dissemination of content. (Source: https://www.manilaprinciples.org/)

In Argentina, the draft law on intermediary liability states that 'internet service providers shall not be held liable for content created by third parties, except when they have been duly notified of a court order to remove or block content'.

(Source: Comisión de Sistemas de Communicación y Libertad de Expresión, https://www.infobae.com/tecno/2017/11/21/como-es-el-proyecto-de-ley-que-regula-la-responsabilidad-de-los-intermediarios-de-internet/)

KEY FINDINGS

- It is useful to think of security in terms of governance because it emphasizes how a variety of state and non-state actors exercise power and authority over security, both formally and informally and at the international, national, and local levels.
- Governance is an umbrella term that can be applied to security in general to explain how international, national, and local actors play a role in shaping and implementing decisions about security.
- The principles of good SSG are accountability, transparency, the rule of law, participation, responsiveness, effectiveness, and efficiency.
- Good SSG is based on the view that the security sector should be held to the same high standards of public service delivery as other public sector service providers.
- Good SSG is founded on a set of principles; the same core principles of good governance therefore apply differently to each security sector.
- Good SSG means continuously adapting to respond to ever-changing security threats.
- SSR improves the ability of the security sector to provide security for the state and its citizens.
- SSR ensures the efficient use of public resources in the security sector.
- SSR reduces the risk of corruption by strengthening oversight and accountability.
- SSR protects the professional independence of security personnel, enabling them to fulfil their tasks effectively. It also enhances professional standards and strengthens accountability, reducing cases of abuse.
- SSR promotes inclusive security provision as well as equal opportunities within the security sector.
- SSR prevents conflict by promoting unity, political neutrality, equality, and professionalism within the security sector.

RESOURCES

DCAF, Security Sector Governance: Applying the Principles of Good Governance to the Security Sector, DCAF SSR Backgrounder series, (Geneva: DCAF 2015), https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf.

DCAF, Security Sector Reform: Applying the Principles of Good Governance to the Security Sector, DCAF SSR Backgrounder series (Geneva: DCAF 2015), https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf.

DCAF-The International Security Sector Advisory Team (ISSAT), SSR in a Nutshell: Manual For Introductory Training on Security Sector Reform, https://issat.dcaf.ch/download/2970/25352/ISSAT%20LEVEL%201%20TRAINING%20MANUAL%20-%20SSR%20IN%20A%20NUTSHELL%20-%205.3.pdf.

DCAF-ISSAT, 'Introduction to Security Sector Reform', A free e-learning course available on the DCAF-ISSAT Community of Practice website: http://issat.dcaf.ch.

Heiner Hänggi, Security Sector Reform – Concepts and Contexts in Transformation: A Security Sector Reform Reader (Pasig: INCITEGov, 2011, pp. 11-40).

Hans Born and Albrecht Schnabel (eds.), Security Sector Reform in Challenging Environments (Münster: LIT Verlag, 2009).

Global Forum on Cyber Expertise, 'Raising Cybersecurity Awareness by Building Trust through Transparency', https://thegfce.org/raising-cybersecurity-awareness-by-building-trust-through-transparency/.

Evert A. Lindquist and Irene Huse, 'Accountability and Monitoring Government in the Digital Era: Promise, Realism and Research for Digital-era Governance' (Canadian Public Administration, 2017), https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12243.

CHAPTER 2
HOW DO CYBERSPACE AND CYBERSECURITY RELATE TO GOOD SECURITY SECTOR GOVERNANCE?

OBJECTIVES

This chapter's goal is to increase readers' knowledge of cyberspace and cybersecurity, as well as to highlight the complexities of implementing good security sector governance (SSG) practices in these fields.

THIS CHAPTER AIMS TO:

- increase knowledge of the scope and risks of cyberspace and the actors involved;
- increase knowledge of cybersecurity and its impact on human security, national security, and service provision; and
- improve understanding of the methods and challenges of implementing good SSG practices in cyberspace.

1. Introduction

As discussed in the previous chapter, good SSG practices are necessary to support an effective and accountable environment where human rights and the rule of law are respected. Since the security sector includes both state and non-state actors, the principles of good SSG should extend beyond state practice alone.

Good SSG in cyberspace is a relatively new concept that has a profound impact on both governments and private citizens. Since cyberspace and related activities and services have become an integral part of everyday life, it is essential to ensure the protection of data and information in cyberspace.

Despite the need for data protection – and perhaps owing to its diverse nature – the concept of cyberspace, including its various components, is not well defined. To apply good SSG practices to cyberspace effectively, a better understanding of the meaning of 'cyberspace' and 'cybersecurity' is needed.

What is cyberspace?

The meaning of the term cyberspace is unclear because the concept seems, by its nature, abstract and detached from the physical world.

Organizations and nations often define cyberspace in a way that reflects their objectives or uses for it. These definitions frequently focus on security, militarization, or vulnerabilities present in cyberspace, with each organization, nation, or group focusing on different aspects therein. There is, however, a common ground found in most definitions: cyberspace is an environment created by both physical and virtual components where data, information, or communication are stored, modified, or exchanged.

While the internet may be the most common and easily accessible form of cyberspace for individuals, it is by no means the only one.[1] Cyberspace includes any computer network system that serves to store, modify, or exchange[2] information This function can be found, for example, in an increasing number of watches, appliances, and other items connected in cyberspace, also known as the 'internet of things' (IoT). These different streams of data and information combine to form the 'virtual' construct that is referred to as cyberspace.

Cyberspace is a global domain, offering a wealth of resources, information, and opportunities. It has become such an integral aspect of everyday life that the United Nations Human Rights Council, in 2016, affirmed 'that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Article 19 of the Universal Declaration of Human Rights and the International

1 Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward, DCAF Horizon Working Paper No. 4, (Geneva: DCAF, 2015), p. 8, https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf.

2 Benjamin Buckland, Fred Schreier, and Theodor H. Winkler, Democratic Governance Challenges of Cybersecurity, DCAF Horizon Working Paper No. 1, (Geneva: DCAF, 2015), p. 9, https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

Covenant on Civil and Political Rights'.[3]

Cyberspace also comprises physical components, including computers, laptops, tablets, and smartphones, as well as servers and cables that form the infrastructure of the internet. Cyberspace enables people to conduct activities that often resemble those of the physical world: people rely on cyberspace to communicate, trade, research, engage in recreational activities, and keep up to date with the news. However, cyberspace can also be used for more sinister activities, such as criminal operations, military attacks, and other nefarious activities.

Defining cyberspace

Definitions of cyberspace currently include the following:

International Telecommunication Union (ITU)

'Cyberspace is the environment in which communication over computer networks occurs. And almost everybody in one way or another is connected to it.'

International Organization for Standardization

'[The] complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.'

European Union

'Cyberspace is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information.'

South Africa

'"Cyberspace" means a physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks and their computer programs, computer data, content data, traffic data, and users.'

(Sources: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), https://ccdcoe.org/cyber-definitions.html; ENISA, ENISA Overview of Cybersecurity and Related Terminology, ver. 1. European Union, (September 2017), https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology; State Security Agency, 'The National Cybersecurity Policy Framework of South Africa', Government Gazette, No. 609 (December 2015), p. 8)

3 The promotion, protection and enjoyment of human rights on the Internet. 32nd session of the Human Rights Council (27 June 2016), A/HRC/32/L.20.

EXAMPLE OF GOOD PRACTICE

At the beginning of the 21st century, France had one of the lowest rates of internet and computer usage within the European Union. Today, however, a large majority of the population uses cyberspace. To further increase the accessibility and usability of cyberspace, France has launched 'Très Haut Débit', a new initiative to promote high-speed internet access, particularly for rural and under-connected communities. By partnering with public and private groups, France aims to reach 100 per cent broadband coverage and to offer digital access to all citizens by 2022.

(Source: http://www.francethd.fr/le-plan-france-tres-haut-debit/qu-est-ce-que-le-plan-france-tres-haut-debit.html)

Although the institutional definitions of cyberspace have certain features in common, their ambiguous nature allows actors in cyberspace to interpret them in a way that suits their needs and justifies their actions. This is particularly striking when considering how to utilize best or protect the medium. The definitions are also indicative of the way in which states view cyberspace, whether as a tool for the military, a platform through which to distribute services, or an arena for trade and communication.

For the purposes of this report, cyberspace is defined as the global, networked environment that enables the exchange, storage, and modification of data and information, and that is accessible to both state and non-state actors.

The use and control of cyberspace

Given the wide-ranging character of cyberspace, it is only logical that it involves a variety of uses and users, including both state and non-state actors. States use cyberspace to hold elections, to provide services to their populations, and to protect national security and vital national interests.[4] Non-state actors range from companies to individuals, all using cyberspace for different purposes. All of these actors contribute to influencing and shaping cyberspace.

The global nature of cyberspace also places constraints on governments regarding its regulation and governance. Although strengthening cybersecurity as a part of national security policy is important, supporting good SSG in cyberspace also has a significant impact on both economic and human security.[5] In a world that is increasingly dependent on the services and freedoms provided by cyberspace, it is essential to ensure the protection of human rights and human security, as well as national security.[6]

4 Liaropoulos, Andrew N., 'Cyberspace Governance and State Sovereignty', in Democracy and an Open-Economic World Order, edited by George C. Bitros and Nicholas C. Kyriazis, (Springer International Publishing AG, 2017), pp. 25-35.

5 Cole, Kristina et al., Cybersecurity in Africa: An Assessment. Atlanta: Georgia Institute of Technology, https://www.researchgate.net/publication/267971678.

6 Benjamin Buckland, Fred Schreier, and Theodor H. Winkler, "Democratic Governance Challenges of Cybersecurity" DCAF Horizon 2015 Working Paper no. 1. Geneva: Democratic Control of Armed Forces, p. 9, https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

CASE STUDY: SECURING DEVICES

Recent initiatives have aimed to strengthen the security of computer devices, such as laptops, tablets, and smartphones. The European Union and its member states, as well as the United States, have all begun to put pressure on technology manufacturers to ensure their products' security.

In 2016, the United States Department of Homeland Security released a number of strategic principles aimed at securing the IoT. This approach begins by securing the devices at the manufacturing stage, then goes on to maintain security through updates and vulnerability management.

The United Kingdom created a 'security code of practice' for manufacturers to encourage them to strengthen the security of devices during the manufacturing phase. To increase the security of the devices themselves, the code recommends that IoT devices have unique passwords It also calls for greater transparency in case of security breaches and encourages the public to disclose any device vulnerabilities. The code is currently applied on a voluntary basis only, but the UK has not ruled out the possibility of making it mandatory for devices manufactured in the country.

The EU is still developing a plan to increase device security. Its aim is to create an EU-wide certification process for IoT devices.

All of these approaches endeavor to encourage other nations to develop their own approaches and policies with a view to securing cyberspace-connected devices.

(Source: https://www.ft.com/content/d21079b0-8a79-11e8-affd-da9960227309)

Cybersecurity

With the increasing use of cyberspace by governments, individuals, and companies, the amount of sensitive data and information circulating in cyberspace is growing exponentially and becoming subjected to new and evolving vulnerabilities.[7] Protecting information effectively is essential to create a secure environment both within and outside of cyberspace. Cybersecurity, as the term implies, refers to practices and methods for securing data, information, and the integrity of various elements of cyberspace, including, but not limited to, its physical components.[8]

Although cybersecurity is often associated with national security strategies, it is important to consider broader definitions of the term. The International Telecommunications Union (ITU) describes cybersecurity as a set of tools, policies, guidelines, and other approaches to protect integrity and confidentiality in cyberspace for private organizations, governments, and civil society.[9]

7 Schreier, Fred, Barbara Weekes, Theodor H. Winkler, Cyber Security: The Road Forward, DCAF Horizon Working Paper, No. 4, (Geneva: DCAF, 2015), p. 11, https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf.

8 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

9 International Telecommunication Union (ITU), Guide to Developing a National Cybersecurity Strategy (2018), p. 13, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Cybersecurity is an evolving domain within the broader framework of security and good SSG; its development reflects the growing importance of cyberspace for professional, recreational, and political activities. The norms pertaining to cyberspace security are constantly evolving to respond to the rapid growth of cybersecurity practices and techniques, as well as the diverse range of actors.[10] As states develop strategies to enhance cyberspace security at the national level, certain norms are emerging on the scope and application of their control over cyberspace.[11]

Cybersecurity Metrics

The diverse range of definitions of cyberspace and cybersecurity complicates any analysis of what constitutes cybersecurity. The ITU created the Global Cybersecurity Index to determine the commitment of member states to strengthening cybersecurity. The index evaluates five different aspects of cybersecurity – legal, technological, organizational, capacity building, and cooperation – to measure each state's level of commitment.

While the tool serves to evaluate the commitment of states and their activities related to cyberspace governance, it does not take into account the role of non-state actors in both cyberspace and cybersecurity. Since it evaluates policies rather than practices, it also does not assess the practical impacts or effectiveness of these commitments.

2. SSG in cyberspace

Cyberspace presents a unique set of freedoms, restrictions, and complexities. The diverse range of actors in cyberspace, along with the fact it serves both positive and negative purposes, creates challenges for developing a framework for good SSG practices, which differ from those faced by states regulating more traditional 'territorial' security issues. Some of these challenges were discussed in the previous chapter and relate primarily to elements that undermine the rule of law, transparency, and accountability.

In viewing SSG through a cyberspace lens, it is important to consider various actors in this sphere, to evaluate who controls which areas of cyberspace, and to analyse how best to influence or incentivize behaviours and practices that will ultimately strengthen good SSG in cyberspace. The diverse range of actors in cyberspace and cybersecurity creates an unprecedented challenge for policy-makers, since states are unable to ensure unilaterally effective security and regulation.

10 Microsoft, 'International Cybersecurity Norms', Microsoft Policy Papers, https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-overview.

11 Ibid.

Good Practice: It is important to implement a cybersecurity approach that involves actors from both public and private sectors in cyberspace.

Since cyberspace is a platform for both private and public actors, the creation and implementation of policies tackling SSG should include entities that exist outside of the public sphere. Recognizing the role that information and communication technology (ICT) companies and private cybersecurity companies play in terms of training, protecting users' rights, and security is an important step towards creating a more secure cyber environment.

EXAMPLES OF GOOD PRACTICE

The Government of Cameroon works with a number of private sector partners on cybersecurity-related issues and has established working relationships with other countries when managing and responding to cyber threats. Most notably, following an online scam involving a company selling pharmaceuticals, Cameroon partnered with the Czech Republic, INTERPOL, and Nigeria to investigate cases of internet fraud. Cameroonian authorities support several confidence-building measures and promote international cooperation agreements in cyberspace by exchanging information on cyber incidents and best practices for cybersecurity.

Current challenges for applying the principles of SSG to cyberspace

Applying the principles of good SSG to cyberspace can help ensure that human security, the rule of law, and other aspects of good governance are observed and protected in cyberspace.

As mentioned briefly in the previous chapter, one of the challenges facing SSG in cyberspace is a lack of understanding of how to implement effective governance principles to it, resulting in inadequate policies and regulations, and creating an environment conducive to criminal activity.[12] This lack of knowledge can also impact the effectiveness of state regulation of private sector actors, undermining the state's ability to apply the principles of good SSG to cyberspace.

Currently, many cyberspace security services are provided by private commercial entities, posing challenges for the effective implementation of SSG practices in cyberspace. One aspect of good governance that is becoming increasingly difficult for states to ensure is transparency. There is no clear definition of what constitutes transparency within the context of good SSG; however, the term transparency in this domain is increasingly associated with disclosing when – and to what extent – a breach of information systems has occurred.[13]

12 Buzatu, SSG/SSR in Cyberspace, pp. 7-8.

13 See, for example, ICANN Organization's Cybersecurity Transparency Guidelines (2018), https://www.icann.org/en/system/files/files/cybersecurity-transparency-guidelines-03aug18-en.pdf.

A state can strengthen good SSG practices by encouraging or requiring actors to disclose cybersecurity breaches. This not only increases transparency within cyberspace, but also ensures that gaps within current cybersecurity practices are addressed, thus helping to prevent the proliferation of cyber-attacks and improving security practices in cyberspace.[14] A lack of transparency in relation to cyber-attacks greatly undermines human security in cyberspace, as it can increase the number of victims affected by malicious cyber-attacks.

CASE STUDY: ENFORCING TRANSPARENCY

Australia

The Australian parliament passed an amendment to the Privacy Act of 1998 in 2017 that requires Commonwealth government organizations, private sector organizations, and other specified bodies to disclose information regarding cybersecurity breaches to those impacted by the incident. If these actors fail to comply with the new regulation, they are obliged to pay compensation to those affected by the violation and to offer a public apology that acknowledges their responsibility and may be subject to serious civil penalties for repeat offences.

(Source: Ben Allen, 'Australia: Cybercrime – New Mandatory Data Breach Reporting Requirements', Mondaq, : http://www.mondaq.com/australia/x/573188/Security/Cybercrime+New+Mandatory+Data+Breach+Reporting+Requirements)

The United States

The US Securities and Exchange Commission imposed a large fine of USD 35 million on Yahoo for failing to disclose a cyber-attack that affected over 500 million accounts. It was the first time a company had been fined for failing to comply with disclosure requirements imposed on publicly traded companies.

(Source: Kadhim Shubber, 'Yahoo's $35m Fine Sends a Message', Financial Times, https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53)

The transnational nature of cyberspace also creates a dilemma for states seeking to implement good SSG practices. Individuals are increasingly engaged in transactions that cross international territorial borders, which significantly reduces the ability of states to control these operations and their impact on the population. In most cases, states have to rely on commercial intermediaries, such as social media platforms, to oversee and regulate online behaviour.[15] This can undermine good SSG practices, as the state typically cannot know how information is filtered or removed. The transnational nature of information on the internet presents an additional challenge, because the data can be stored on one or more servers located in multiple jurisdictions. State authorities must therefore rely on a new form of cooperation with other states to investigate, persecute, and convict cybercriminals. As a result, cyberspace can undermine good

14 Paul Smith 'New mandatory data breach notifications laws to drag Australia into cyber age', Financial Review, (23 Feb 2018), https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa.

15 Niva Elkin-Koren and Haber, Eldar, 'Governance by Proxy: Cyber Challenges to Civil Liberties', Brooklyn Law Review, Vol. 82, No. 1, p. 105.

governance practices as it involves not only actors within the jurisdiction of a single state, but also a variety of international actors.

Despite these challenges, applying good SSG practices to cyberspace is not impossible. International frameworks and norms providing guidance on how to integrate SSG into cyberspace are beginning to emerge. While practices and policies must be tailored to fit the national context, identifying the relevant international and regional frameworks for cyberspace is a key step towards applying the principles of good SSG to cyberspace.

CASE STUDY: INTERNATIONAL INVESTIGATIONS

Cybersecurity has already led to international investigations and criminal prosecution. In April 2018, a website that sold distributed denial-of-service (DDoS) services, Webstresser.org, was frozen and the administrators charged with cybercrimes thanks to an international investigation led by the Dutch National High-Tech Crime Unit and the UK National Crime Agency, with the support of many other organizations. Operation Power Off is just one example of how international actors can work together to create a more secure cyber environment for users.

(Sources: Cal Jeffrey, 'Operation Power OFF pulls the plug on "DDoS-for-hire" website', TechSpot, (25 April 2018), https://www.techspot.com/news/74327-operation-power-off-pulls-plug-ddos-hire-website.html and Europol, 'World's Biggest Marketplace Selling Internet Paralysing DDoS Attacks Taken Down', Press Release (25 April 2018), https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down)

KEY FINDINGS

- Cyberspace extends to both physical and virtual domains and comprises any platform used to transfer, transform, or modify information, data, and communication from one computer to another. It also encompasses the physical infrastructure of the internet that spans the globe.
- Governments, citizens, and companies are increasingly reliant on the resources provided by cyberspace for day-to-day activities.
- A wide variety of actors are involved in cyberspace and cybersecurity.
- Initiatives aimed at applying the principles of SSG to cyberspace face several challenges, including the diverse range of actors who influence various elements of cyberspace and a lack of general knowledge on how to use cyberspace safely.
- Although some states have policies and frameworks in place for cybersecurity and cyberspace governance, a general lack of knowledge makes it difficult to ensure the proper implementation of SSG practices in cyberspace.

Resources

Buckland, Benjamin, Fred Schreier, and Theodor H. Winkler, Democratic Governance Challenges of Cybersecurity, DCAF Horizon Working Paper, No. 1. (Geneva: DCAF, 2015), https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf.

Elkin-Koren, Niva and Haber, Eldar, 'Governance by Proxy: Cyber Challenges to Civil Liberties', Brooklyn Law Review, Vol. 82, No. 1, p. 105 (2016).

Schreier, Fred, Barbara Weekes, Theodor H. Winkler, Cyber Security: The Road Forward, DCAF Horizon Working Paper, No. 4. (Geneva: DCAF, 2015), https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf.

Liaropoulos, Andrew N., 'Cyberspace Governance and State Sovereignty', in Democracy and an Open-Economic World Order, edited by George C. Bitros and Nicholas C. Kyriazis, pp. 25-35 (Springer International Publishing AG, 2017).

Smith, Paul, 'New mandatory data breach notifications laws to drag Australia into cyber age', Financial Review, (23 February 2018), https://www.afr.com/technology/new-mandatory-data-breach-notifications-laws-to-drag-australia-into-cyber-age-20180222-h0whxa.

Cole, Kristina, Marshini Chetty, Christopher LaRosa, Frank Rietta, Danika K. Schmitt and Seymour E. Goodman, Cybersecurity in Africa: An Assessment, (Atlanta: Georgia Institute of Technology), https://www.researchgate.net/publication/267971678.

CHAPTER 3
INTERNATIONAL AND REGIONAL LEGAL FRAMEWORKS IN CYBERSPACE

OBJECTIVES

This chapter provides readers with an overview of the international and regional legal frameworks applicable to cyberspace, and highlights noteworthy and innovative approaches and initiatives.

THIS CHAPTER AIMS TO:

- increase knowledge of various international and regional organizations relevant to cyberspace and cybersecurity;
- increase awareness of available resources supporting the implementation of international and regional legal frameworks at the national level; and
- increase knowledge of cybercrime, cyberterrorism, and terrorist use of the internet.

Introduction

Effective legal frameworks – at the international, regional, and national levels – are pillars of good governance and constitute prerequisites for the rule of law. In general, legal frameworks play a key role in regulating lawful behaviour and prohibiting or criminalizing unlawful activities. Legal frameworks for cyberspace are also crucial to ensuring respect for human rights.

There has been much debate and confusion about how to apply and implement legal frameworks in cyberspace. Given its cross-border, information-centric nature, cyberspace poses challenges to state-centric approaches to governance. While the physical infrastructure of cyberspace is subject to the jurisdiction and authority of the state, it is difficult for states to control effectively the flow of data and information as it constantly crosses international borders. As a result, many actors have called for the development of new norms and standards to regulate cyberspace.

While there is now a consensus that the principles of international law should apply to cyberspace, it is less clear how to put this into practice. Consequently, this gap between policy and practice leads to uncertainties and even legal loopholes that can undermine efforts to protect the human rights of internet users. International and regional organizations have therefore launched initiatives aimed at identifying and interpreting how to apply the principles of international law to cyberspace .

1. International and regional legal frameworks

Numerous initiatives at the international and regional level aim to promote more responsible behaviour and develop regulatory frameworks and confidence-building measures in cyberspace. This section summarizes some of these initiatives.

United Nations

There is currently no legally binding instrument at the international level regulating behaviour in cyberspace. Several non-legally binding initiatives, however, identify norms that can be applied to cyberspace, and provide guidance for states on how to implement these.

It is now widely accepted that international law – particularly the United Nations Charter, international human rights law, and international humanitarian law – applies in cyberspace.

CASE STUDY: UN GROUP OF GOVERNMENTAL EXPERTS REPORT

The 2015 report of the UN GGE lists the following recommendations for the responsible behaviour of states to contribute to an open, secure, stable, accessible, and peaceful cyberspace:

Positive norms:

- States should cooperate to increase the stability and security of information and communication technologies (ICT) use and to prevent harmful practices.
- States should consider all relevant information with regard to attribution in the ICT environment.
- States should take appropriate measures to protect critical national infrastructure from ICT-related threats, and respond to requests for assistance from other states.
- States should take reasonable steps to ensure the integrity of the supply chain and to prevent the proliferation of malicious ICT tools and techniques.
- States should encourage responsible reporting of ICT vulnerabilities and share related information.

Limiting norms:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
- States should adhere to United Nations General Assembly (UNGA) resolutions on human rights.
- States should not knowingly support ICT-related activities that violate its obligations under international law.
- States should not conduct or knowingly support activities that aim to harm the information systems of authorized emergency response teams.

For example, since 2004, the United Nations, has established six consecutive Groups of Governmental Experts (UN GGE) to develop norms for responsible behaviour in cyberspace. Each group's membership is based on 'equitable geographical representation' and includes key 'cyber powers', such as the United States, China, Russia, France, the United Kingdom, and Germany.

CASE STUDY: ONLINE ELECTION INTERFERENCE: A CASE FOR INTERNATIONAL LAW?

Cases of interference in political processes, whether covertly or overtly, are not a new phenomenon in international relations. However, since 2016, governmental officials, primarily from Western states, have expressed concern about instances of election interference through targeted cyber operations and misinformation campaigns.

In 2014, CyberBerkut targeted the Ukrainian Central Election Commission, disrupting parts of the commission's networks for almost 20 hours and announcing false results on election day. In 2016, the Fancy Bear hacking unit targeted the computer networks of the German Bundestag, the Germany Foreign and Finance Ministries, and the Christian Democratic Union. In 2017, presidential candidate Emmanuel Macron's campaign was subject to cyber attacks that aimed to install malware on campaign websites.

Under international law obligations, it is likely that these incidents constitute a violation of a state's sovereignty. Sovereignty is widely considered a key principle and rule of international law – a definition echoed in the 2015 report of the UN GGE:

> 'States sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.'

Generally, the principle of sovereignty is intended 'to afford states the full control over access to and activities on their territory'.

What are the implications for election interference through cyber attacks? According to experts in the field, to assess whether an action constitutes a violation of the principle of sovereignty, the key consideration is 'not that there was a nexus between the targeted system and the election, but instead simply that the operation resulted in the requisite harm – a loss of functionality'. According to the Tallinn Manual 2.0, the following actions may constitute a violation of sovereignty: altering cyber infrastructure or programmes through cyber operations; modifying or deleting data stored in cyber infrastructure without physical or functional consequences, as described above; installing malware on a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a serious distributed denial-of-service operation.

A major breakthrough came in 2013, when the UN GGE – consisting of only 15 members at the time – adopted by consensus a report endorsing the application of international law in cyberspace. The 2015 UN GGE report, also adopted by consensus, reaffirmed this statement and clarified the scope of the normative framework for states' use of cyber capabilities. The section on 'norms, rules, and principles for the responsible behaviour of states is of particular interest.

Unfortunately, the 2016-2017 UN GGE failed to adopt a report by consensus, leading to confusion within the international community about how to apply international law

in cyberspace. However, in October 2018, the UNGA adopted resolution A/C.1/73/L.37 establishing another GGE in 2019 and tasking the group to report back in 2021 at the UNGA's 76th session. In parallel, through resolution A/C.1/73/L.27/Rev.1, the UNGA also created an Open-Ended Working Group, to be convened in June 2019, to develop rules, norms, and principles for regulating responsible state behaviour in cyberspace, as well as to consider their practical implementation.

It is generally accepted that the international human rights law framework, including the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), applies to cyberspace. This was affirmed by the Human Rights Council (HRC) in resolution A/HRC/20/L.13, which states that the 'same rights that people have offline must also be protected online'.[1] This resolution is particularly important because it was the first time that the international body explicitly stated that human rights also apply to cyberspace.

INFOBOX: ANONYMITY ON THE INTERNET

Anonymity is fundamental to safeguard human rights. With the advent of the Internet, it has become clear that the importance of anonymity cannot be restricted only to the freedom of individuals to communicate with each other, exchange information and ideas, but also to protect individuals from unnecessary and undue scrutiny.
However, the right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data (see Article 12 UDHR, 17 ICCPR).
In addition, anonymity is a key concept in the protection of freedom of expression as well as the right to privacy. At its simplest, anonymity is the fact of not being identified and, in this sense, it is part of the ordinary experience of most people on a daily basis, e.g. walking as part of a crowd or standing in a queue of strangers. In this way, an activity can be anonymous even though it is also public.

Source: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

Following the Snowden revelations,[2] in 2015, the UNGA decided to establish a new Special Rapporteur on the right to privacy to strengthen privacy in the digital age and to create a safer digital environment. The Special Rapporteur on the right to privacy is mandated to conduct state visits, make recommendations, and investigate individual complaints.

Another important resolution that the UNGA adopted is A/RES/57/239, which aims to create a global culture of cybersecurity and recognizes that cybercrime poses a major challenge to cybersecurity.[3]

The United Nations Guiding Principles on Business and Human Rights[4] (also known as the 'Ruggie Principles'), adopted in 2011, are also relevant for the identification of norms in cyberspace. The principles provide guidance to states and businesses on how to protect human rights. The Ruggie Principles are based on the UN's 'Respect, Protect and Remedy' framework. The introduction states that 'business enterprises as specialized organs of society performing specialized functions [are] required to comply with all applicable laws and to respect human rights'.[5]

In the context of regulating certain forms of illegal speech on the internet, particularly hate speech, the report of the UN High Commissioner for Human Rights, adopted by the HRC in 2013 (also known as the 'Rabat Plan of Action'), provides a set of criteria for identifying hate speech as well as guidance on online activities.[6]

1 United Nations General Assembly, Human Rights Council on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012

2 The Guardian, The NSA files, https://www.theguardian.com/us-news/the-nsa-files

3 https://www.sbs.ox.ac.uk/cybersecurity-apacity/system/files/UN_resolution_57_239.pdf.

4 OHCHR, Guiding Principle on Business and Human Rights, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

5 https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, p 1

6 OHCHR, Rabat Plan of Action, https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf.

CASE STUDY: THE RABAT PLAN OF ACTION

The Rabat Plan of Action identifies a six criteria for assessing the severity of certain forms of expression that may be considered criminal offences. The six criteria are the context, speaker, intent, content and form, the extent of the dissemination, and likelihood (including imminence).

The Rabat Plan of Action states that the context is of 'great importance when assessing whether particular statements are likely to incite discrimination, hostility or violence against the target group, and it may have a direct bearing on both intent and/or causation. Analysis of the context should place the speech act within the social and political context prevalent at the time the speech was made and disseminated.'

(Source: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf)

Several UN agencies and offices – such as the UN Institute for Disarmament Research (UNIDIR), the UN Interregional Crime and Justice Research Institute, and the UN Office on Drugs and Crime (UNODC) – address issues related to cybersecurity, as well as the Working Group on Countering the Use of the Internet for Terrorist Purposes, which operates under the auspices of the UN Counter-Terrorism Implementation Task Force.[7]

The International Telecommunication Union (ITU), a UN agency specialized in telecommunications, also addresses cybersecurity as part of its mandate. To this end, the ITU develops publicly available model laws and country profiles on cybersecurity, and supports UN member states in developing effective normative frameworks for cyberspace.

CASE STUDY: THE INTERNATIONAL TELECOMMUNICATION UNION'S PROJECT TO SUPPORT THE HARMONISATION OF ICT POLICIES IN SUB-SAHARAN AFRICA (HIPSSA)

HIPSSA was established in response to a request from economic integration organizations, as well as regional regulatory associations, in Africa to the ITU and the European Commission for assistance in harmonizing ICT policies and legislation in Sub-Saharan Africa.

HIPSSA plays a key role in establishing global pan-African harmonized ICT policies and frameworks.

(Source: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx)

7 United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Council of Europe

While the Budapest Convention is the only international legal framework to regulate cybercrime, human rights advocates note that it is based on the assumption that states already have human rights protection measures in place. Non-CoE member states, however, do not necessarily have these measures in place.

The Council of Europe (CoE) is comprised of 47 member states. Its Convention on Cybercrime (also known as the 'Budapest Convention')[8] is currently considered the most effective international legal instrument for addressing cybercrime. The Budapest Convention may be ratified by CoE member states, as well as by non-member states; 61 states have ratified it to date.[9] An Additional Protocol on the criminalization of acts of a racist and xenophobic nature committed through computer systems supplements the Budapest Convention.[10]

The convention is an important tool because it provides states with '(i) the criminalisation of a list of attacks against and by means of computers, (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence'.

The CoE also drafted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS Convention No. 108),[11] which aims to 'protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy'.[12]

This convention was the first legally binding international instrument on data protection. Under this convention, parties are required to adopt the necessary measures in their national legislation to ensure that the fundamental human rights of all individuals are respected in their territory with regard to the processing of personal data. The convention was updated in May 2018 to take into account the latest developments in the field of new technologies and data protection. To date, the convention has been ratified by 53 member and non-member states of the CoE.[13]

In addition, the CoE offers guidance on how to interpret the conventions as well as a range of capacity-building program, such as the Global Action on Cybercrime Extended (GLACY+) program, which supports states in developing effective legislation for cyberspace.[14]

African Union

In 2014, the African Union adopted the Convention on Cybersecurity and Personal Data Protection (also known as the 'Malabo Convention').[15] However, the convention

8 Council of Europe, Convention on Cybercrime, CETS No. 185, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

9 Notably, Senegal is party to the Budapest Convention. Tunisia and Morocco are in the process of signing and ratifying the Budapest Convention.

10 Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

11 Council of Europe, Convention for the protection of individuals with regard to the processing of personal data, CETS No. 180, https://www.coe.int/en/web/data-protection/home.

12 Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

13 The Convention No 108 was ratified by Cabo Verde, Mauritius, Senegal and Tunisia.

14 Council of Europe, Global Action on Cybercrime (GLACY), https://www.coe.int/en/web/cybercrime/glacyplus.

15 African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

has not yet entered into force, as it has been adopted by only five member states of the African Union (Ghana, Guinea, Mauritius, Namibia and Senegal) and signed by nine member states. Article 25 (1) of the Convention states that: 'Each State Party shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language used in international best practices'.

CASE STUDY: THE AFRICAN UNION'S CONVENTION ON CYBERSECURITY AND THE BUDAPEST CONVENTION

The Budapest Convention is the only legally binding international legal framework that regulates cybersecurity, cyberspace, and the state's role in this domain. Although only a few African nations have signed it or been invited to ratify it, it has served as a guiding framework for the development of the African Union's Convention on Cybersecurity. This is an example of how international norms can be adapted and adopted in a regional context.

(Source: 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime', Global Action on Cybercrime Extended. Version 20 (November 2016), pp. 3-5.)

Economic Community of West African States

In 2010, the Economic Community of West African States (ECOWAS) adopted the Supplementary Act on Personal Data Protection in the region.[16] The instrument, which mirrors the EU Data Protection Directives, specifies the provisions that should be included in data protection legislation and requires member states to establish a data protection authority.

ECOWAS also adopted a Directive on Fighting Cyber Crime (2011) and the Supplementary Act on Electronic Transactions within ECOWAS.[17]

Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) tackles cyber and ICT security issues, particularly with the aim of combating terrorism and cybercrime. In 2013, the OSCE adopted confidence-building measures (CBMs) for cyberspace through Permanent Council Decision No. 1106, 3 December 2013.[18] These CBMs aim to reduce conflict stemming from the use of ICTs.

16 ECOWAS, Supplementary Act on Personal Data Protection, See http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.

17 ECOWAS, Economic Community of West African States (ECOWAS), Directive C/DIR.1/08/11 on Fighting Cyber Crime within ECOWAS, 2011, https://www.ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf and Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS, 2010, http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Electronic-Transaction-Act.pdf.

18 OSCE Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202, 10 March 2016, https://www.osce.org/pc/227281?download=true.

The CBMs that the OSCE include the exchange of information between states, on a voluntary basis, on the following topics: cyber threats; security and the use of ICTs; national organizations and strategies, and terminology used at the national level. The CBMs also include holding consultations in order to reduce the risk of misunderstandings and possible tensions, sharing information on measures taken to ensure an open and secure internet, exchanging points of contact, and using the OSCE as a platform for dialogue.

However, the CBMs are implemented on a voluntary basis and are therefore not a legally binding instrument.

Organization of American States

The Organization of American States (OAS) established the Working Group on Cyber-Crime in 1999 as a key forum to 'strengthen international cooperation in the prevention, investigation and prosecution of cybercrime, facilitate the exchange of information and experiences among its members, and make necessary recommendations to enhance and ensure efforts to combat these crimes'.[19] The Working Group meets on a biannual basis, and provides recommendations to member states.

The SCO refers to the concept of 'international information security', focusing on the importance of content as a source of potential security threats.

The OAS also deals with cybersecurity in a wider sense. In 2004, the OAS General Assembly adopted resolution AG/RES.2004 (XXXIV-O/04), titled 'The Inter-American Integral Strategy to Combat Threats to Cyber Security', which mandated the Secretariat of the OAS Inter-American Committee to tackle terrorism. The secretariat's main tasks are to help establish national computer security incident response teams (CSIRTs), to create a network of CSIRTs, and to support the development of national cybersecurity strategies. Since 2007, the secretariat has developed a comprehensive capacity-building programme, through workshops, technical courses, roundtable policy discussions, and crisis management exercises, and encouraged the exchange of best practices.

Shanghai Cooperation Organisation

In 2009, the Shanghai Cooperation Organisation (SCO), an international organization composed of six member states (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan), adopted the Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security.[20] In 2011, four member states of the SCO submitted a draft of the International Code of Conduct for Information Security to the UNGA, and in 2015 an updated draft of the code of conduct was submitted to the UNGA.[21]

19 http://www.oas.org/juridico/english/cyber_faq_en.htm#1

20 Agreement among Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 2009, http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf.

21 Shanghai Cooperation Organisation, Draft International Code of Conduct, Letter dated 9 January 2015 to the United Nations General Assembly, A/69/723, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

CASE STUDY: SCO INTERNATIONAL CODE OF CONDUCT DRAFT (2015)

According to the SCO member states, the draft code is intended 'to push forward the international debate on international norms on information security, and help forge an early consensus on this issue'.

Some observers argue that the draft code emphasizes state sovereignty and territorial integrity in cyberspace and focuses on intelligence, national security, and regime stability imperatives. It does not provide significant human rights protection and focuses primarily on the restrictions on freedom of expression that states may impose by law. It is also noteworthy that the draft code does not mention the right to privacy.

(Source: https://citizenlab.ca/2015/09/international-code-of-conduct/)

Asia-Pacific Economic Cooperation

In 2002, the Asia-Pacific Economic Cooperation (APEC) issued its Cyber Security Strategy, which provides recommendations on cybercrime legislation, security and technical guidelines, public awareness, and training and education.[22] The Lima Declaration (2005) aims to strengthen information infrastructure to advance the work of the information society.[23] The declaration also addresses network security and emphasizes the importance of establishing computer emergency response teams (CERTs). APEC's Strategy to Ensure a Trusted, Secure and Sustainable Online Environment aims to ensure information and network security, to harmonize frameworks for securing transactions and communications, and to combat cybercrime. These goals rely increasingly on close cooperation with the private sector and other international organizations. APEC's TEL Strategic Action Plan 2010-2015 aims to 'promote a secure, resilient and trusted ICT environment' and focuses on the following key areas: resilience of critical domestic infrastructure; security and risk management; cybersecurity capacity building; cybersecurity awareness raising; cybersecurity initiatives with private companies; activities to promote a safe and secure online environment for vulnerable groups; and the internet economy.[24]

Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN), consisting of 10 member states (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar (Burma), the Philippines, Singapore, Thailand, and Vietnam), issued a Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security and explored cybersecurity-related issues in the context of counterterrorism and transnational crime.[25]

22 APEC Cyber Security Strategy, https://ccdcoe.org/sites/default/files/documents/APEC-020823-CyberSecurityStrategy.pdf.

23 APEC, Lima Declaration, 2005, https://ccdcoe.org/sites/default/files/documents/APEC-050603-LimaDeclaration.pdf.

24 https://ccdcoe.org/apec.html

25 https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf

Commonwealth of Nations

The Commonwealth of Nations comprises 53 members states and focuses on capacity building, information sharing, and providing assistance to member states to implement legal frameworks pertaining to cybercrime. Two platforms within the Commonwealth of Nations deal with this issue: the Cyber Security Forum and the Cyber Security Initiative operating under the Commonwealth Telecommunication Organisation. The latter has adopted the Commonwealth Cybergovernance Model,[26] approved by the Abuja Declaration in October 2013 and launched during the Commonwealth Cybersecurity Forum in London in 2014.[27]

The Commonwealth Cybergovernance Model[28] provides a draft set of principles for consideration, aimed at fostering a safe and effective global cyberspace, supporting economic and social development, acting individually and collectively to tackle cybercrime, and exercising rights and fulfilling responsibilities in cyberspace.

European Union

As per personal data protection, only 16 out of 55 countries in Africa have enacted comprehensive personal data protection legislation, namely: Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia.

The most relevant documents adopted by the European Union (EU) on cybersecurity are either legally non-binding documents, such as communications, or various types of legally binding acts that impose obligations on its member states or specific entities.

In 2013, the EU published its first comprehensive document – the Cybersecurity Strategy – tackling a wide range of cyber threats. In 2016, the EU adopted the Directive on Security of Network and Information Systems (NIS Directive).[29] The strategy outlines the EU's vision, roles, and responsibilities along with the actions needed in the area of cybersecurity. Importantly, the document stresses that issues related to cybersecurity should not be subject to EU oversight. Instead, state authorities should be responsible for overseeing the prevention of and responses to cyber incidents at the national level.

One of the objectives of the EU Cyber Security Strategy is to develop cyber defence policies and capacities within the framework of the Common Security and Defence Policy. The strategy also lists activities that could be carried out jointly by the European Defence Agency and members states.

Cybersecurity-related activities have also been integrated into the EU's Digital Agenda, which considers trust and security on the internet to play a key role in fostering a dynamic digital society. Notably, the European Agenda on Security identifies cybercrime as one of the most serious emerging threats.

Importantly, the EU Cyber Security Strategy stipulates that a 'particularly serious cyber incident or attack could constitute sufficient ground for a member state to invoke the EU Solidary Clause' (Article 222 of the Treaty on the Functioning of the European Union).

26 Commonwealth Cybergovernance Model, https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf.

27 Commonwealth Cybersecurity Forum in London in 2014, https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf.

28 https://ccdcoe.org/sites/default/files/documents/CommW-140304-CommonwealthCybergovernanceModel.pdf

29 European Union, Directive on security of network an information systems, L 194/1, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

On 25 May 2015, the EU General Data Protection Regulation (GDPR) entered into force.[30] This regulation has fundamentally reshaped the way data is processed across every sector, from healthcare to banking and beyond. Importantly, the GDPR applies not only to organizations within the EU but also to organizations outside of the EU, provided they offer goods and services to, or monitor the behaviour of, EU subjects.

The GDPR applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

North Atlantic Treaty Organization

The North Atlantic Treaty Organization's (NATO) first cyber-defence policy was prepared in 2008. At the Lisbon Summit in 2010, cyber defence was integrated into NATO's Strategic Concept, and the summit declaration precipitated the update of the cyber-defence policy in 2011 and the development of an accompanying action plan in 2012.

A new and improved cyber-defence policy was approved at the Wales Summit, stating that 'a major digital attack on a member state could be covered by Article 5 [of the North Atlantic Treaty]'.[31]

The policy further seeks to improve information sharing and mutual assistance among allies, enhance training and exercises, and to increase cooperation with private companies. At the Warsaw Summit in 2016, NATO included cyberspace as an area of operation, and pledged to further develop NATO-EU cyber-defence cooperation and to commit more resources to cyber-defence capacity building. In 2018, the defence ministers of NATO member states agreed to create a new cyber operation centre at Supreme Headquarters Allied Powers Europe (SHAPE) to help integrate cyberspace issues into NATO planning and operations at all levels.

NATO has established a Cyber Defence Committee (CDC), previously known as the Defence Policy and Planning Committee – Cyber Defence. The committee is a senior advisory body. It provides guidance to NATO member states and is responsible for overseeing NATO's internal cyber-defence capacities. In addition, the Cyber Defence Management Board (CDMB) operates under the auspices of the Emerging Security Challenges Division of NATO Headquarters, and is composed of representatives of all major cybersecurity stakeholders within NATO. Notably, the CDMB provides strategic planning and executive direction for NATO networks and signs memorandums of understanding with member states in order to facilitate information exchange and coordinate assistance.

Furthermore, the NATO Consultation, Command and Control (C3) Board is the main consultation committee on technical and implementation issues related to cyber defence.

30 European Union General Data Protection Regulation, https://eugdpr.org/the-regulation/gdpr-faqs/.

31 North Atlantic Treaty, 1949, https://www.nato.int/cps/ie/natohq/official_texts_17120.htm.

The Group of Seven

The Group of Seven (G7) is in informal group of seven states (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States – the EU has observer status) that regularly meets to discuss important political and economic questions. Since 2016, the G7 has produced a number of documents on cybersecurity, which has become a major theme in various summit declarations.[32]

2. Initiatives by Non-State Actors

Owing to that fact that states have been reluctant to clarify their policies and practices in cyberspace, there is no consensus on how international law should apply to cyberspace, which has prompted some non-state actors to start filling this void. Private ICT companies and civil society organizations, in particular, have taken the lead in proposing human rights-based norms for regulating cyberspace to help create a safer, more secure, and more reliable internet.

A group of academics and experts in international humanitarian law produced the Tallinn Manual on the Application of International Humanitarian Law to Cyber Warfare.[33] Although it is an academic publication, the manual reaffirms the need to apply the basic principles of international humanitarian law – such as distinction, proportionality, and necessity – to cyberspace. This group of experts also published the Tallinn Manual 2.0, which examines how international law applies to cyberspace in peacetime.[34]

32 Group of 7, Charlevoix G7 summit communique, https://g7.gc.ca/en/official-documents/charlevoix-g7-summit-communique/.

33 Tallinn Manual, https://ccdcoe.org/tallinn-manual.html.

34 Tallinn Manual 2.0 Factsheet, https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf.

CASE STUDY: THE CONCEPTS OF 'ARMED ATTACK' AND 'USE OF FORCE' IN CYBERSPACE – BRIDGING THE LANGUAGE GAP BETWEEN THE LEGAL, POLITICAL, AND TECHNICAL COMMUNITIES

It is important to differentiate between the different regimes of international law: (i) ius ad bellum determines the circumstances under which a state may use force to implement its national policy, and (ii) ius in bello establishes the rules of international humanitarian law (IHL) governing the conduct of armed operations in conflict.

With regard to ius ad bellum, Article 51 of the UN Charter states that an armed attack may justify self-defence. Therefore, the key question is whether a cyber operation constitutes an armed attack that a state may legally retaliate against using cyber or kinetic force. The term 'armed attack' is important in this context; indeed, in the case of Nicaragua, the International Court of Justice held that there are 'measures which do not constitute an armed attack but may nevertheless involve a use of force'. Consequently, states may face a cyber operation that constitutes a use of force but may be unable to defend themselves legally if the cyber operation does not qualify as an armed attack. In order to address this dilemma, a number of international law scholars advocate expanding the concept of 'armed attack' in cyberspace to include any act with consequences similar to those caused by kinetic actions (physical consequences).

As far as ius in bello is concerned, IHL can only apply in the event of an attack, defined in relation to the consequences of the 'attack'.

In February 2017, Microsoft, a private transnational corporation, proposed that states adopt a 'Digital Geneva Convention', identifying norms in peacetime for cyberspace. Microsoft regularly publishes policy papers and blog posts that aim to build trust among various stakeholders in cyberspace. However, while states generally welcome initiatives by non-state actors, many remain sceptical about their prospect of success.[35]

At the same time, ICT companies are increasingly calling on states to regulate certain malicious behaviour in cyberspace. For instance, Microsoft urged the United States Congress to adopt regulations that would limit the use of facial recognition technology.[36]

Other soft-law instruments, such as the Manila Principles on Intermediary Liability,[37] have also been developed and provide guidance for states with respect to policies governing the legal liability of intermediaries for content posted on their platforms. Non-state actors, in particular ICT companies and civil society organizations, have also proposed norms applicable to cyberspace. Microsoft has been a forerunner in this area in recent years.[38]

35 Microsoft Policy Paper, A Digital Geneva Convention to protect cyberspace, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH; see also Microsoft cyber security guidelines, https://www.microsoft.com/en-us/cybersecurity/default.aspx.

36 Natasha Singer, The New York Times (13 July 2018): Microsoft Urges Congress to Regulate Use of Facial Recognition, https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html.

37 Manila Principles on Intermediary Liability, https://www.manilaprinciples.org/.

38 Microsoft policy paper, A Digital Geneva Convention to protect cyberspace, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace.

INFOBOX: PERSONAL DATA PROTECTION GUIDELINES FOR AFRICA

In May 2018, the Personal Data Protection Guidelines for Africa were launched by the Internet Society and the African Union Commission at the African Internet Summit in Dakar, Senegal.
The guidelines set out 18 recommendations centred around three issues:
Recommendations to create trust, privacy, and the responsible use of personal data.
Recommendations for actions to be taken by governments and policy-makers, data protection authorities, and data controllers and data processors.
Recommendations for multi-stakeholder solutions to ensure the well-being of 'digital' citizens and to adopt enabling and supportive measures.

(Source: https://www.internetsociety.org/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/)

INFOBOX: INTERMEDIARY LIABILITY

All communications involving the internet are facilitated by intermediaries. Given the complexity of the internet, there are a number of different types of intermediaries:
Internet service providers (ISPs) provide access to the internet.
Web hosting providers ('hosts') are individuals or companies who control websites or webpages that allows third parties to post and upload content.
Social media platforms, such as Facebook, Twitter, and YouTube, encourage individuals to connect and interact with other users and to share content.
Search engines, such as Google, are software programmes that use algorithms to retrieve data, files, or documents in response to a request for information.
Internet service providers, social networks, and search engines are therefore intermediaries. Intermediary liability refers to policies that govern the legal liability of intermediaries for the content of these communications.

(Source: https://www.manilaprinciples.org/ and https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf)

Civil society organizations have also launched initiatives to fill the legal vacuum left by states in cyberspace, proposing norms aimed at promoting human rights in cyberspace. For example, Article 19 – a London-based non-governmental organization (NGO) – along with a number of other NGOs, adopted the Camden Principles on Freedom of Expression and Equality.[39] In addition, soft-law instruments, such as the Manila Principles on Intermediary Liability, have been adopted as well.

The Global Network Initiative is a multi-stakeholder initiative that has developed global standards for the internet. Its Global Principles on Freedom of Expression and Privacy provide direction and guidance to the ICT industry and its stakeholders to ensure the promotion and protection of human rights around the world.[40]

Social media companies, namely Facebook, Twitter, YouTube, and Microsoft, came together to form the Global Internet Forum to Counter Terrorism,[41] a coalition to prevent violent extremism on the internet. As part of the initiative, these internet giants are developing normative standards to regulate violent extremism on their platforms.

Generally, private ICT companies should undertake effective, proactive, and inclusive human rights due diligence, including engaging meaningfully with individuals whose human rights may be affected by private ICT companies.

The Guiding Principles of Business and Human Rights (GPBHR) stipulate that companies have a responsibility to respect human rights. For ICT companies, this means taking into account issues specific to their sector, such as freedom of expression, privacy, and security. Importantly, some of the most pressing due diligence issues arise from the use of company products, service, technologies, and applications by users, as well as attempts by governments to restrict users' rights.

39 Article 19, The Camden Principles on Freedom of Expression and Equality, https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf.

40 More information regarding the Global Network Initiative is available at: https://globalnetworkinitiative.org/.

41 Google public policy, Update on the Global Internet Forum to Counter Terrorism (4 December 2017), https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/.

Key Findings

- When national legal frameworks fail to criminalize offences, these gaps can create safe havens for offenders, which may in turn impact other countries.
- Differences in the criminalization of offences in cyberspace pose challenges for international cooperation on issues related to cyber-crime, particularly regarding the concept of 'dual criminality'.
- A comparative analysis of cybercrime offences helps to identify good practices that states may adopt to develop national legislation in compliance with existing international standards in this area.

Resources

Many Possibilities. https://manypossibilities.net/african-undersea-cables/

Schmitt, Michael, N., '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', Exeter Centre for International Law (ECIL) Working Paper (2018), https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Schmitt_-_Virtual_Disenfranchisement_ECIL_WP_2018-3.pdf.

CHAPTER 4
IMPLEMENTING INTERNATIONAL AND REGIONAL NORMS AND STANDARDS AT THE NATIONAL LEVEL

OBJECTIVES

This chapter examines how the international and regional legal frameworks discussed in the previous chapter, as well as other norms within cyberspace, can be implemented at the national level, including through legislation, policies, and strategies.

THIS CHAPTER AIMS TO:

- increase understanding of the frameworks and other norms in cyberspace and how to implement them at the national level;
- increase understanding of the need for national legislation, policies, and strategies on cyberspace; and
- increase knowledge on how to develop or amend national legislation, policies, and strategies on cyberspace, based on good security sector governance (SSG) practices.

Introduction

Individuals, governments, and companies are increasingly using cyberspace, whether for accessing information, providing and receiving public and private services, or supporting operational processes. As a result, these actors are at greater risk of cyber-attacks and security breaches, which pose a threat not only to human rights, but also to national and human security.

At the regional and national level, a number of norms have been adopted to make cyberspace more secure and to establish a general framework outlining the legal obligations of states to protect human rights in cyberspace. There is now an increased focus on developing coherent and comprehensive national approaches to cyberspace challenges. The growing reliance on cyberspace has led to an increasing need for effective national legislation, policies, and strategies to protect the data, information, and knowledge transmitted and used in cyberspace, as well as to increase the security of citizens.

The previous chapter examined the international or regional frameworks – consisting of resolutions, reports, conventions, and agreements on human rights – that regulate cyberspace. These frameworks have established a set of norms for states to observe when amending their cyberspace and cybersecurity legislation, policies, and strategies, and can assist them in drafting or updating national policies and strategies on cyberspace and cybersecurity. In addition, private companies and nongovernmental organizations have sought to expand upon these frameworks and norms to elaborate on existing approaches to cybersecurity. States can draw on these various elements to establish a holistic approach to cyberspace and cybersecurity governance, based on the principles of good security sector governance (SSG).

The following good practices highlight key regulatory aspects states should address and strengthen when developing or amending their national cybersecurity strategies.[1]

National policies and strategies should also include an international dimension or be complemented by policies and strategies that focus specifically on international cooperation, so that the impacts of regulatory initiatives in the area of cybersecurity extend beyond national borders.

Good Practice 1: Governments should develop and adopt national laws, policies, and strategies to regulate cyberspace.

Although cyberspace is a global medium, the legal obligation of regulating it and ensuring its good governance falls on states as there is no international governance structure.[2] The principle that 'the same rights people have offline must also be protected online' also reflects this dynamic.[3] Thus, allowing information and communication technology (ICT) companies to operate without a sufficient regulatory framework can lead to practices that do not serve the public interest and potentially violate human

1 The good practices are based on: Microsoft, Cybersecurity Policy Framework: A Practical Guide to the Development of National Cybersecurity Policy (2018).

2 International Telecommunication Union (ITU), ITU National Cybersecurity Strategy Guide, p. 26.

3 United Nations Human Rights Council, Resolution on the promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012, para. 1.

rights.[4] It is therefore primarily the responsibility of the state, as the guardian of public interest, to ensure that human rights obligations are fulfilled. The state must also adopt legislative measures that take into account the latest technological advances, in order to limit the potentially harmful consequences of private sector actions. To ensure good governance practices, it is therefore essential to develop national legislation, policies, and strategies and to involve the security sector in efforts to regulate cyberspace and ensure cybersecurity.

Additionally, international and regional frameworks and norms are more general in nature, while national legislation, policies, and strategies can respond to specific cyberspace and cybersecurity needs at the national level.

Furthermore, the frameworks and norms established at the international and regional level constitute a set of mostly non-legally binding principles. There is therefore no guarantee that other states will abide by them, nor that private and public actors within a single state will observe the norms.[5] Last but not least, adopting or amending national cyberspace and cybersecurity legislation, policies, and strategies for cyberspace and cybersecurity governance can serve as a more comprehensive and coherent way in which to ensure respect for the law and human rights in cyberspace in the respective state.

Cybercrime legislation should be drafted with the following requirements in mind:

The legislation should be sufficiently neutral (in terms of technology) to be able to adapt to the constant evolution of technology and crime, thus avoiding the risk of becoming obsolete by the time it enters into force.

Law enforcement powers should be subjected to safeguards that ensure respect for the rule of law and human rights obligations.

The legislation should be sufficiently harmonized, or at least compatible, with laws of other countries to allow for international cooperation – for example, the criteria for dual criminality.

4 Mihr, Anja. 'Good Cyber Governance: The Human Rights and Multi-Stakeholder Approach', Georgetown Journal of International Affairs, (2014), pp. 24-34, http://www.jstor.org/stable/43773646.

5 Wolfgang Ischinger, 'Foreword' in International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World, Microsoft (2014), p. 1.

EXAMPLE OF GOOD PRACTICE

National legislation and policies are critical in the area of cybercrime. African states preparing legislation on cybercrime may draw on guidance, in particular, from the African Union Convention on Cyber Security and Personal Data Protection adopted in Malabo in June 2014.[6]

Since 1997, Algeria has progressively acquired the means to combat cybercrime. It has adopted legislation aimed at tackling crime in accordance with many fundamental principles, although challenges remain. Algerian law accommodates most of the provisions of the Budapest Convention adopted by the Council of Europe, with alternative wording in some cases. It includes the following offences: fraudulent access and retention of data in a system; the interception of communications and speech exchanged privately or confidentially; the deletion or modification of data held in the system as a result of fraudulent access or retention; the alteration of the functioning of a system as a result of fraudulent access or retention; the misuse of electronic devices; child pornography; and infringements related to intellectual property and related rights.

(Source: https://www.coe.int/en/web/octopus/)

Good Practice 2: Governments should update national legislation to take into account current cyberspace challenges.

When drafting, revising and adopting national legislation national cyberspace and cybersecurity legislation, legislators and policy-makers must take into account the ever-changing challenges that cyberspace poses.

Firstly, the pace of technological advances in cyberspace is much faster than national legislative processes. As a result, even the most up-to-date cyberspace legislation can – and likely will – lag behind the latest technologies. Secondly, cyberspace legislation requires substantial IT knowledge and expertise, which are rare in the public sector as they are much better rewarded in the private sphere. Thirdly, even if a state legislator manages to adopt relevant laws on the regulation of cyberspace, the transnational character of cyber-related issues makes the application of domestic laws complicated and sometimes impossible.

The speed of technological innovation contrasts sharply with the slow and often protracted nature of national legislative processes.[7] As a result, many technologies and cyber tools are used without the necessary regulation. The use of artificial intelligence (AI) is a noteworthy example of this regulatory vacuum. While the vast majority of states have failed to adopt appropriate legislation to regulate content hosted by social media companies that rely on individuals to moderate content, AI-powered tools are already being deployed to perform this task.[8]

6 African Union Commission and Symantec, Cyber Crime and Cyber Security Trends in Africa Report (2017), https://www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa.

7 European Court of Auditors, Challenges to effective EU cybersecurity policy – Briefing Paper, (2019), p. 18, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.

8 United Nations General Assembly, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/73/348, 29 August 2018, para. 18.

Nevertheless, states should avoid developing legislation in a hurried and uncoordinated manner. Public concern about the rapid pace of technological progress may serve as an incentive to adopt legislation in order to demonstrate the competence and responsiveness of state institutions. However, rushing to adopt laws may prove more damaging than temporarily allowing private companies to operate without comprehensive regulation while new technologies are being tested. For this reason, states should observe new technologies and identify new trends but legislate only after a careful review process encompassing all stakeholders, including the private sector and civil society.

Moreover, when developing legislation in this area, states should avoid being overly prescriptive. as this may impede innovation and research processes and discourage smaller ICT companies that may be unable to fulfil the high standards of overly prescriptive legislation. That said, when deciding whether to legislate on a specific cyber-related matter, states should consider options other than legislation. For example, the adoption of voluntary codes of conduct or a set of non-binding guiding principles may fulfil the regulatory objective. Also, such soft-law instruments are easier to amend and thus more able to reflect the latest technological trends.

EXAMPLES OF GOOD PRACTICE

Ghana has specific regulations for banking and financial institutions – the sector most affected by cybercrime. In 2008, state authorities adopted a Cyber Security Directive for financial institutions of the Bank of Ghana.

The directive requires each bank's senior executives and board to be actively involved in initiatives to strengthen cybersecurity. All banks in the country must appoint a Chief Information Security Officer (CISO) to advise senior management and the board on cybersecurity issues, and to propose appropriate measures to manage cyber and information security risks.

(Source: https://www.bog.gov.gh/privatecontent/Public_Notices/CYBER%20AND%20INFORMATION%20SECURITY%20DIRECTIVE.pdf)

Many African economies have strengthened their cybersecurity measures. In South Africa, the Protection of Personal Information (POPI) Act of 2013 created the Information Regulator to ensure data privacy. In 2017, this regulatory body launched an investigation into the country's biggest data breach of the year, in which the personal data of more than 30 million people was stolen. The agency also made formal requests to the concerned companies to provide explanations.

(Source: http://www.justice.gov.za/inforeg/)

Good Practice 3: Governments should enhance cyber expertise.

A lack of IT expertise and knowledge in the public sector is another serious obstacle for states in adopting legislation on cyber-related issues.[9] To solve this problem, states must find ways in which to strengthen their expertise in this area. This objective can be achieved in many ways; one of the most straightforward methods is for states to employ the necessary number of IT experts. However, states tend to have much more limited financial and other resources than private ICT companies and may face problems in recruiting and retaining experts on specialized issues such as cybersecurity, AI, or data analytics.

A partial solution is to use alternative regulatory schemes, which enable states to benefit from the expertise and involvement of the private sector without losing overall responsibility. Given that private companies have a high level of expertise and know-how on issues pertaining to cyberspace, this cooperation with the private sector may overcome the traditional gap between the advancement of technology and national legislation. Moreover, these co-regulatory arrangements can be much less politicized than traditional legislative processes.

EXAMPLES OF GOOD PRACTICE

In some countries, national cyber expertise has increased as a result of coordination with the private sector and foreign multinational companies.10

In Kenya, private sector cybersecurity initiatives led to the establishment of a Cyber Immersion Centre in Nairobi in March 2018 by Serianu, a Pan-African based cybersecurity and business consulting firm. The centre provides an environment for firms to experiment and test their cybersecurity capabilities. It also provides educational facilities to train cybersecurity professionals. A similar centre was opened in Mauritius in mid-2017.

(Source: https://www.serianu.com/acic.html)

In Nigeria, Microsoft teamed up with Paradigm Initiative Nigeria (PIN) to educate Nigerians on cybercrime and create economic opportunities. In October 2009, the country's Economic and Financial Crimes Commission (EFCC) announced that it had shut down around 800 websites associated with cybercrime and arrested 18 cybercrime gangs. The EFCC noted that it had relied on 'smart technology' that Microsoft provided.

(Source: https://paradigmhq.org/about/)

9 Raymond, Mark, 'Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot', Strategic Studies Quarterly, Vol 10: No. 4 (2016), pp. 137, http://www.jstor.org/stable/26271532.

10 Nir Kshetri, 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management, Vol. 22: Iss. 2 (2019), pp. 77-81, DOI: 10.1080/1097198X.2019.1603527.

Good Practice 4: Governments should develop and update laws protecting privacy and personal data.

The protection of privacy and personal data is an essential component of cybersecurity and concrete steps have been taken to ensure this is achieved, particularly in the EU. The EU's General Data Protection Regulation (GDPR – see Chapter 3), which came into effect in May 2018, created a regional regulatory regime to give individuals control over their personal data. This regulation has also spawned a number of privacy and data protection laws at the national level.

In 2014, the African Union adopted the Malabo Convention on cybersecurity and personal data protection (see Chapter 3); however, the convention has not yet entered into force. As such, the Budapest Convention is currently the only legally binding international legal framework on the topic of cybersecurity, cyberspace, and the state's role in the area. Although only a handful of African nations have signed it or been invited to ratify it, it has been used as a guiding framework for the creation of the African Union's Convention on Cybersecurity.

EXAMPLES OF GOOD PRACTICE

In Kenya, a new data protection bill was submitted for review by parliament in November 2018. The bill incorporates many elements of the EU's GDPR. For instance, the bill requires organizations to inform users about why and how the data will be used and for how long it will be stored. The bill also includes a provision giving consumers the right to request that organizations delete their data. In addition, these organizations must meet a number of security requirements in order to store data.

(Source: http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf)

France enacted the 'Loi relative à la protection des données personnelles' in June 2018 in order to bring French national legislation into compliance with the EU's GDPR. Building on the French Data Protection Act of January 1978, the 2018 law expands the mandate of the Commission national de l'informatique et des libertés (CNIL) regarding data protection, empowering CNIL in the following ways:

- It has increased regulatory powers to implement security regulations and codes of conduct and to develop reference documents and recommendations. Furthermore, the CNIL has the authority to approve certifying bodies as well as to certify products and persons, in accordance with the GDPR and French law.

- It has increased oversight powers, allowing CNIL agents to make requests for any documents not protected by legal privilege. Additionally, CNIL agents are allowed to use new types of sanction, and administrative fees have been raised significantly. If a company fails to protect personal data, it could face fines ranging from 10 million Euros or 2% of its global revenue to 20 million Euros or 4% of its global revenue (whichever is higher) for the most severe infractions.

(Source: https://www.francecompetences.fr/Protection-des-donnees-personnelles.html)

Good Practice 5: Governments should develop and update laws protecting critical infrastructure.

Critical information infrastructure (CII) plays a key role in ensuring the well-being of the general population. CIIs include physical and virtual assets, systems, and networks that are essential to fulfil vital social needs, including health, security, and economic and social well-being, and whose disruption or destruction would have a significant negative impact on the population.

Examples of critical infrastructure installations include:

- Power plants
- Water and food supplies
- Public safety, including security forces, emergency organizations, and civil defence
- Public health, including hospitals, medical care, and laboratories
- Public administration
- Transport, such as road, rail, and air transport
- Waste disposal (waste and wastewater)
- Financial services, such as banking and insurance companies
- Information and communication technology (ICT) networks

A significant proportion of CIIs rely on new technologies to support their operations. While this modernization has helped make this infrastructure more efficient in delivering services to the population, it has also exposed them to vulnerabilities that can have potentially devastating effects on local populations.

States have a duty to protect CIIs from cyber-attacks within their borders. Protecting CIIs from cyber-attacks should be a priority for states' cybersecurity strategies. To this end, states need to develop and implement cyber defence measures to tackle

vulnerabilities in CII systems. These measures must be able to detect, defend against, and neutralize cyber-attacks.

EXAMPLES OF GOOD PRACTICE

In March 2019, the South African parliament adopted CII legislation aimed at, among other things, enabling the identification and classification of infrastructure as critical infrastructure; providing guidelines to ensure the transparent identification and classification of critical infrastructure; and ensuring measures are put into place for the protection, safeguarding, and resilience of critical infrastructure. The legislation also establishes the Critical Infrastructure Council, gives the interior minister the authority to classify certain installations as critical infrastructure, and prescribes how these are protected in the interest of national security.

(Source: http://www.policesecretariat.gov.za/downloads/bills/CIP_Bill_for_Publication.pdf)

KEY FINDINGS

- International or regional frameworks provide a set of norms for developing, adopting, and amending cybersecurity legislation, policies, and strategies.
- Governments play a primary role in ensuring good cybersecurity governance.
- Governments should develop, adopt, and update national legislation, policies, and strategies to regulate cyberspace and respond to emerging challenges, including the protection of privacy and personal data and critical infrastructure.
- Increasing cyberspace expertise through education and knowledge sharing, particularly through public-private partnerships (PPPs), is essential to ensure good cybersecurity governance.

Resources

Venice Commission of the Council of Europe, The Rule of Law Checklist, (2016).

Microsoft, Cybersecurity Policy Framework. A Practical Guide to the Development of National Cybersecurity Policy (2018).

Microsoft, International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World (2014).

African Union Commission and Symantec, Cyber Crime and Cyber Security Trends in Africa Report (2017), https://www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa.

CHAPTER 5
NATIONAL CYBERSECURITY STRATEGIES

OBJECTIVES

This chapter provides readers with an introduction to national cybersecurity strategies (NCSSs). It aims to increase readers' knowledge of the main elements of NCSSs and share examples of good practices.

THIS CHAPTER AIMS TO:

- increase knowledge of national cybersecurity strategies;
- increase knowledge of the key elements of a national cybersecurity strategy; and
- increase awareness of resources available to support national legislators and policy-makers in developing national cybersecurity strategies.

Introduction

Since its advent, cyberspace has provided a variety of new opportunities for economic, technological, and social development. At the same time, transnational threats – such as state-sponsored cyber espionage, military cyber activities, cybercrime, cyberterrorism and terrorist use of the internet – have continued to grow. Since these security risks are linked to or facilitated by cyberspace, states must ensure they are adequately addressed through comprehensive strategies and action plans. Without these measures, states may find themselves unable to protect national and human security or to maintain economic growth.

In response to the ever-evolving threats that cyberspace poses, states around the world have developed and adapted strategies, either by adopting new national security policies or amending old ones. National security policies that address these threats are referred to as national cybersecurity strategies (NCSSs).

NCSSs take various forms, and their level of detail varies depending on the country's capacity to respond to cyber threats. Because these national strategies are context-specific, developing a blueprint for an effective NCSS is problematic. It is, however, possible to define a set of strategic priorities that can be applied to most NCSSs, including regulatory frameworks, the protection of critical infrastructure, international cooperation, and public-private collaboration, as well as research and development (R&D).

While there is no commonly agreed definition of an NCSS, the International Telecommunications Union (ITU) defines it as:

- an expression of the vision, high-level objectives, principles, and priorities that guide a country in addressing cyber threats;
- an overview of the stakeholders tasked with improving the country's cybersecurity and their respective roles and responsibilities; and
- a description of the steps, programmes, and initiatives that a country will undertake to protect its national cyber infrastructure and thereby increase its security and resilience.[1]

The scope of NCSSs has had to adapt to respond to rapidly changing cyber threats. As a result, the focus has shifted from protecting individuals and organizations to safeguarding society as a whole.

Broadly speaking, an NCSS has two interrelated objectives:

1. to strengthen cybersecurity to support the internet economy and foster economic and social prosperity; and
2. to protect cyber-reliant societies from cyber threats.

1 International Telecommunication Union (ITU), Guide to Developing a National Cybersecurity Strategy (2018), p. 13

Cybersecurity is a complex challenge, encompassing different governance, policy, operational, technical, and legal aspects. National policies generally define the methodology and goals for achieving national priorities.

Good Practice 1: The NCSS should be integrated into the wider national security policy.

NCSSs should serve as a tool to help states achieve their strategic national priorities. They should therefore form part of the state's broader security strategy, which in turn supports a comprehensive approach to national security.

Integrating cybersecurity into the national security strategy, and vice versa, underscores how both elements are interrelated. It also demonstrates that a government recognizes that cybersecurity forms a crucial part of all aspects of national security.

EXAMPLES OF GOOD PRACTICE

The Swedish NCSS states that it is 'based on the objectives for Sweden's security: protecting the lives and health of the population, the functioning of society, and our [Sweden's] capacity to uphold fundamental values such as democracy, the rule of law and human rights and freedoms'.

(Source: https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213)

Finland's NCSS is based on the principles and procedures established in its Cyber Security Strategy for society.

(Source: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf)

To develop a comprehensive NCSS, the country's vision and objectives should be translated into concrete actions that will ultimately contribute to achieving the identified goals and objectives.

The diagram below, developed by the ITU, outlines the lifecycle of an NCSS to guide those responsible for developing such strategies:

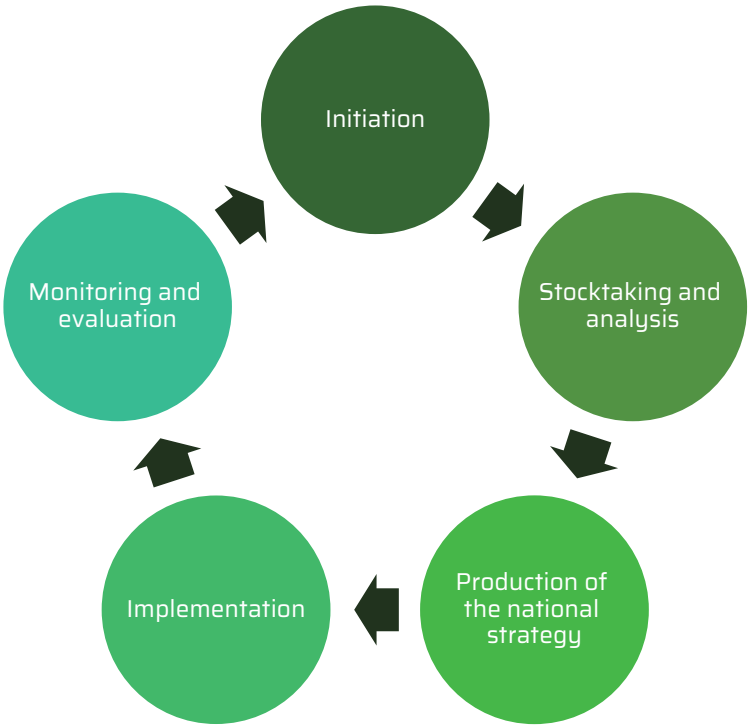


Figure 1: Lifecycle of an NCSS based on the ITU Guide to Developing a National Cybersecurity Strategy

Before developing an NCSS, state authorities should identify the strategy's objectives and purpose and clearly articulate its vision for cybersecurity.

CASE STUDY: OAS TECHNICAL ASSISTANCE MISSION TO MEXICO

In 2017, the Organization of American States (OAS) established – through its cybersecurity programme and at the request of the Government of Mexico – a commission of international experts to share best practices with Mexican entities and improve understanding of the current state of cybersecurity in Mexico; to identify the country's current level of cybersecurity maturity; and to support the development of a national cybersecurity framework. The commission included representatives from other states, the private sector, technical experts, international organizations, and civil society.

(Source: http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-049/17 and http://www.oas.org/documents/eng/press/Recommendations-for-the-Development-of-the-National-Cybersecurity-Strategy.pdf)

Good Practice 2: The development of an NCSS should be steered by an authority responsible for overseeing the process and should involve a wide range of stakeholders.

Beore developing an NCSS, an authority – whether a pre-existing entity or a newly established agency – should be idenitified as responsible for overseeing the NCSS process. Its responsiblilies should include coordinating the process in a neutral manner, identifying key stakeholders to be involved in the development of the NCSS, and ensuring ongoing exchange among stakeholders and engagement of those with relevant knowledge and expertise. This authority should also be responsible for clearly defining the roles and responsibilities of key stakeholders.

CASE STUDY: CHILEAN INTER-MINISTERIAL COMMITTEE

In Chile, an inter-ministerial committee composed of representatives from the Ministry of the Interior and Public Security and the Ministry of National Defence led the process of developing an NCSS.

This inter-ministerial committee organized and coordinated working group sessions to consider the following topics identified for the NCSS: information infrastructure; prevention and sanctions; education and awareness raising; cooperation and international relations; and institutionalization. The permanent members of these working groups included the under-secretariats for the ministries of the interior, defence, justice, economy, and telecommunications, as well as the Ministry Secretary General of the Presidency and the national intelligence agency.

(Source. http://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf)

Although the private sector plays a key role in ensuring cybersecurity, cooperation between the public and private sector is not always institutionalized.

As critical infrastructure is largely owned and operated by private entities, public-private cooperation is essential to ensure the protection of this infrastructure. These entities should therefore be actively involved in the development of strategies aimed at protecting national critical infrastructure against cyber threats.

As many stakeholders as possible should be involved in the process of developing an NCSS to promote ownership of the strategy – a key factor in ensuring effective implementation – and to benefit from relevant expertise.

EXAMPLES OF GOOD PRACTICE

To support the development of its NCSS, the United Kingdom launched an online open consultation process, allowing anyone to provide feedback on the strategy.

(Source: https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession)

The UK Cyber Security Strategy states that achieving the goal of a safe, secure internet depends on the cooperation of all relevant actors, including

the private sector, individuals, and government. Everyone benefits from the use of cyberspace, so everyone is responsible for helping protect it.

The Canadian government also undertook an online public consultation process to seek the views of citizens, the private sector, academia, and other informed stakeholders involved in cybersecurity in Canada. A report of this review process has been published and made available online.

(Source: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnsltns-rprt/index-en.aspx)

Although public-private partnerships are the most common form of institutionalized cooperation between the public and the private sector, challenges remain. These include the lack of clarity regarding the mandate of these partnerships and roles and responsibilities; mistrust among stakeholders; barriers to information sharing; the lack of incentives for collaboration; and a lack of effective oversight and therefore accountability.

Typical mechanisms to involve different stakeholders include committees, round-tables, workshops, expert interviews, and consultations.

CASE STUDY: IDENTIFYING RELEVANT STAKEHOLDERS

Not all stakeholders need to be involved in every discussion. It is, however, important to identify and engage those with relevant expertise or experience in a particular area.

Relevant stakeholders in the development of an NCSS include, but are not limited to:

- **Government:** relevant ministries (such as information, communication, and technology (ICT), economy, and communications), regulatory agencies, judiciary and law enforcement agencies, defence, and security services
- **Private sector:** ICT companies, information security companies, and businesses
- **Civil society:** interest-driven groups (such as human rights or child online protection), identity-based groups (faith, minority, women's rights), and civil society organization networks.
- **Academia:** universities, research entities, think tanks, and independent researchers
- **Technical community:** computer emergency response teams, computer security incident response teams, and domain name system standardization organizations
- **International Organizations:** regional and international organizations (such as the AU, OSCE, OAS, CoE) and international institutions (such as the World Bank and ITU)

(Source: https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf)

Good Practice 3: The development of an NCSS should identify and address the country's strengths and weaknesses in the context of cybersecurity.

The next phase in the development process involves assessing and analysing the country's cybersecurity landscape to identify strengths and weaknesses. As part of this stocktaking, the following should be identified and reviewed: national regulatory frameworks (including laws, regulations, policies, and programmes related to cybersecurity); national critical infrastructure; public-private partnerships; and the country's technical and institutional capacity to prevent cybersecurity risks (for example, through computer emergency response teams) and threats (for example, through data protection officers).

This stocktaking and analysis process assesses the country's level of cyber maturity to ensure the NCSS is tailored to its needs.

CASE STUDY: EVALUATING CYBER MATURITY, GHANAIAN MINISTRY OF COMMUNICATIONS

The Cyber Maturity Model was developed to support the review of Ghana's cybersecurity capacities by examining five areas:

- cybersecurity policy and strategy
- cyber culture and society
- cybersecurity education, training, and skills
- legal and regulatory frameworks
- standards, organizations, and technologies

The assessment aimed to enable the Ghanaian government to gain a better understanding of its strengths and weaknesses with regard to cybersecurity and to invest more effectively in capacity building.

(Source: https://moc.gov.gh/cybersecurity-capacity-maturity-model-assessment-held)

The designated authority should begin developing an NCSS – with significant support from key stakeholders – building on the results of the assessment. Ideally, working groups should be established to draft specific sections of the NCSS based on their area of expertise. It is also considered best practice to submit the draft NCSS to a diverse range of stakeholders for review, through an online consultation or workshop, before it is adopted – thus helping to ensure that it is based on a shared vision.

Depending on the country's regulations, either the parliament or the government is authorized to adopt an NCSS. The adopted NCSS should be published in an official journal or on a ministry's website to ensure the public is aware of the content and purpose of the strategy – as well as the government's priorities concerning cybersecurity – and can actively contribute to achieving its strategic priorities.

There is no single approach to managing the drafting process of an NCSS. Good practices will differ depending on the scope of the NCSS, the range of stakeholders involved, and the technical requirements in place.
In Chile, Kenya, and Mexico the draft version of the NCSS was also published online to allow different stakeholders to provide comments and to foster ownership.

Good Practice 4: The NCSS should include the following strategic priorities: enhanced governmental coordination at the policy and operational level, reinforced public-private cooperation, improved international cooperation, and respect for fundamental rights.

Most NCSSs underline the importance of international cooperation for promoting cybersecurity and the need to strengthen alliances and partnerships with like-minded countries, particularly to support capacity building. In addition, most NCSSs recognize that respect for fundamental rights, in particular the right to privacy and freedom of expression and opinion, as well as the free flow of information, are indispensable for a secure cyberspace.

In addition, the prevention of cybercrime is included as a strategic priority in the majority of NCSSs.

EXAMPLES OF GOOD PRACTICE

Canada's NCSS reflects Canadian values such as the rule of law, accountability, and privacy.

(Source: Canada National Cyber Security Strategy, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx)

Malawi's national information and communication technology strategy underlines the government's commitment to providing an enabling environment for both public and private sector participation in the development, deployment, and use of ICT in both urban and rural communities.

(Source: http://www.malawi.gov.mw/Publications/Malawi_2013_Malawi_ICT_Policy.pdf)

Good Practice 5: Critical national infrastructure should be identified and included in the NCSS.

Identifying critical national infrastructure – including a clear definition and list of what constitutes critical infrastructure – is essential for developing policies to protect them from cyber threats.

A growing number of critical infrastructures depend on information communication technology in order to operate and function. Protecting critical national infrastructure

from cyber threats is vital because these threats may have real-life consequences. Many states therefore include it as a priority in their NCSSs, and an increasing number identify their critical national infrastructure, especially water, electricity, and hospitals.

The EU Council's Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection constitutes an important document in this respect. In particular, the directive defines critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.

EXAMPLES OF GOOD PRACTICE

Article 17 of the South African Critical Infrastructure Protection Act lists several factors to consider when classifying a facility as critical infrastructure, including:

- the sector in which the infrastructure primarily functions;
- the strategic importance of the infrastructure – including the potential impact of the destruction, disruption, failure, or degradation of the infrastructure – or the interruption of a service that might affect the state's ability to function, deliver basic public services, or maintain law and order;
- the risk category of the infrastructure;
- the resources available to the person in control of the infrastructure;
- the impacts (or risk) of the destruction, disruption, failure, or degradation of the infrastructure;
- the size and location of any population at risk;
- historic incidents of destruction;
- the level of risk or threats to which the infrastructure is exposed;
- special characteristics or attributes of the infrastructure;
- the extent to which the classification of a facility as critical infrastructure will promote public interests; and
- and any other factors determined by the minister.

(Source: https://www.parliament.gov.za/storage/app/media/Docs/bill/8e3d69b4-509f-4108-b6ec-d0f44bb8632c.pdf)

Germany's strategy on national critical infrastructure (2009) defines critical infrastructure as 'organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences'.

(Source: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1)

France defines critical infrastructure as 'institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life. The operators themselves draw up the list of critical infrastructures, which may be production sites, control centres, network nodes or data centres.'

(Source: http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf)

Switzerland includes the following sectors as part of critical infrastructure: public administration, energy, waste disposal, finance, health, water and food, information and communication, transport, and public safety.

(Source: https://www.babs.admin.ch/en/aufgabenbabs/ski.html)

Good Practice 6: The NCSS should include an implementation plan, including research and development.

The success of an NCSS depends on its implementation. The NCSS must therefore be supported by an implementation plan (also referred to as action plan) to translate the strategy into concrete actions and policies, by coordinating efforts and resources.

Key indicators to monitor and evaluate the success of the NCSS also form an essential part of this plan, enabling state authorities to ensure that the NCSS is being implemented in accordance with its action plan. The evaluation phase provides the opportunity to ensure that implementation efforts correspond to the plan's objectives and priorities – and to amend these if not.[2]

In addition, the implementation plan should include the establishment of an incident reporting mechanism and procedures for raising awareness of cyber risks and threats. Cybersecurity incident reporting plays an essential role in enhancing cybersecurity at the national level. It also allows cybersecurity measures to be adjusted and tailored to respond to evolving threats. Incident reporting depends on cooperation between the public and private sectors. It is therefore essential to build trust to support open information sharing on cyber risks and threats. Establishing a computer security incident response team (CSIRT) is considered to be a key element in ensuring effective incident management.

For an implementation plan to be effective, awareness-raising initiatives need to improve individuals' knowledge of cybersecurity threats and vulnerabilities. Individual

2 ITU, Guide to Developing a National Cybersecurity Strategy (2018), p. 26.

users should learn how to protect themselves from security risks in cyberspace that may impact cybersecurity at the national level.

Investing in and fostering research and development is also essential for developing new tools for deterring, protecting, detecting, and adapting to all types of cyber threats.

EXAMPLES OF GOOD PRACTICE

Kenya's NCSS sets the following objective: 'The Government of Kenya is committed to safety, security, and prosperity of our nation and its partners. We see cybersecurity as a key component in that commitment, providing organizations and individuals with increased confidence in online and mobile transactions, encouraging greater foreign investment, and opening a broader set of trade opportunities within the global marketplace. Successful implementation of the strategy will further enable Kenya to achieve its economic and societal goals through a secure online environment for citizens, industry, and foreign partners to conduct business'.

(Source: Kenya, Cybersecurity Strategy, 2014, p. 4)

Nigeria's NCSS identifies the individual user as the weakest link in the cybersecurity chain. The strategy therefore proposes 'initiatives and measures that help safeguard general public internet users, provide materials and facilitate tools to help safeguard Nigerian citizens against cyber threats and unwholesome vulnerability'.

(Source: Nigeria, National Cyber Security Strategy, Chapter Eleven)

Malawi's National ICT Policy is accompanied by a detailed Implementation, Monitoring and Evaluation Strategy while the implementation of the policy is monitored and evaluated for effectiveness and responsiveness on an annual basis or when necessary.

(Source: Malawi, National ICT Policy, 2013, p 11)

Mauritania's NCSS includes a detailed implementation plan.

(Source: Mauritania, Stratégie Nationale de Modernisation de l'Administration et des TICs 2012-2016)

Poland's NCSS identifies increasing user awareness of safety measures and practices in cyberspace as a critical component of its strategy.

(Source: Poland, National Cyber Security Strategy, 2013)

Tunisia, South Africa, and Kenya have established computer emergency response teams (CERTs).

Good Practice 7: Well-resourced public awareness-raising campaigns should accompany the implementation of an NCSS.

Everyone connected to the internet – from government officials, business owners, and the financial and trading sector, to the general public and children – is vulnerable to cybersecurity threats.

Generally, it is commonly understood that no single agency, entity, or individual is responsible for cybersecurity. Instead, this responsibility is shared by everyone connected to the internet or using its applications.

According to the Organization of American States (OAS), 'cybercrimes are constituted by a vast range of different behaviours and techniques – including identify theft, child exploitation, cyberbullying, insider threats, phishing, spear phishing and many, many others – that needs to be addressed'.[3]

As anyone can be affected by various types of cybercrime, it is crucial to help the public understand risks and threats in cyberspace.

CASE STUDY: OAS CYBERSECURITY AWARENESS CAMPAIGN TOOLKIT – SITUATION ANALYSIS

In order to develop effective awareness-raising campaigns, it is essential to understand the context and background of cybersecurity threats.

OAS has developed some questions to help analyse the current situation:

- How connected is your country?
- Where and how are people connecting to the Internet?
- Who is online?
- With what kind of devices?
- What kinds of operating systems and communications channels?
- For what kinds of products and services?
- How is the Internet being used for business?
- What is the scale of these businesses (e.g. sole proprietorships, agriculture cooperation, small and medium enterprises, light manufacturing?)
- What are the cybersecurity risks is your country facing?
- What kinds of cybercrimes do your retail consumers face?
- What kinds of cybercrimes to your businesses face?
- Are these cybercrimes distinguishable by cohort?

3 OAS, Cybersecurity Awareness Campaign Toolkit (2015), p. 8, https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

- What are the risks to your critical infrastructure?
- Have there been major breaches – either governmental or commercial – in the recent past?
- Are there treats of major breaches in the future?
- What are the economic losses or potential from cyber threats?

Source: OAS, Cybersecurity Awareness Campaign Toolkit (2015) p. 26, https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf .

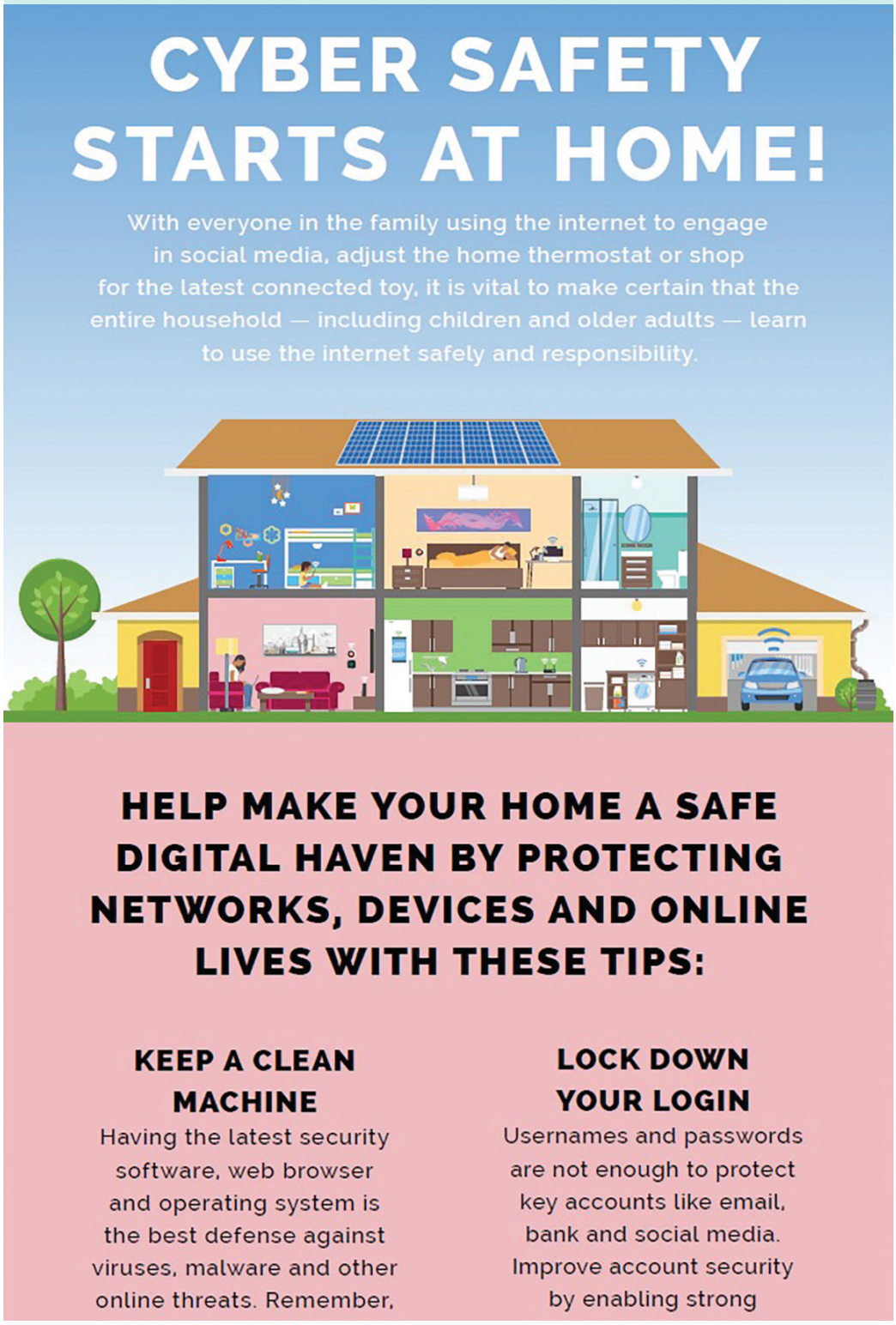
Successful awareness-raising campaigns convey messages that are easy to understand, targeted to a specific audience, and planned and developed through a multi-stakeholder process., It involves government officials, private companies, such as internet service providers and telecommunications companies, and civil society representatives, such as non-governmental organizations, the media, and academia.

EXAMPLES OF GOOD PRACTICE

In 2015, Jordan passed a law on combating cybercrime and established a specialized Cyber Crime Unit. The unit, with the support of the United Nations Office on Drugs and Crime, produced an awareness-raising video on the risks, types, and legal consequences of cybercrime.

Source: https://www.unodc.org/middleeastandnorthafrica/en/web-stories/jordan_-releasing-a-video-on-cyber-security-awareness-raising.html

In the United States, the National Cyber Security launched the StaySafeOnline initiative is powered by the National Cyber Security Alliance and seeks to promote a culture of cybersecurity. As part of the initiative, it published an infographic on its website on how to ensure all household members – including children and older adults – use the internet safely and responsibly.



Source: https://staysafeonline.org/wp-content/uploads/2018/09/NCSAM-2018-Week1.pdf

KEY FINDINGS

- States must continuously monitor and adapt their NCSSs to respond to current and emerging cybersecurity threats.
- Specific objectives and strategic priorities must be set to ensure the NCSS is implemented effectively.
- Cybersecurity strategies should recognize the importance of respect for fundamental rights, such as privacy and freedom of expression and belief, as well as the free flow of information, in promoting a free and open cyberspace.
- Cybersecurity issues involve a large number of different sectors and public agencies. The effective implementation of an NCSS therefore depends on close cooperation among governmental authorities, as well as with the private sector.
- Governments should invest more resources in research and development to develop new tools to deter, protect against, detect, and respond to new types of cyber threats.
- To protect critical national infrastructure from cyber threats, it is important to define what 'critical national infrastructure' means in a given context.

RESOURCES

International Telecommunication Union (ITU), Guide to Developing a National Cybersecurity Strategy (2018), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

EU Agency for Cybersecurity (ENISA), NCSS Good Practice Guide (2016), https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Microsoft, Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi.

Global Partners Digital, Multistakeholder Approaches to National Cybersecurity Strategy Development (June 2018), https://www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf.

Organization for American Scientists (OAS), Cybersecurity Awareness Campaign Toolkit (2015),

https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf.

CHAPTER 6
EFFECTIVE COOPERATION BETWEEN THE PUBLIC AND PRIVATE SECTOR IN CYBERSPACE

OBJECTIVES

This chapter provides an overview of the benefits and challenges of public-private partnerships in cyberspace, particularly in relation to law enforcement agencies and private companies investigating crimes and illegal content on the internet.

THIS CHAPTER AIMS TO:

- increase knowledge of the concepts of multi-stakeholder initiatives and public-private partnerships in cybersecurity;
- raise awareness of cooperation between law enforcement agencies and private companies; and
- improve understanding of the elements needed to develop effective multi-stakeholder approaches to cybersecurity.

Introduction

Owing to the cross-cutting nature of cybersecurity, all national cybersecurity strategies (NCSSs) seek to foster collaboration between public and private actors to enhance cybersecurity. Multi-stakeholder approaches to cyberspace and cybersecurity, also referred to as public-private partnerships (PPPs), play an increasingly critical role in cybersecurity governance, due to both the significant role of private companies and the transnational nature of cyberspace. Effective cooperation among stakeholders – notably governments, the ICT sector, academia, and civil society – is essential to fulfil international norms and standards and implement NCSSs effectively.

The increasing use of public, public-private, and private mechanisms to ensure cybersecurity is symptomatic of a more fundamental shift in international relations. Cooperation among various stakeholders – states, businesses, and civil society – can in this respect be seen as a pragmatic response to fill certain governance gaps that traditional regulatory approaches are no longer able to address. Indeed, such initiatives aim to support effective governance by ensuring commercial actors operate within a framework of the rule of law and respect for human rights. Multi-stakeholder groups can develop more effective approaches and solutions by working together rather than alone.

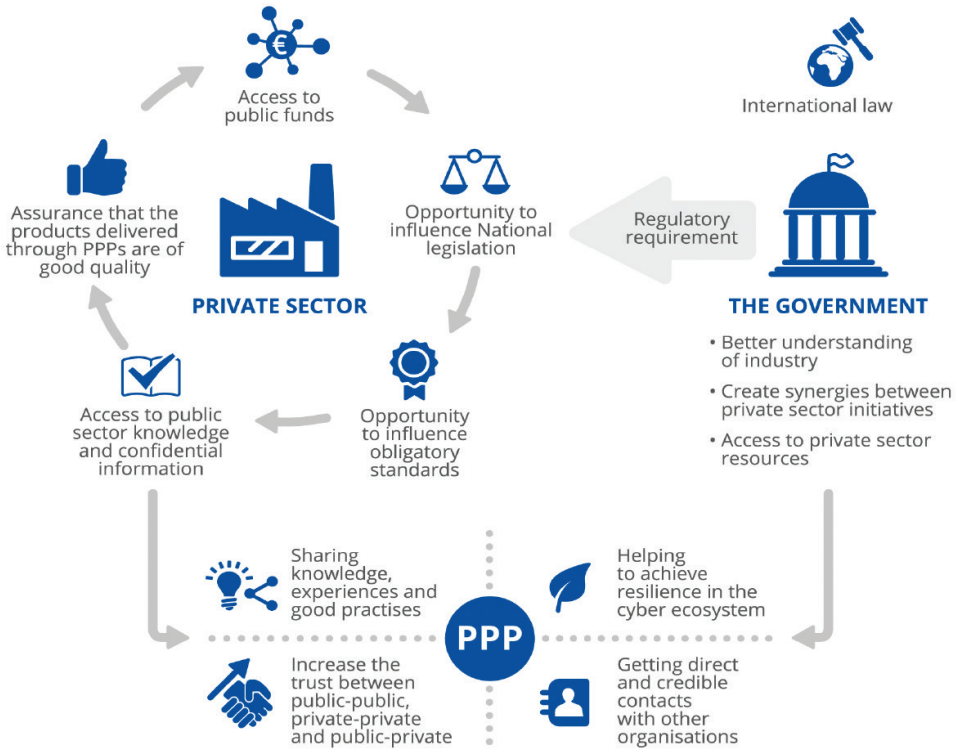
1. Understanding public-private partnerships

Overview

PPPs enable the sharing of resources (assets, skills, expertise, and financing), risks, and benefits among stakeholders. In the area of cybersecurity, PPPs involve collaboration between state authorities and public institutions on the one hand, and among ICT companies, academia, and civil society on the other, to raise awareness of cybersecurity, mitigate cybersecurity risks, and build national cybersecurity capacities. This cooperation is multifaceted and may include cyber defence capacity building and information sharing. Economic interests, regulatory requirements, and public relations may also be driving forces for PPPs. In developing countries, cybersecurity PPPs are primarily concerned with raising awareness of cybersecurity or building national cybersecurity capacities.

PPPs can strengthen cybersecurity in many ways, including by:

- raising awareness of cybersecurity in relevant organizations and throughout society;
- improving cyber skills at the national level through initiatives designed to identify, inspire, and enable more people to become cybersecurity experts;
- providing cybersecurity professionals with the required financial and technical resources through dedicated initiatives;
- strengthening research and development in the field of cybersecurity;
- reinforcing crime and fraud prevention measures;
- supporting cybersecurity certification and accreditation; and
- fostering collaboration between public and private entities involved in cybersecurity.



Reasons and incentives for public-private partnerships
Source: Public-Private Partnerships in Cyberspace, ENISA, November 2017, p. 14

Cybersecurity PPPs can be divided into four categories:

- **Institutional PPPs** are established under legislation related to the protection of critical infrastructure. This type of partnership usually operates through working groups, rapid-response groups, and long-term communities.

- **Goal-oriented PPPs** are created to build a cybersecurity culture through a platform or entity that brings the private and public sectors together to exchange knowledge and good practices. This type of partnership focuses on a specific subject or goal.

- **Outsourced cybersecurity services** are used when state authorities are unable to address effectively the private sector's needs. These PPPs act as an autonomous third party, but actively address the needs of businesses and support the government in policy-making or implementation.

- **Hybrid PPPs** mobilize computer emergency response teams (CERTs). State authorities assign these PPPs to provide CERT services to the government or to the country as a whole.

2. Roles of state authorities and other stakeholders

Public institutions play a key role in multi-stakeholder collaboration

The primary responsibility for the development of effective NCSSs lies with the state authorities. Legislators and policy-makers are therefore responsible for creating appropriate frameworks that meet the state's obligations under international and national legislation. State authorities engage with private actors, such as ICT companies, to ensure that co-regulatory and self-regulatory processes comply with international human rights law as well as national law.

Beyond this purely legalistic approach, governments can play an important role in coordinating and engaging the ICT sector and civil society by creating and supporting collaborative platforms. These are of particular relevance to national internet referral units, which search for and report suspicious online content and request its removal via referral processes with ICT companies. Collaborative platforms can provide valuable input to governments and contribute to fostering a more inclusive decision-making process. Open communication channels among relevant stakeholders also help to identify and fill critical gaps in cybersecurity, and to prevent potential conflicts of interest. Institutionalized and coordinated efforts can also promote complementary actions by various stakeholders and help to channel human and financial resources more effectively.

CASE STUDY: COMPUTER EMERGENCY RESPONSE TEAMS

Computer emergency response teams (CERTs) are groups of experts responsible for providing assistance to individuals or institutions that fall victim to a cyber-attack. Their primary function is to identify hostile malware and prevent it from spreading further in the network, while mitigating the impact of the attack. These units are often incorporated within private companies or public institutions but may also exist as government agencies at the national level specifically tasked with assisting a wide range of private and public entities.

Although national CERTs are public agencies, they represent a good example of public-private cooperation. CERTs are tasked primarily with gathering information about recently discovered cyber vulnerabilities, including relevant software updates and patches. Most national CERTs can be notified about cyber risks or cyber incidents via an online form. Some national CERTs also offer mobile teams that can be dispatched to an institution requiring assistance in the event of a cyber-attack.

Cooperation between the private and public sectors is essential for maintaining a stable and secure cyberspace. Public institutions cannot secure cyberspace on their own for two main reasons. Firstly, the private sector drives innovation in the field and controls the majority of cyberspace.

Secondly, even state-owned and state-controlled critical cyber infrastructure relies heavily on products and services provided by private companies for their protection.

Moreover, governments are obligated to respect and protect the human rights of their citizens online and must therefore ensure that the actions of private companies and national CERTs do not violate human rights, especially the right to privacy and freedom of expression. CERTs should therefore operate independently – without political interference – and should not be used by governments to access computer systems, networks, or communications to undermine privacy.

When establishing national CERTs, governments should consider the three human dimensions of cybersecurity: confidentiality, accessibility, and integrity. The fundamental goal of cybersecurity is therefore not to secure networks but to enhance human security. Consequently, the right to privacy must be one of the guiding principles of efforts to protect and enhance data privacy. To ensure the accessibility of data, it is essential that freedom of expression and information is respected and protected.

(Source: https://www.africacert.org/african-csirts/)

CASE STUDY: EU AND NATIONAL INTERNET REFERRAL UNITS

The European Union Internet Referral Unit (EU IRU) forms part of EUROPOL's European Counter Terrorism Centre and comprises a team of experts in religiously inspired terrorism, translators, information and communication technology (ICT) developers, and law enforcement agencies specialized in counter terrorism.[1] It started its work in 2015 and has the following mandate:

- to support the relevant EU authorities by providing strategic and operational analysis;
- to flag terrorist and violent extremist online content and share it with relevant partners;
- to detect and request the removal of internet content used by smuggling networks to attract migrants and refugees; and
- to swiftly carry out and support the referral process, in close co-operation with the industry.[2]

According to the EU IRU's Transparency Report in 2017, 'cooperation with the private sector is fundamental in prevention'.[3] From its establishment in July 2015 through December 2017, the EU IRU assessed 46,392 items with terrorist content, which led to the referral of 44,807 decisions with a content removal rate of 92%.[4]

1 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
2 https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru
3 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017
4 https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-transparency-report-2017

As stated in the transparency report and in the EU IRU's mandate, the IRU is responsible for assessing online content and referring it to the relevant ICT company for removal. As such, the EU IRU focuses on content published by Al-Qaeda and Daesh and affiliated groups and assesses this content according to the Europol's mandate and the principles set out in the EU Directive on combating terrorism. The EU Directive on combating terrorism provides safeguards for the removal of content, as specified in Article 21 (3):

'Measures of removal and blocking must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.'[5]

If the assessed content falls under Europol's mandate, it is referred to the ICT company hosting the content. Nevertheless, the decision on whether to delete the content is left to the discretion of the company, which assesses it according to its own terms of service. The EU IRU has no legal power to remove content.

Similar referral units exist in the United Kingdom, France, and the Netherlands; Europol has reported that parallel mechanisms have also been established in Belgium, Germany, and Italy.[6]

In addition, the EU IRU organizes joint Referral Action Days with ICT companies such as Google, Twitter, and Telegram. These events bring together specialized law enforcement units from multiple national IRUs as well as representatives from the EU IRU and ICT companies. Law enforcement specialists assess several hundred cases of potential terrorist content on a specific platform and aim to detect patterns in the use of the platform by terrorist and violent extremist groups. The findings are then shared with the ICT companies in attendance, which review the detected content against their own terms and conditions. The final decision to remove the content detected lies with the company. The joint Referral Action Days promote a coordinated approach between governments and ICT companies to combat violent extremist and terrorist content online.[7]

Initiatives led by ICT companies and civil society

ICT companies often face challenges in co-regulating and self-regulating their platforms, particularly with regards to protecting human rights, such as freedom of expression and the right to privacy. These challenges are exacerbated by the fact that social media platforms have become essential tools for discussing, sharing, and accessing information. To address these challenges and strengthen cybersecurity, ICT companies have developed initiatives to promote knowledge and technology sharing among companies; to create platforms that facilitate the development of resources and interactive tools to regulate content; and to conduct training sessions for small companies, led by large companies, on how to remove content.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN

6 See https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

7 See https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-google-take-terrorist-propaganda-in-latest-europol-referral-action-days; https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram

CASE STUDY: INHOPE

Active in 43 countries, the International Association of Internet Hotlines (INHOPE) aims to contribute to an internet that is 'free of child sexual abuse and exploitation'.[8] Its mission is to 'strengthen the international efforts to combat child sexual abuse material'.[9] INHOPE partners with a variety of stakeholders, including Interpol, Europol, Twitter, Crisp, Microsoft, Google, Facebook, and Trend MICRO.

INHOPE has 48 hotlines that allow the public to report content or activity online that is suspected to be illegal. INHOPE divides illegal activities into two categories: criminally illegal activities that are investigated and prosecuted by law enforcement agencies – the focus of INHOPE's work – and civil illegal activities that can be prosecuted by civilian bodies.

INHOPE's primary focus is child sexual abuse material, including online grooming, but it also addresses hate speech and xenophobic content online. While INHOPE provides a definition for hate speech, it also acknowledges that hate speech is an 'extremely complex' issue and that the dissemination of hate speech is often not illegal under criminal law. Therefore, when hate speech is reported to a hotline, it is assessed according to national legislation (that is, the legislation applicable where the content is hosted).[10]

Content reported anonymously is reviewed by a hotline content analyst to assess whether the material is illegal. If the hotline content analyst considers the content illegal, the location of this content is traced. If the content is hosted in the same country, the material is reported to national law enforcement agencies and/or the ICT company for removal. If the material is hosted in a foreign country, it is transferred to the hotline in the relevant country.

INHOPE has also developed a code of practice for internet service providers stating that INHOPE members should regularly consult major stakeholders, including governments, law enforcement agencies, ICT companies, and child protection institutions, and that members should apply the principles of transparency, accountability, responsibility, and trustworthiness to their work.

INHOPE also emphasizes the importance of staff well-being for those who are responsible for reviewing reported content and acknowledges that assessing content concerning child sexual abuse, violent extremism, or terrorism can have a psychological impact on reviewers.

Point de Contact, the internet crime reporting platform in France, has developed and published a white paper that identifies a shared set of best practices for the operational handling and processing of harmful and potentially illegal content, which may endanger the physical safety and psychological well-being of professional content reviewers.[11]

8 http://88.208.218.79/gns/home.aspx
9 http://88.208.218.79/gns/who-we-are/our-mission.aspx
10 http://88.208.218.79/gns/internet-concerns/overview-of-the-problem/hate-speech.aspx
11 http://88.208.218.79/Libraries/External_reports_Library/White_Paper__PointdeContact.sflb.ashx

3. Creating cybersecurity PPPs

Good Practice 1: It is crucial to create an enabling environment for PPPs.

Establishing an enabling environment is critical for the creation of effective PPPs. This process should include four key areas: policy formulation, a legal and regulatory framework, institutional arrangements, and financial support and investment. The EU Guidelines also stress the importance of flexibility and transparency from all partners involved, as well as mutual recognition of the needs and objectives of the various stakeholders.[12]

To create an enabling environment, stakeholders should agree on the legal basis of the PPP. Public institutions should take the lead in creating PPPs or national action plans and be allocated adequate resources for internal coordination and collaboration processes. A pragmatic approach should be adopted to resolve challenges related to coordination or collaboration. It is also important to encourage private sector participation, particularly small and medium sized enterprises, both to ensure an enabling environment and to promote cooperation and collaboration among relevant stakeholders. Finally, PPP stakeholders should communicate openly with the wider public.

Good Practice 2: Clear lines of responsibility and accountability should be established to protect human rights.

Establishing clear lines of responsibility and accountability for all stakeholders is essential, particularly to prevent human rights violations. PPPs, especially those created to implement national cybersecurity strategies (NCSSs), can face numerous challenges, including the reluctance of politicians to take responsibility for stricter cybersecurity legislation and the unwillingness of the private sector to accept responsibility or liability for national security. These partnerships may therefore lack clear lines of responsibility and accountability, which form an integral part of PPP agreements since they mitigate risks and ensure that all stakeholders understand their roles and responsibilities.

Good Practice 3: Trust among stakeholders must be established and maintained.

Building and maintaining trust between public and private entities is one of the biggest challenges for PPPs. This is an ongoing process that is culturally specific and involves personal relations. Trust cannot be achieved without an enabling environment. Other challenges include the lack of human resources in both the public and private sector; insufficient funds and resources for the public sector, which fail to meet the expectations of the private sector; and a lack of understanding and dialogue between the public and private sector regarding the concept of PPPs.

12 EU Guidelines https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

Public agencies and private entities need to build trust by adhering to the principles of openness, fairness, and mutual respect. Information sharing among partners is therefore an important measure of trust. Participants need to feel they are gaining access to information by being a part of a particular partnership, but also that their data is safe and secure.

CASE STUDY: GLOBAL FORUM ON CYBER EXPERTISE

The Global Forum on Cyber Expertise (GFCE) is a platform for states, international organizations, and private companies to exchange best practices and expertise on cyber capacity building.

Launched in April 2015, the GFCE's primary objective is to provide a dedicated, informal forum for policy-makers, practitioners, and experts from different countries and regions to facilitate the sharing of experiences, expertise, and assessments on key regional and thematic issues related to cyberspace. Since its launch, the GFCE's focus has shifted to coordination. Capacity-building activities and training initially focused on cybersecurity, cybercrime, data protection, and e-governance. In 2019, the GFCE led efforts to facilitate and coordinate knowledge and expertise sharing aimed at strengthening cyber capacity building. The various GFCE working groups are also working to establish a clearinghouse mechanism.

Source: Global Forum on Cyber Expertise (GFCE), 'History of the GFCE'

KEY FINDINGS

- In the field of cyberspace and cybersecurity, collaboration among groups composed of diverse stakeholders is often more effective than individual initiatives. Multi-stakeholder approaches, also referred to as PPPs, can jointly develop more effective processes and solutions, and are playing an increasingly vital role in governing cyberspace and addressing cybersecurity issues.
- PPPs are structured around collaborative agreements between public and private institutions.
- Governments can play an important role in coordinating and engaging with the ICT sector and civil society by creating and supporting collaborative platforms.
- Private actors such as the ICT industry can also lead effective multi-stakeholder cybersecurity initiatives.
- Governments should adopt a pragmatic approach to building PPPs that promotes open communication, inclusive participation, and increased private sector participation.

RESOURCES

EU Agency for Cybersecurity (ENISA), Public-Private Partnerships in Cyberspace (November 2017), https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport.

Carr, Madeline, Public–Private Partnerships in National Cyber-security Strategies (2016), https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

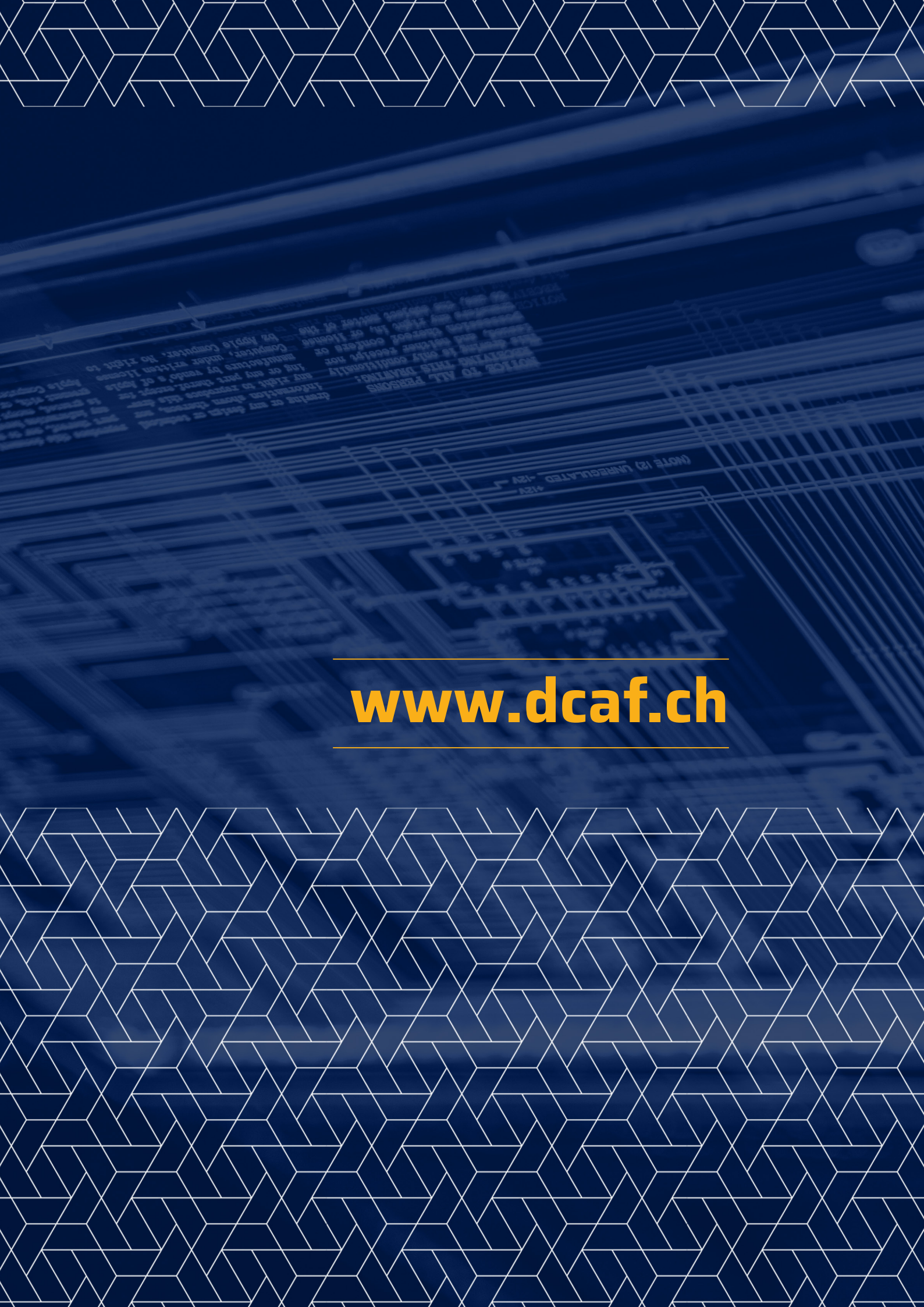
US National Council for Public-Private Partnerships, 'Definition of PPPs' (2016).

European Court of Auditors, Public Private Partnerships in the EU: Widespread Shortcomings and Limited Benefits (2018),

http://publications.europa.eu/webpub/eca/special-reports/ppp-9-2018/en/.

AfricaCERT, https://www.africacert.org/african-csirts/.

EU Internet Referral Unit (IRU), https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.



www.dcaf.ch