Foreign, Commonwealth & Development Office

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

Contents

INTRODUCTION		4
CHAPTER 1	INTRODUCING GOOD SECURITY SECTOR GOVERNANCE	5
CHAPTER 2	HOW DO CYBERSPACE AND CYBERSECURITY RELATE TO GOOD SECURITY SECTOR GOVERNANCE	25
CHAPTER 3	INTERNATIONAL AND REGIONAL LEGAL FRAMEWORKS IN CYBERSPACE	39
CHAPTER 4	IMPLEMENTING INTERNATIONAL AND REGIONAL NORMS AND STANDARDS IN A NATIONAL CONTEXT	57
CHAPTER 5	NATIONAL CYBER SECURITY STRATEGIES	69
CHAPTER 6	EFFECTIVE COOPERATION BETWEEN THE PUBLIC AND PRIVATE SECTOR IN CYBERSPACE	87

General 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. 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 have to come together to address the challenges of cybersecurity governance. In addition, legal and policy frameworks will have to adapt to better respect and implement international human rights norms, while effectively combating cybercrime, cyber malicious acts, cyber attacks as well as the use of the Internet for terrorist purposes and the promotion of violent extremism. Only vigorous action in this direction will promote a secure, stable and open cyberspace.

It is in this context that the Security and Defense Cooperation Directorate (DCSD) of the French Ministry for Europe and Foreign Affairs and the Center for Security Sector Governance, Geneva (DCAF) launched in 2018 the drafting of this guide to good practices for the promotion of good governance in cyberspace. In 2020, this guide was translated into Serbian, Albanian, Macedonian and English languages 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.

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

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

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

CHAPTER 1
INTRODUCING GOOD SECURITY SECTOR GOVERNANCE

OBJECTIVES

This chapter seeks to increase users' knowledge and understanding of key terms regarding good security sector governance; with a view to situating them within the context of cyberspace. To this end, this chapter aims at focusing on three essential components of security sector good governance pertinent to cyberspace as well:

- a. Accountability,
- b. Transparency, and
- c. Rule of law.

Following the introduction of these concepts, specific challenges pertaining to promotion of good governance principles in cyberspace will be presented supported by identified good practices.

Learning objectives of this chapter are the following:

- Increased awareness of key terms and definitions with regard to governance, security sector governance, and good security sector governance.
- Increased understanding of the underlying concept of good governance principles, such as accountability, transparency, and rule of law.
- Increased knowledge of underlying security sector good governance principles.
- Increased understanding of the importance of promotion of good governance principles in cyberspace.

1. Introduction

Governance, Security Sector Governance, and Good Security Sector Governance

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

Security sector governance (SSG) is defined as '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 norms or values.

> Good Security Sector Governance focuses specifically on **applying the principles of good governance** to security provision, management and oversight in a national setting.

The concept of good SSG describes how 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 same high standards of public service delivery as other public sector service providers. Therefore, a security sector that fails to comply with these standards might challenge political, economic and social stability in a national context (also described as 'poor SSG').

1 DCAF Security Sector Reform Backgrounder (cf. Resources).
2 Ibid.

What is the security sector?

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

Therefore, a security sector is not necessarily limited to a State as the only provider of security and justice. People themselves often provide security and justice in their own homes and communities, regardless of whether the State acts to meet these needs or not. Notably, people can organise themselves and provide security in various ways, including neighbourhood watches, women's groups or commercial security provision.

Furthermore, customary roles of important community figures in security and justice decision-making, alternative dispute resolution mechanisms, traditions and informal rules can shape security and justice provision within a community. Consequently, these community groups are also part of the security and justice sector in its wider sense.

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

- - Security providers, such as the armed forces, police, border guards, intelligence services, penal and corrections institutions and commercial and non-state security actors;
- - Security management and oversight bodies, such as government ministries, parliament, special statutory oversight institutions, parts of the justice sector and civil society actors with a stake in high standards of public security provision, including women's organisations and the media.

Importantly, security sector reform (SSR) is based on a broader understanding of the security sector. SSR is a process with the ultimate aim to achieve good governance of the security sector promoting human and state security.

Source: DCAF SSR Backgrounder, Security Sector (cf. Resources)

3 Ibid.

Non-state security and justice providers are included in a broader definition of security sector due to their direct effect on security sector governance. In last two decades, private security providers have been increasingly deployed to provision of security and services protecting people and the property. In particular, private military and security companies operating on commercial basis have become a major security actor.

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, 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]

Security sector reform (SSR) is a political and technical process of improving human and state security by making security provisions, management and oversight more effective and accountable within a framework of democratic civilian control, rule of law and respect for human rights.[5]

Good Practice: To recognise that individuals and communities have different security needs, including the ones in cyberspace

Every person present in cyberspace has individual security needs. In cyberspace, women and girls are disproportionately affected by bigotry, hate and misogynist speech. Recognising this and consequently providing effective mechanisms to report incidents and initiate criminal investigations can contribute to increased security of affected vulnerable groups.

4 Ibid.

5 DCAF SSR Backgrounder, p 2 available at https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

EXAMPLES OF GOOD PRACTICE

Benin has launched an annual cyber security campaign as part of its national effort to raise cyber security awareness across the country. The campaign focuses on the country's youth and is to be codified by the national cyber security strategy document.

As part of the no hate speech movement, the Council of Europe Members States launched national campaigns as well as national reporting bodies to introduce national reporting procedures and mechanisms for hate speech, hate crime and cyberbullying.

In Austria, the Ministry of Interior runs a reporting mechanism for violent extremist and radical videos in order to keep platforms safe from hateful speech.

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

The Ukrainian police established a point of contact to report cases of cyberbullying and hate speech and allow affected individuals to file a complaint.

(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 (Ecole Nationale en Cybersécurité à Vocation Régionale - ENVR) was set up with the French backing in November 2018 to strengthen West Africa's defences against computer hackers and use of Internet for terror funding and propaganda. This school will provide training for the security services, judiciary and private enterprises on combating cyber-crime, 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) -Ministarstvo za Evropu i spoljne poslove Francuske)

2. Good Security Sector Governance in Cyberspace

What is good security sector governance?

Good SSG is all about applying principles of good governance to security provision, management and oversight in a national setting. Seven main principles of good governance have been listed as follows:

- **Accountability**: there are clear expectations from security providers, and independent authorities oversee whether these expectations are met and impose sanctions if they are 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:** all women and men of all backgrounds have the opportunity to participate in decision-making process and service provision on a free, equitable and inclusive basis, either directly or through legitimate representative institutions.
- **Responsiveness:** institutions are sensitive to different security needs of all parts of the population and fulfil their mandates in the spirit of culture of service.
- **Effectiveness:** institutions fulfil their respective roles, responsibilities and missions up to a high professional standard.
- **Efficiency:** institutions make the best possible use of public resources in fulfilling their respective roles, responsibilities and missions.

Applying good governance principles in cyberspace

Had cyberspace been a country, it would have been the biggest and the most populous one in the world. However, it would neither have a legislative or other representative decision-making body, nor there would be a designated law enforcement mechanism or a mechanism to protect human rights of its citizens since there is no entity exercising exclusive authority and control over the entire digital space.[6]

Quite the opposite, governance of cyberspace is characterised by a multitude of diverse actors with different roles and responsibilities influencing policy decisions and regulatory deliberations.

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

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

This coupled with a lack of knowledge on how to effectively implement good governance principles in cyberspace can result in poor governance, making the security sector generally ineffective in supporting human and state security. The following sections take a closer look at three key good governance principles: accountability, transparency and the rule of law.

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

CASE STUDY: PROGRAM NADZORA AMERIČKE DRŽAVNE BEZBEDNOSNE AGENCIJE

In 2013, Edward Snowden, CIA employee, leaked top-secret documents that revealed that US and UK intelligence agencies had been operating mass surveillance programmes worldwide, including but not limited to interception of Internet and telephone traffic passing through undersea fibre optic cables, collection of data from Google and Yahoo user accounts and cell phone records, spying on foreign governments, hacking and infecting computers with malware.

Notably, companies received disclosed orders under the US Foreign Intelligence Surveillance Court (FISA) to hand-in their customers' data. Moreover, vast intelligence-sharing practices between members of the 'Five-Eyes Alliance' and other countries were uncovered. Although former President Obama responded with reforming the NSA's surveillance programmes and the FISA Court to increase transparency, the US Congress is still at an impasse to establish a system that would ensure critical protection for privacy, while preserving investigative capabilities.

(Source: ACLU, available at https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance?redirect=nsa-surveillance i https://www.aclu.org/blog/national-security/nsa-legislation-leaks-began?redirect=NSAreform)

2.1. Developing norms and institutions contributing to and strengthening accountability of the security sector in cyberspace.

Democratic and civilian control is a must for effective accountability. It can be exercised by national parliaments as well as more generally by civil society. This form of oversight is essential to ensure accountability of the security sector. In cyberspace, however, democratic and civilian control of the security sector is often undermined due to a number of reasons.

Democratic oversight quite often faces the following obstacles:[7]

- **Complexity of the online network**

Firstly, oversight challenges derive from the network complexity. A large and diverse number of States, private, international and other non-state actors take part in cyber security. Similarly, a diverse group of actors participate in what we might broadly term 'cyber attacks'. Technical complexity of the network makes it difficult for oversight bodies, such as parliamentary committees – often with limited capacity – to keep track of relevant actors, gain knowledge of their existence and activities or even acquire a legal mandate to do so.

- **Technical knowledge required to draft and implement effective regulation**

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

Secondly, oversight challenges are exacerbated by highly technical nature of cyberspace. As a result, oversight bodies such as parliaments often lack the required expertise to adequately understand and consequently draft legislation that can effectively regulate activities in cyberspace. Public-private cooperation can be further complicated by the division between highly paid and sophisticated technical experts involved in developing and implementing effective regulation on one side and often poorly paid and less well-informed government actors charged with their oversight on the other.

- **Legal complexities vested in cyberspace, such as jurisdiction and attribution**

Thirdly, oversight challenges are exacerbated by legal complexities as well. Interconnected, "borderless" nature of cyberspace brings about real challenges to traditional territorial law enforcement framework. Data and cyber activities can shift from servers located in one jurisdiction to those in another at the speed of light. Furthermore, while it is often said that the same laws offline should apply to activities online, it is frequently not clear what this actually means in practice. Cyber security poses complex legal questions related, among others, to right to privacy and freedom of expression. This complexity is further on magnified by public private cooperation and associated legal questions pertaining to responsibility and control.

- **Diverse nature of actors involved confounding traditional lines of responsibility and oversight**

Fourthly, oversight challenges are exacerbated by diverse nature of actors involved. In most instances, national oversight institutions are organised along agency or functional lines. For example, a parliamentary committee may oversee intelligence services, the armed forces, or justice institutions. Public private cooperation involved in cyber security, however, cuts across agency boundaries, areas of expertise and oversight mandate. The result is a large number of areas with inadequate or no oversight.

When it comes to breaking of responsibility lines and control, actions of every single government agency are intertwined in a chain of responsibility. For example, a Paris police officer is linked up his or her hierarchy to the police prefect (politically appointed head of the force) and ultimately, to the Interior Ministry and the executive. There is thus a mix of responsibilities and oversight among institutions of democratic governance (such as the parliament) and individuals or agencies carrying out government directives. These links can be severed by the introduction of private actors and 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 informational asymmetries reducing transparency and preventing oversight mechanisms from operating effectively.

- **Understanding mandate by an oversight body itself**

In general, government oversight bodies deal with government agencies they have direct responsibility over. This can leave private partners of such agencies out of the oversight reach, even in cases when they are directly funded by, or work in close collaboration with those agencies.

CASE STUDY: GERMAN BUNDESTAG, ENQUIRY 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 lobby to regulate surveillance technologies that harm human rights.

(Source: EDRi Protecting Digital Freedom, available at: https://edri.org/germany-exports-surveillance-technologies-to-human-rights-violators/)

Technical complexity of cyberspace further exacerbates traditional difficulties faced by parliamentarians in overseeing the security sector, which may undermine effective accountability. This coupled with the difficulty to reliably attribute violations of law in cyberspace to an actual actor, can make it difficult if not even impossible for civilian authorities to hold the security sector accountable, thereby contributing to the culture of impunity.

The justice sector plays a pivotal role in overseeing actions by the security sector. For example, the justice sector may vest special powers in law enforcement and intelligence service agencies by issuing search warrants. This can be particularly relevant in the context of communication interception. However, judicial control is often circumvented or limited for reasons of national security and state of emergency.

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

The Swedish parliament has fifteen committees. The roles of these parliamentary committees are various. They can, for example, conduct public hearings to gain knowledge on specific issues they would have to legislate. While it is unclear which parliamentary committee is solely tasked with overseeing cyber security governance, it is likely that various committees have a role depending on the context. For instance, the Committee on Defence may be tasked with issues related to cyber security.

Sweden's national cyber security strategy 2016 addresses a whole range of subjects; from regulation of ICT providers to critical infrastructure protection. However, it seems that there are no committees or sub-committees specifically tasked with cyber security. Such an issue very often implies cross-government responses and it seems it is the case in Sweden. This may be further complicated by the fact that important part of cyber protection is ensured by private actors and parliamentary committees do not have an adequate mandate to scrutinise such activity. Nevertheless, unlike several national cyber security strategies, the Swedish strategy sets up strategic principles and an action plan, which may help the parliament to hold actors to account.

In addition to parliamentary and judicial control functions, civil society plays a crucial part in overseeing the security sector. Civil society can contribute to providing policy advice as well as technical expertise and might facilitate dialogue and negotiations in their role of a public watchdog.

Civil society further contributes to increasing awareness on various issues and can steer policy-making. Especially, the media can investigate and support the access to information by looking deeper into issues of concern

CASE STUDY: 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 means of repression and 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 organisations are raising awareness about this business practise, and even released a searchable database on more than 520 surveillance companies that sell their tools to governments around the world, this issue remains highly unregulated.

2.2. Developing norms and institutions that promote and strengthen transparency and make information freely available and accessible.

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

Transparency can generally be considered to have a two-fold purpose: to allow for information-sharing fostering effectiveness of security sector institutions, as well as being a prerequisite for their accountability. In addition, information and communication technologies (ICTs) are a tool themselves to promote and strengthen transparency, making information accessible to citizens.

However, absolute transparency is both unfeasible and not necessarily recommended depending on the context. .

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

Transparency also increases understanding of cyber security risks and encourages governments, private companies and civil society to more effectively coordinate and collaborate in order to be able to prevent and respond to these cyber security risks.

Understanding cyber risks can contribute to informed decision-making by individual users. 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 success rates of a vast majority of malicious activities.

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

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

EXAMPLES OF GOOD PRACTICE

The Organisation for Security and Cooperation in Europe (OSCE) in 2014 adopted an agreement on Confidence-Building Measures. Voluntary measures include the provision of national views on cyber doctrine, strategy and threats. OSCE Members further agreed to share information on national organisations, programmes or strategies relevant to cyber security, identify a point of contact to facilitate communication and dialogue on ICT-security matters.

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

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

The Organisation of American States published a report on computer security incident response teams (CSIRT) that identifies different means to enhance cooperation between CSIRTs for information sharing.

(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 enabling environment for information sharing and accessing information.

2.3. Strengthening the rule of law principle in cyberspace.

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

"The digital environment can by its very nature erode privacy and other fundamental rights, and undermine accountable decision-making.[10] Consequently, there is an increasing danger of undermining the rule of law principle by eroding 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, available at http://www.statewatch.org/news/2014/dec/coe-hr-comm-rule-of-law-on-the%20internet-summary.pdf

10 Ibid. p. 6.

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 developed a rule-of-law test where "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 been urging private companies, owners of social media platforms, to make sure their services are not hijacked by violent extremism and terrorism.

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 entities, public and private, 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., available at https://www.un.org/ruleoflaw/files/2004%20report.pdf.

In order to meet these government requests, private companies – especially social media companies such as Facebook, Google, and Twitter – have developed terms of service and codes of conduct to regulate content hosted on these social media platforms – de facto creating norms on the Internet. However, these terms of service and codes of conduct are not the same across various platforms – creating ambiguity and legal uncertainty as to what content is prohibited where.

11 Ibid, p. 8

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

While it is uncontested that social media companies should have a right to police their platforms and identify community standards, when it comes to terrorism social media company de facto act as regulators that can restrict free speech on their platforms – without having obligations under international human rights law. Moreover, social media companies are also experiencing increased pressure from states to keep their platforms free from any violent speech that incites, glorifies or apologies terrorism.

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

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

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

Twitter on the contrary does not refer to terrorism in the Twitter Rules. Twitter prohibits hateful content that promotes violence against or directly attacks or threatens other people based on race, ethnicity, national origin, sexual orientation, gender, gender identify, 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 can include mass murder, terrorist attacks, rapes 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 by using back-doors. In other words, in relation to national security, there is no real cornerstone to uphold the rule of law. Yet, there are at least certain basic principles that could make a foundation for such an essential part of the universal human rights edifice. Given the increased number of partnerships between law enforcement, intelligence and security agencies, this weakening of the rule of law threatens to spread among policemen and prosecutors as well. Absence of clear legal frameworks in this regard, domestically and internationally, is a further jeopardy to the rule of law on Internet and wider global digital environment.

The principle of the rule of law has also been challenged in the international law context, as there is a tendency to move towards voluntary, non-binding and rather 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: PRIVATISED LAW ENFORCEMENT IN CYBERSPACE

The fact that the Internet and the global digital environment is largely controlled by private entities (especially, but not only US corporations) 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 state limitations of the right to freedom of expression. These private entities can also be ordered by domestic courts, acting at the request of other private entities, to perform highly intrusive analyses of their data to detect probable (or just possible) infringements of private property rights, often intellectual property rights.

They can be ordered to "pull" data, including governmental, commercial and personal data, from servers in other countries, for law enforcement or national security purposes, without obtaining the consent of the other country – or the consent of the companies or data subjects in the other country – in violation of the sovereignty of the other country, the commercial confidentiality that companies are entitled to, and the human rights of the data subjects.

The liability of social media companies ("intermediary liability") should be interpreted more closely. To put it differently, when platforms such as Google, Facebook, or YouTube are held responsible for content their users post on their platforms it should be assessed very carefully, as this can have a direct effect on freedom of expression and other human rights. However, governments around the world have increasingly pressured these 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 further advocate that "evidence sufficient to document the legal basis of the order" is provided before any content is restricted by an intermediary. The Manila Principles furthermore stress the importance of building transparency and accountability into laws, noting that governments must not use extra-judicial measures to restrict content, which includes collateral pressures to force changes in terms of serve, to promote or enforce so-called "voluntary" practices and to secure agreements in restraint of trade or in restraint of public dissemination of content.

(Source: https://www.manilaprinciples.org/)

The Argentina draft law on intermediary liability states that "internet service providers shall not be liable for content created by third parties, except when, having 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

- Thinking of security in terms of governance is useful because it emphasises how a variety of state and non-state actors exercise power and authority over security, both formally and informally and at 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 role in shaping decisions about security and their implementation.
- Key principles of good SSG are: accountability, transparency, rule of law, participation, responsiveness, effectiveness, and efficiency.
- Good SSG is based on the idea 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 a collection of principles and therefore, the same core principles of good governance apply differently in each security sector.
- Establishment of a good SSG is a matter of on-going adjustment as security threats continuously evolve.
- SSR improves ability of the security sector to provide security for the state and its citizens.
- SSR makes use of public resources in the security sector more efficient.
- SSR reduces opportunities for corruption by improving oversight and professionalism.
- SSR protects professional independence of security personnel so that they can effectively fulfil their legitimate tasks, enhances professional standards and strengthens accountability, reducing abuse of the population.
- 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 SSR Backgrounder, Security Sector Governance. Applying the principles of good governance to the security sector, available at https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf

DCAF SSR Backgrounder, Security Sector Reform. Applying the principles of good governance to the security sector, available at https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_2_Security%20Sector%20Reform.pdf

DCAF, The International Security Sector Advisory Team, SSR in a Nutshell. Manual For Introductory Training on Security Sector Reform, available at 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, available at 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), available at 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 seeks to provide participants with a closer look at cyberspace and cybersecurity. Specifically, the goal of this chapter is to increase participant's knowledge of cyberspace and cybersecurity as well as to highlight complexities in implementation of good security sector governance (SSG) practices in these fields.

Learning objectives of this chapter are the following:

- Increased knowledge of cyberspace medium in terms of scope, actors, and risks.
- Increased knowledge of cybersecurity and its impact on human security, national security, and service provision.
- Understand limitations and ways SSG practices can be implemented in the context of cyberspace.

1. 1. Introduction

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

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

Despite this, and perhaps due to its diverse uses, the concept of cyberspace and its various components is not well defined. To best approach the good SSG in cyberspace, a more concise understanding of what is meant by "cyberspace" and "cybersecurity" is needed.

What is Cyberspace?

Nature of cyberspace as an abstract concept seemingly not grounded in the physical world, has led to a lack of clarity regarding to what this term actually means.

Organisations and nations often define cyberspace in a manner that best suits their purpose or use of it. Frequently these definitions focus on security, militarisation, or vulnerabilities present in cyberspace, with each organisation, nation, or a group focusing on different aspects. However, there is a common ground found in most definitions: cyberspace is an environment created by both physical and virtual components where data, information, or communication is stored, modified, or exchanged.

While the Internet may be the most common and easily accessible form of cyberspace to an average citizen, it is far from its only aspect[1]. Cyberspace includes any computer-based network systems for the aforementioned purposes of storing, modifying, or exchanging[2], and as such it can be found in increasing number of watches, appliances and other items connected in cyberspace (also known as the Internet of Things – IoT). Taken together, these different flows of data and information make up the "virtual" construct called cyberspace.

1 Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward, DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, 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 2015 Working Paper no. 1. Geneva: Democratic Control of Armed Forces, p. 9. available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

Cyberspace is a global domain, full 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 articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights[3]".

Additionally, cyberspace touches upon physical aspects, including computer-based desktops and laptops, tablets and smartphones, servers and physical cables creating the Internet infrastructure. Cyberspace as a medium allows for activities that quite often resemble activities in the physical world: people rely on cyberspace to communicate with each other, trade, research, engage in recreational activities, and keep up-to-date with the news. However, not all uses of cyberspace are as innocent: this same medium can serve as a space for criminal activity, military attacks, and other nefarious activities.

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

Defining Cyberspace
Some examples of cyberspace definitions currently in use:

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

International Organisation for Standardisation
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: CCDCOE, available at: https://ccdcoe.org/; EENISA, ENISA overview of cybersecurity and related terminology ver. 1. European Union. September 2017 available at: 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), 8.)

EXAMPLE OF GOOD PRACTICE

At the beginning of the 21st century, France had one of the lowest rates of internet and computer penetration within the European Union. However, today a large majority of the population is participating in cyberspace. To further increase the accessibility and ease-of-use of cyberspace, France has launched "Très Haut Débit", a new initiative to promote a high- speed access to the Internet, particularly for rural and under-connected communities. Through partnering with public and private groups, France aims to see 100% coverage in high speed internet connection and give 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 there are some commonalities between different institutional definitions of cyberspace, the imprecise nature of all these definitions makes it possible for actors in cyberspace to shape its varied aspects to best suit their needs and justify their actions. This is particularly striking when describing how to best utilise or protect the medium. The definitions are also indicative of the way states view cyberspace, either as a tool for the military, a platform which they use to distribute services, or an arena for trade and communication.

For our purposes, cyberspace will be defined as: the global, networked environment where data and information are exchanged, stored and modified, and which is accessible by both state and non-state actors.

Use and Authority in Cyberspace

Given the wide-ranging character of cyberspace, it is only logical that its uses and users, are as varied as the medium itself. Actors include both state and non-state actors. States utilise cyberspace to hold elections and provide services for its population, as well as a tool to protect national security and national vital interests.[4] Non-state actors range from companies to citizens, all utilising cyberspace for different purposes. All these actors contribute to influencing and shaping cyberspace.

This global nature of cyberspace 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 will also have important effects on both economic and human security.[5] As the world becomes more reliant on services and freedoms granted by cyberspace, it becomes increasingly imperative that human rights and human security, as well as national security, are protected[6] .

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

5 Cole, Kristina, et all, 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. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

CASE STUDY: SECURING THE PHYSICAL COMPONENT

There has been a recent push to increase security of computer-based 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 tech manufacturers to ensure their products' security.

The Department of Homeland Security of the United States of America released a number of strategic principals in 2016 aimed at securing the Internet of Things. The first stage of this approach is to secure the devices during their manufacturing, then maintaining security through updates and vulnerability management.

The United Kingdom created a "security code of practice" for manufacturers to encourage them to increase security of the devices while in the development phase. To increase security of the devices themselves, the code calls for Internet of Things devices to have more unique password requirements, as well as a push for greater transparency in security breaches by encouraging public disclosure of any vulnerabilities in the devices. Currently this code is on a voluntary basis only, but the UK has not ruled out the possibility of making it mandatory for devices manufactured in the country.

Although the EU approach to increasing device security is still being drafted, it will create a certification process for IoT devices on an EU-wide scale.

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

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

Cybersecurity

With the proliferation of cyberspace use by governments, individuals and companies, amount of sensitive data and information within cyberspace is increasing exponentially and becoming subjected to new and ever-changing vulnerabilities.[7] Effective protection of the information is essential to creating a secure environment within and outside of cyberspace as well. Cybersecurity, as its name would suggest, consists of practices and methods for securing data, information, and integrity of various components of cyberspace, including but not limited to the physical aspects of the medium.[8]

7 Fred Schreier, Barbara Weekes, Theodor H. Winkler, Cyber security: The Road Forward, DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, 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

Although cybersecurity is often associated with national security strategies, it is important to look at broader applications of the term. The ITU describes cybersecurity as set of tools, guidelines, and other approaches made to protect integrity and confidential nature of cyberspace for private organisations, government, and civil society[9] .

In line with the growing importance of cyberspace for professional, recreational and political activities, cybersecurity is a developing field in the realm of security and good security sector governance. The norms pertaining to security in cyberspace have been evolving in order to respond to a rapid expansion of cybersecurity practices and techniques, as well as ever-changing actors in the field.[10] As nations craft their national approaches to ensure a safer cyberspace environment in their respective countries, certain norms on the extent of their power over cyberspace as well as ways states can exert their powers over cyberspace are emerging[11] .

Cybersecurity Metrics

Given the vast and competing definitions of cyberspace and cybersecurity, analyzing cybersecurity is no easy feat. The ITU created the Global Cybersecurity Index to determine their member-states' commitment to strengthening cybersecurity. This Index evaluates five different aspects of cybersecurity, legal, technological, organizational, capacity building, and cooperation, to see the commitment of a nation.
While this is a good tool to establish the government's response and actions to cyberspace governance, it neglects non-state actor's role in both cyberspace and cybersecurity. Since it evaluates policies and not practices, it does not take into consideration the practical impacts or efficacy of these commitments.

9 ITU guide to develop NCSS, 13

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

11 IBID

2. SSG in Cyberspace

Cyberspace presents a set of liberties, restrictions, and complexities unique to the nature of the medium itself. Given the diverse array of actors in cyberspace and the way it can be utilised or abused, creation of a framework for good SSG practices faces different sets of obstacles for a more traditional 'territorial' security. Some of these obstacles were elaborated on in previous chapter, primarily those weakening the rule of law, transparency, and accountability.

In viewing SSG through a cyberspace lens, it is important to take various actors in this sphere into consideration, evaluate who controls which aspects of cyberspace, and how to best influence or incentivise behaviours and practices that will ultimately strengthen good SSG in the cyberspace arena. Diverse array of actors in cyberspace and cybersecurity creates an interesting paradigm for policy-makers to explore, since states are unable to unilaterally provide effective security and regulation of the medium.

Good Practice: Implement a cybersecurity approach involving actors from both public and private sectors in cyberspace

Since cyberspace is a platform for both private and public actors, creation and implementation of different policies tackling on SSG need to include all entities that exist outside of the public sphere. Recognising the role of information and communication technologies (ICT) companies and private cybersecurity corporations play in formation and protection of users' rights and security is an important step towards creation of 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 pharma sales company, Cameroon partnered with the Czech Republic, INTERPOL, and Nigeria to conduct digital investigations. Cameroonian authorities promote several confidence-building measures and international cooperation agreements in cyberspace by exchanging information on cyber incidents and best practices for cyber security.

Current issues with SSG in Cyberspace

Good SSG practices in cyberspace can help ensure that human security, rule of law, and other aspects of good governance are further observed and protected in cyberspace.

As briefly mentioned in the last chapter, one of challenges facing security sector governance in cyberspace is a lack of understanding on how to implement effective governance principals in cyberspace, resulting in inadequate policies and regulation, and creating an enabling environment for criminal activity.[12] The lack of knowledge can also have impact

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

on states' effective regulation over private sector actors, undermining the state's ability to enact good SSG practices in cyberspace.

Currently many cyberspace security services are provided by private commercial entities posing challenges for effective implementation of SSG practices in cyberspace. Transparency is one aspect of good governance that is becoming increasingly difficult for states to implement. Definition of transparency in cyberspace from a good SSG perspective has not been agreed upon. However, more and more term transparency in this context is associated with disclosing when, and to what extent, a breach of information systems has occurred.[13]

CASE STUDY: MANDATING TRANSPARENCY

Australia

In 2017, the Australian Parliament passed an amendment to the Privacy Act 1998 that requires Commonwealth government organizations, private sector organizations, and other specified bodies to disclose information regarding cybersecurity breaches to those impacted by the breaches. Failure to comply with this new regulation would result in a monetary compensation to those impacted by the violation, public acknowledgement and apology for failing to comply and large civil penalties for those who experience multiple instances of non-compliance.

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

The United States

The United States Securities and Exchange Commission imposed a large fine of $35 million USD on Yahoo as a result of not disclosing a cyberattack that impacted over 500 million accounts. This was the first instance of a company receiving a fine for failing to comply with disclosure requirements mandated of publicly traded companies.

Source: Kadhim Shubber, "Yahoo's $35m Fine Sends a Message" (Jahuova kazna od 35 miliona dolara šalje poruku), Financial Times, www.ft.com. Available at: https://www.ft.com/content/4c0932f0-6d8a-11e8-8863-a9bb262c5f53

Encouraging or mandating actors to disclose cybersecurity breaches is one way a state can increase good SSG practices, as it not only increases the transparency within cyberspace, but also ensures that gaps within the current cybersecurity practices are addressed, helping stop proliferation of cyberattacks and improving security practices in cyberspace.[14] A lack of transparency in relation to cyberattacks greatly undermines human security in cyberspace, as it allows malicious cyberattacks to hurt more victims.

In addition to this, transnational nature of cyberspace creates a dilemma for states to enact good SSG practices within it. As citizens engage in transactions crossing international territorial borders on constant basis, a state's ability to exert authority over what impacts their population significantly diminishes. In most cases, States have to rely on commercial intermediaries – such as social media platforms – to oversee

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

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

and regulate behaviours online.[15] This could undermine good SSG practices, as the state typically does not have the access to see how information is filtered or taken down. Another challenge is a transnational nature of information on Internet, which can be stored on one or more servers located in multiple jurisdictions. The reliance on other states in investigating, persecuting, and convicting cybercriminals also creates a different dynamic. In this way, cyberspace undermines good governance practices as it relies not only on actors within a single jurisdiction, but instead impacts an international array of actors.

CASE STUDY: INTERNATIONAL INVESTIGATIONS

International investigation and criminal prosecution in the field of cybersecurity is not an unheard-of phenomenon. 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 effort of 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.

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

Although it may seem as though there are many obstacles in applying good SSG practices to cyberspace, it is far from an impossible task. Some international frameworks and norms providing guidance on how to integrate SSG into cyberspace have begun to concretise. While practices and policies have to be tailored to fit a national context, identifying what international and regional cyberspace related framework are in force is a key step towards good SSG in cyberspace.

15 Niva Elkin-Koren; Eldar Haber, Governance by Proxy: Cyber Challenges to Civil Liberties, Brooklyn Law Review 82 no. 1. 105

KEY FINDINGS

- Cyberspace exists on both physical and non-physical level and is made up of any platform used for transfer, transformation of alteration of information, data, and communication from one computer to another. It also encompasses physical infrastructure of the Internet that spans the globe.
- Governments, citizens, and companies are becoming increasingly reliant on resources cyberspace provides in daily life.
- There is a vast array of actors within cyberspace and cybersecurity.
- Various obstacles to SSG in cyberspace exist, ranging from multiple actors impacting different aspects of cyberspace, to a general lack of knowledge on the safe use of cyberspace.
- Although some states have policies and frameworks in place for cybersecurity and cyberspace governance, a general lack of knowledge makes it difficult to ensure proper implementation of SSG practices in cyberspace.

Resources

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

Elkin-Koren, Niva, and Eldar Haber, Governance by Proxy:Cyber Challenges to Civil Liberties, 82 Brook. L. Rev.105 (2016)

Fred Schreier, Barbara Weekes, Theodor H. Winkler, "Cyber security: The Road Forward" DCAF Horizon 2015 Working Paper No. 4 Geneva: Democratic Control of Armed Force, https://www.dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf

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

Paul Smith "New mandatory data breach notifications laws to drag Australia into cyber age" Financial Review, afr.com, Feb. 23, 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

CILJEVI

This chapter seeks to provide users with an overview of the international and regional legal frameworks applicable in cyberspace, and highlights interesting and innovative approaches and initiatives.

Learning objectives of this chapter are the following:

- Increased knowledge of various international and regional organisations pertaining to cyberspace and cybersecurity.
- Increased awareness of available resources supporting implementation of international and regional legal frameworks on a national level.
- Increased knowledge of cybercrime, cyberterrorism and terrorist use of the Internet.

Introduction

Effective legal frameworks – at international, regional, and national levels – are one of the pillars of good governance and constitute a prerequisite for the rule of law principle. Generally speaking, legal frameworks are essential to regulate lawful behaviour and prohibit or criminalise unlawful activities. Legal frameworks in cyberspace are also important to ensure respect for human rights.

There has been a lot of discussion and confusion over how legal frameworks can and do apply to cyberspace. Because of its trans-border, information-centric nature, cyberspace poses challenges to state-centric approaches to governance. On one hand, the physical infrastructure that makes up cyberspace is subject to national jurisdiction and authority. On the other hand, flow of data and information across that infrastructure is constantly crossing through (multiple) territorial jurisdictions, making it difficult for one legal jurisdiction to exercise "effective control" over this flow of information. This has led many to call for the development of new normative regimes to regulate cyberspace.

Nowadays it is uncontested that principles of international law should be applicable in cyberspace. What is less clear is how these principles translate into practice. Consequently, this gap between policy and practice leads to legal uncertainties and even legal lacunae that can undermine protection of users' human rights on the Internet. Therefore, international and regional organisations have undertaken actions to launch initiatives aiming to identify and interpret how existing legal principles of international law apply in cyberspace.

1. International Legal and Regional Framework

Numerous initiatives on international and regional level aim to promote more responsible behaviour in cyberspace and develop regulatory frameworks and confidence-building measures in cyberspace. The following provides an overview of most initiatives in question.

United Nations

There is currently no legally binding instrument on international level that regulates behaviour in cyberspace. However, there is a number of "soft-law" initiatives (legally not binding) identifying norms in cyberspace and providing guidance for states on how to apply these norms.

Nowadays it is generally uncontested that international law – in particular the United Nations Charter, international human rights law, and international humanitarian law – applies in cyberspace.

CASE STUDY: UN GROUP OF GOVERNMENT EXPERTS REPORT

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

Positive norms:

- States should cooperate to increase stability and security in the use of ICTs and to prevent harmful ICT practices.
- States should consider all relevant information with regard to attribution in the ICT environment;
- States should take appropriate measures to protect national critical infrastructure from ICT threats, and respond to appropriate requests for assistance by another State;
- States should take reasonable steps to ensure the integrity of the supply chain and should prevent the proliferation of malicious ICT tools and techniques.
- States should encourage responsible reporting of ICT vulnerabilities and share associated 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 resolutions linked to human rights.
- States should not conduct of knowingly support ICT activity contrary to its obligations under international law.
- States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams.

The United Nations, for instance, since 2004 has established six consecutive Groups of Governmental Experts (UN GGE) – based on "equitable geographical distribution" and including key "cyber powers", such as the United States of America, China, Russia, France, the United Kingdom and Germany – with the aim to propose norms of responsible behaviour in cyberspace.

CASE STUDY: ELECTION MEDDLING THROUGH ONLINE INFORMATION CAMPAIGN – A CASE FOR INTERNATIONAL LAW?

While interfering in political processes through covertly and overtly means is nothing new in international relations, since 2016, governmental officials primarily in Western states express concerns over election interference via targeted cyber operations and misinformation campaigns.

In 2014, CyberBerkut operations targeted the Ukrainian Central Election Commission, taking down the parts of the Commission's networks for nearly twenty hours and announcing a false winner on election day. In 2016, the "Fancy Bear" hacking unit targeted the German Bundestag, Germany's Foreign and Finance Ministries, and the Christian Democratic Union's systems. In 2017, cyber operations that aimed to implant malware on a campaign's website, targeted Emmanuel Macron's campaign for the French Presidency.

Under international law obligations, it is likely that these constitute a violation of a State's sovereignty. Sovereignty has been widely considered a principle and primary rule of international law – which was also embraced by the UN GGE report 2015

"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's object and purpose is "to afford states the full control over access to and activities on their territory".

What does this mean in election meddling through cyber operations?

Experts argue that the critical point to assess whether such an action amounts to a violation of the principle of sovereignty is "not that there was a nexus between the targeted system and the election, but instead simply that the operation resulted in the requisites harm – a loss of functionality." According to the Tallinn Manual 2.0 actions that could qualify as violations of sovereignty are: a cyber operation causing cyber infrastructure or programmes to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major distributed denial of service operation.

A major breakthrough was achieved in 2013, when the UN GGE consisting of only fifteen members at the time adopted its consensus report affirming applicability of international law in cyberspace. The UN GGE 2015 consensus report reaffirmed this statement and further specified a normative framework for state's use of cyber capabilities. Herein the section focusing on "norms, rules and principles for the responsible behaviour of states" is of a particular interest.

Unfortunately, the 2016-2017 UN GGE was not successful in adopting a consensus report, throwing the international community in a certain disarray regarding how to best apply the international law in cyberspace. However, in October 2018, the UN General Assembly (UNGA) adopted resolution A/C.1/73/L.37 to create another GGE in 2019, 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 in order to develop rules, norms and principles of a responsible State's behaviour in cyberspace, as well as to consider their practical implementation.

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

It is generally accepted that the international human rights law framework, including the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights, apply in digital space. This was affirmed by the Human Rights Council (HRC) in resolution A/HRC/20/L.13 stipulating that "same rights that people have offline must also be protected online".[1] This resolution bears particular importance as it was the first time the international body explicitly stated that human rights protection apply to cyberspace as well.

In the aftermath of the Snowden revelations[2] the UNGA decided to establish a new Special Rapporteur on the Right to Privacy in order to better address privacy in the digital age and to create a safer digital environment in 2015. The Special Rapporteur on the Right to Privacy is mandated to conduct state visits, make recommendations, and deal with individual complaints.

Another important UNGA resolution is A/RES/57/239 on creation of a global culture of cyber security recognising cybercrime as a major challenge to cyber security.[3]

Another UN instrument relevant for identification of norms in cyberspace is the United Nations Guiding Principles on Business and Human Rights[4] (also known as the 'Ruggie Principles') adopted in 2011 and offering guidance to States as well as businesses with regard to human rights protections. The Ruggie Principles are based on the UN framework "Respect, Protect, and Remedy". It is stipulated in the introductory part to these guiding principles that "business enterprises

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

3 https://digitallibrary.un.org/record/482184?ln=en

4 OHCHR, Guiding Principle on Business and Human Rights, available at https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

as specialised organs of society performing specialised functions, are required to comply with all applicable laws and to respect human rights." [5]

In the context of regulating certain forms of unlawful speech on Internet, hate speech, in particular, a report by the UN High Commissioner for Human Rights, adopted by the Human Rights Council in 2013 (known as 'Rabat Plan of Action') identifies criteria serving to identify hate speech and can provide guidance in the online realm as well[6].

CASE STUDY: RABAT PLAN OF ACTION

The Rabat Plan of Action identifies a six-part threshold test to assess the severity of certain expression that can be considered as criminal offences. These six criteria are: context; speaker; intent; content and form; extent of the speech act; likelihood; including imminence.

As per the element of 'context', the Rabat Plan of Action concretises that 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

Various other 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 cyber security, as well as the Working Group on Countering the Use of the Internet for Terrorist Purposes which operates under the UN Counter-Terrorism Implementation Task Force.[7]

The International Telecommunication (ITU), a UN agency specialised in telecommunications, addresses cybersecurity as part of its mandate. To this end, the ITU develops model laws and cyber security country profiles publicly available and supports UN Member States in developing effective normative frameworks for cyberspace.

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

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

7 United Nations Office on Drugs and Crime (2012): The use of the Internet for terrorist purposes, available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

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

HIPSSA was initiated as a result of the request made by the economic integration organisations in Africa, as well as regional regulators associations, to the ITU and the European Commission for assistance in harmonising ICT policies and legislations in Sub-Saharan Africa.

HIPSSA became an important building block in establishing global pan-African harmonised ICT policies and frameworks.

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

Council of Europe

The Council of Europe (CoE) is comprised of 47 Member States. Its Convention on Cybercrime (also known as "Budapest Convention")[8] is considered – for the time being – the most relevant international legal instrument providing a legal framework to address cybercrime. The Budapest Convention is open for accession by CoE Member States as well as by non-member States. To date, the Budapest Convention has been ratified by 61 States.[9] The Budapest Convention is supplemented by its Protocol on Xenophobia and Racism committed through computer systems.[10]

Importantly, the Budapest Convention 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.

In addition, the CoE drafted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No CETS 108),[11] with the objective 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 in the data protection field. Under this Convention, parties are required to take necessary steps in their respective national legislations to apply the principles in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data. The Convention No 108 has been updated in May 2018 to

8 Council of Europe, Convention on Cybercrime, CETS No. 185, available at 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, available at 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, available at 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, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8

capture 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 for interpreting the Conventions and various capacity building programmes, such as GLACY+ programme supporting states in developing effective legislation for cyberspace.[14]

While the Budapest Convention is the only international legal framework to regulate cybercrime, human rights advocates a particular stress on the fact that the Budapest Convention is based on the assumption of States having human rights safeguards in place.

However, non-CoE Member States do not necessarily have the same human rights safeguards in place

African Union

AIn 2014, the African Union adopted the Convention on cyber security and personal data protection (also known as the "Malabo Convention").[15] However, the convention has not entered into force yet, as it has been adopted by only five Member States of the African Union (Senegal, Mauritius, Guinea, Namibia and Ghana) and signed by nine Member States. Its Article 25 (1) namely "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 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 currently the only legally binding international legal framework on the topic of cybersecurity, cyberspace, and the state's role in the arena. Although only a handful of African nations have directly signed it or been invited to accede, it has been used as a guiding framework for the creation of the African Union's Convention on Cybersecurity. This is an example of the way in which broader international norms can be adapted and adopted into a region-specific context.

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

Economic Community of West African States

EThe Economic Community of West African States (ECOWAS) adopted the Supplementary Act on Personal Data Protection within ECOWAS in 2010,[16] which is influenced by the EU Data Protection Directives, specifying that required content of data privacy laws and obligates member states to establish a data protection authority.

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

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

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

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

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

Organisation for Security and Co-operation in Europe

The Organisation for Security and Co-operation in Europe (OSCE) addresses cyber / ICT security issues, especially in light of counter-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 at reducing conflict stemming from the use of information and communication technologies.

CBMs identified by the OSCE include: exchanging information on cyber threats, security and use of ICTs, national organisations, strategies and terminology, holding consultations in order to reduce risks of misperception and of possible emergence of tension, sharing information on measures taken to ensure an open and secure internet, exchange of points of contact, and the use of the OSCE as a platform for dialogue.

However, the CBMs are based on a voluntary approach and therefore are a non-legally binding instrument.

Organisation of American States

The Organisation of American States (OAS) established a Working Group on Cyber-Crime already in 1999, as the principal 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 biannual basis, providing recommendations for Member States.

The OAS also deals with cyber security in a wider sense. In 2004, the OAS General Assembly provided a mandate in resolution AG/RES.2004 (XXXIV-O/04), titled "The Inter-American Integral Strategy to Combat Threats to Cyber Security" for the Secretariat of the OAS Inter-American Committee against Terrorism. The main tasks for this Secretariat are to help establish national Computer Security Incident Response Teams (CSIRTs), create a network composed of these CSIRTs and support the development of national cyber security strategies. Since 2007, the Secretariat has endeavoured to create a comprehensive capacity-building programme based on a number of workshop, technical courses, roundtable policy discussions, crisis management exercises, and exchange of best practices.

17 EECOWAS, Economic Community of West African States (ECOWAS), Directive C/DIR.1/08/11 on Fighting Cyber Crime within ECOWAS, 2011, available at http://www.osiris.sn/Directive-C-DIR-1-08-11-du-19-aout.html

18 OSCE Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, (Odluka OEBS-a broj 1202, OEBS-ove mere izgradnje poverenja u cilju smanjivanja rizika od pojave konflikta kao posledica upotrebe IKT-a) PC.DEC/1202, 10.03.2016, dostupno na https://www.osce.org/pc/227281?download=true

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

Shanghai Cooperation Organisation

The Shanghai Cooperation Organisation (SCO), an international organisation with six member states (namely China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) adopted in 2009 an Agreement among 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 International Code of Conduct for Information Security to the UN General Assembly. In 2015, a new Draft International Code of Conduct was submitted to the UN General Assembly.[21]

CASE STUDY: SCO DRAFT INTERNATIONAL CODE OF CONDUCT, 2015

According to the sponsors of this draft code – namely, the SCO's 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".

According to some analysts, the draft code emphasises state sovereignty and territoriality in cyberspace and is preoccupied with intelligence, national security and regime stability imperatives and lacks substantial human rights protection and primarily addresses restrictions on freedom of expression available to states under the law. It is also noteworthy that the draft code does not refer to the right to privacy at all.

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

Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation (APEC) issued in 2002 the APEC Cyber Security Strategy containing recommendations in the area of cybercrime legislation, security and technical guidelines, public awareness, and training and education.[22] The Lima Declaration (2005) aims at improving information infrastructures in order to advance work of the information society.[23] The declaration also addresses network security and importance of establishment of computer emergency response teams (CERTs). APEC's Strategy to Ensure a Trusted, Secure and Sustainable Online Environment aims to provide information and network security, to harmonise frameworks for securing transactions and communications, and combat cybercrime. Increasingly, this includes close cooperation with the private sector and other international organisations. APEC's TEL Strategic Action Plan 2010 – 2015 aims to "promote a secure, resilient and trusted ICT environment", including the following key areas: enhancement of the resilience of

20 AAgreement among Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 2009, available at https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIxMiJ9

21 Shanghai Cooperation Organisation, Draft International Code of Conduct, Letter dated 9 January 2015 to the United Nations General Assembly, A/69/723, available at https://digitallibrary.un.org/record/786846?ln=en

22 AAPEC Cyber Security Strategy, available at https://www.ccdcoe.org/uploads/2018/10/APEC-020823-CyberSecurityStrategy.pdf

23 APEC, Lima Declaration, 2005, available at https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2005_tel

The SCO refers to the concept of "international information security", underlying the importance of content as a source for a potential security threat

critical domestic infrastructure, security and risk management, cyber security capacity building, raising cyber security awareness, cyber security initiatives with industry, activities to promote safe and secure online environments for vulnerable groups, and the internet economy[24].

Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN) consisting of ten Member States (i.e. 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 discussed cybersecurity in the context of counter-terrorism and transnational crime[25].

Commonwealth of Nations

The Commonwealth of Nations comprises 53 Members States and focuses on capacity-building, information-sharing and providing assistance to Commonwealth Member States in implementation of legal framework pertaining to cybercrime. There are two platforms within the Commonwealth of Nations: the Cyber Security Forum and the Cyber Security Initiative operating under the Commonwealth Telecommunication Organisation. The latter has adopted the Commonwealth Cyber-governance Model,[26] approved by the Abuja Declaration in October 2013 and launched during the Commonwealth Cybersecurity Forum in London in 2014.[27]

The Commonwealth Cyber-governance Model[28] offers a draft set of principles for consideration that would contribute to a safe and an effective global cyberspace; support broader economic and social development; act individually and collectively to tackle cybercrime; exercise rights, and meet responsibilities in cyberspace.

European Union

Documents adopted by the European Union (EU) and most relevant for cyber security are either legally non-binding documents (such as communications) or different types of legally binding acts that place obligations on its Member States or specific entities.

In 2013, the EU published its first comprehensive document – its 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

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

25 http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf

26 Commonwealth Cybergovernance Model, available at https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

27 Commonwealth Cybersecurity Forum in London in 2014, available at https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

28 https://ccdcoe.org/uploads/2018/11/CommW-140304-CommonwealthCybergovernanceModel.pdf

29 European Union, Directive on security of network and information systems, (EU, Direktiva o bezbednosti mreža i informacionih

the vision, roles, responsibilities and required actions for the EU in the domain of cyber security. Importantly, the document underlines that in the context of cyber security, centralised EU supervision is not the answer, hence national governments should remain principle entities in charge of prevention and provision of response to cyber incidents at a national level.

As one of its objectives, the EU Cyber Security Strategy identifies development of cyber defence policies and capabilities relying on the framework of the Common Security and Defence Policy and outlines a list of actions envisaged for collaboration between the European Defence Agency and Members States.

Cyber security-related actions have been further incorporated in the EU's Digital Agenda, dealing with trust and security on Internet vital to a vibrant digital societies. Notably, the European Agenda on Security prioritises cybercrime as one of the most relevant emerging threats.

Importantly, the EU Cyber Security Strategy stipulates that a "particular 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).

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

North-Atlantic Treaty Organisation

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 North-Atlantic Treaty Organisation's (NATO) first cyber defence policy was prepared in 2008. At the Lisbon Summit in 2010, cyber defence was incorporated in NATO's Strategic Concept, and the summit declaration precipitated the update of the Cyber Defence Policy in 2011 and creation of an accompanying Action Plan in 2012.

A new enhanced 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, as well as cooperation with the industry. At the Warsaw Summit in 2016, NATO recognised cyberspace as a domain of operations, and pledged to further develop NATO-EU cyber defence cooperation, and commit more resources to cyber defence capabilities building. In 2018, the defence ministers of NATO Member States agreed on creation of a new Cyber Operation Centre at SHAPE to help integrate cyber into NATO planning and operations at all levels.

sistema), L 194/1, 2016, dostupno na 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

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

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

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.

NATO hosts a Cyber Defense Committee (CDC), previously known as the Defense Policy and Planning Committee (Cyber Defense). This Committee is a senior advisory body and provides consultation platform for NATO Member States and exercises overall governance of NATO's internal cyber defense. In addition, there is a Cyber Defense Management Board (CDMB) operating under auspices of the Emerging Security Challenges Division of NATO Headquarters, and consisting of representatives of all major stakeholders in cyber security within NATO. Notably, the CDMB does the strategic planning and executive direction regarding NATO networks and signs Memorandum of Understanding with Member States in order to facilitate information exchange and coordinate assistance.

Furthermore, the NATO Consultation, Control and Command (NC3) Board constitutes a main committee for consultation on technical and implementation related aspects of cyber defense.

The Group of Seven (G7)

The G7 is in informal group of seven States (Canada, France, Germany, Italy, Japan, United Kingdom, and Unites States of America, with the EU having an observer status) that regularly meets to discuss important political and economic questions. Since 2016, the G7 has been producing a number of documents on cybersecurity, making it a major topic in various summit declarations[32].

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:

1. Recommendations to create trust, privacy and responsible use of personal data
2. Recommendations for actions to be taken by Governments and policy makers, data protection authorities, and data controllers and data processors
3. Recommendations for multi-stakeholder solutions, well-being of the digital citizen and enabling and sustaining measures.

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

2. Initiatives by Non-State Actors

Due to that fact that States have been reluctant to express their opinio iuris and state practice in cyberspace, there is no common agreement on how international law applies in cyberspace, which has in return led non-state actors to start filling this void. Private ICT companies and civil society organisations in particular have been proactive in proposing human-rights compliant cyberspace norms aiming to contribute to 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 Operations.[33] While this document is rather academic, it reaffirms basic principles of international humanitarian law, such as the principle of distinction, proportionality and necessity in cyberspace. In addition, this group of experts published the Tallinn Manual 2.0 addressing the applicable law in peacetime in cyberspace[34].

32 Group of 7, Charlevoix G7 summit communique, available at https://www.consilium.europa.eu/en/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/

33 Tallinn Manual, available at https://ccdcoe.org/research/tallinn-manual/

34 Tallinn Manual 2.0 Factsheet, available at https://www.almendron.com/tribuna/wp-content/uploads/2018/03/ccdcoe-tallinn-manual-onepager-web.pdf

CASE STUDY: THE NOTIONS OF 'ARMED ATTACK' AND 'USE OF FORCE' IN CYBERSPACE – BRIDGING THE LANGUAGE DILEMMA BETWEEN THE LEGAL, POLICY AND TECHNICAL COMMUNITY

It is important to differentiate to regimes in international law: (i) ius ad bellum (which governs when a State may resort to force as an instrument of its national policy), and (ii) ius in bello (international humanitarian law that establishes rules as to how operations may be conducted during an armed attack).

In the ius ad bellum context, according to Article 51 of the UN Charter, an armed attack can trigger self-defence. Therefore, the pressing question is when a cyber operation constitutes an armed attack that a State legally can merit a response with either cyber or kinetic actions at the level of a use of force. The importance hereby is on the notion of 'armed' because the International Court of Justice held in the Nicaragua Judgment 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 leaving the State unable to defend itself as the cyber operations does not qualify as an armed attack. In order to address this dilemma, a number of international law scholars advocate to interpret an 'armed attack' in cyberspace as encompassing any acts that result in consequences analogous to those caused by kinetic actions (physical consequences).

In the ius in bello context, before IHL can apply there needs to be an attack (that is defined through a consequences-based approach when interpreting 'attack'.

Microsoft, a private transnational corporation, proposed in February, 2017 that States should adopt a "Digital Geneva Convention" identifying norms in peacetime for cyberspace. Microsoft regularly publishes policy papers and blog posts that aim to contribute to confidence and trust-building among different stakeholders in cyberspace. However, while States generally welcome proactive initiatives by non-State actors, there is still scepticism towards the prospect of their success.[35]

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

35 Microsoft Policy Paper, A Digital Geneva Convention to protect cyberspace, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH ; see also Microsoft cyber security guidelines, available at 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, available at https://www.nytimes.com/2018/07/13/technology/microsoft-facial-recognition.html

Other soft-law instruments, such as the Manila Principles on Intermediary Liability,[37] khave 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 organisations, have become more proactive in proposing norms applicable in cyberspace. Microsoft has been a forerunner in recent years in particular[38].

In addition to this, civil society organisations have become more active filling the vacuum left by States in cyberspace, proposing norms aimed at promoting human rights in cyberspace. For example, Article 19 (a London-based non-governmental organisation (NGO) supported by a number of other NGOs adopted the Camden Principles on Freedom of Expression and Equality on the Internet.[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 Principles on Freedom of Expression and Privacy provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing enjoyment of human rights around the world[40].

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) refers to internet access providers
- Web hosting providers ('hosts') typically refer to any person or company who controls a website or a webpage, which allows any third party to post and upload content.
- Social media platforms such as Facebook, Twitter, YouTube, etc., that 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 query.

These are internet access providers, social networks and search engines. Intermediary labiality means policies that govern the legal liability of intermediaries for the content of these communications

Source: https://www.manilaprinciples.org/#:~:text=Intermediaries%20should%20be%20shielded%20from,precise%2C%20clear%2C%20and%20accessible.&text=Intermediaries%20must%20not%20be%20held%20liable%20for%20failing%20to%20restrict%20lawful%20content

With regard to preventing violent extremism on the Internet, a coalition of social media companies, namely Facebook, Twitter, YouTube, and Microsoft, joined up to a Global Internet Forum to Counter Terrorism,[41] where these internet giants develop normative standards to regulate violent extremism on their respective 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 impacted by private ICT companies.

The Guiding Principles of Business and Human Rights (GPBHR) stipulate that there is a corporate responsibility to respect human rights. For ICT companies this means taking into account industry-specific issues, 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 and by efforts of governments to restrict users' rights.

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

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

39 Article 19, The Camden Principles on Freedom of Expression and Equality, available at 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, available at https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/

Key Findings

- Criminalisation gaps in any country can create offender's havens with the potential to affect other countries on a global scale.
- Criminalisation differences pose challenges for international cooperation in criminal matters involving cybercrime, in particular with regard to the principle of dual criminality.
- A comparative analysis of cybercrime offences is able to explore good practices that states may use in development of national laws, in accordance with emerging international standards in this area.

Resources

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

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 IN A NATIONAL CONTEXT

OBJECTIVES

This chapter will examine how the international and regional legal frameworks from the preceding chapter, as well as other norms within cyberspace, can be implemented at a national level, notably via corresponding legislation, policies, and strategies.

Learning objectives of this chapter are the following:

- Further understanding of the frameworks and other norms in cyberspace and their applicability in a national context.
- Increased understanding of the need for national legislation, policies, and strategies on cyberspace.
- Increased knowledge on how to create or amend national legislation, policies, and strategies based on cyberspace, based on good SSG practices.

Introduction

Use of cyberspace has become more and more prevalent with individuals, governments, and companies, be it for consumption of information, provision and reception of public and private services, or for sustaining operational processes. This may imply that all these actors are potentially susceptible to increased cyber breaches and attacks, vulnerabilities threatening human rights as well as national and human security.

While some norms for safe practices in cyberspace and a general framework of the legal expectations of rights within cyberspace have been established at international and regional levels, there is now an increased focus on the need for coherent and holistic national approaches to cyberspace challenges. Growing reliance on cyberspace means effective national legislation, policies, and strategies are evermore needed to protect the data, information and knowledge transmitted and utilised in cyberspace, as well as to increase the security of citizens therein.

The international or regional frameworks explored in the last chapter – consisting of resolutions, reports, conventions, and agreements on human rights and regulating cyberspace – have created a set of norms for countries to observe when amending their cyberspace and cybersecurity legislation, policies, and strategies, and can assist them in drafting or updating national polities and strategies on cyberspace and cybersecurity. In addition, private companies and nongovernmental organizations have sought to expand upon the aforementioned frameworks and norms to elaborate on prevalent approaches to cybersecurity. States can draw on these various elements to establish a holistic cyberspace and cybersecurity governance based on principles of good security sector governance.

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

Additionally, national policies and strategies should include an international outlook or be complemented by policies and strategies focusing specifically on international cooperation, so that the cyber regulation and cybersecurity go beyond national borders.

1 The good practices are based on: Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018)

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

Although cyberspace is in practice a global medium, legally speaking the duty of regulating it and ensuring its good governance falls on states as there is no international governance structure.[2] It is also important to mention that "same rights people have offline must also be protected online."[3] Thus, allowing ICT companies to operate without a sufficient regulatory framework may result in practices detached from the public interest and potentially violating human rights.[4] Therefore, states as primary bearers of human rights obligations and guardians of the public interest shall reflect the latest developments in technology in their legislative efforts to limit the space for potential adverse consequences of private sector actions. National legislation, policies and strategies, as well as the role of the security sector in regulating cyberspace and ensuring cybersecurity, are thus essential to ensure good governance practices.

Additionally, international and regional frameworks and norms are of a more general nature, while national legislation, policies and strategies allow to address national needs and specificities of cyberspace and cybersecurity.

Finally, relying solely on frameworks and norms established at the international and regional level do not provide a guarantee that other states will abide to these nonbinding principles, nor does it ensure that private and public actors within a single state will observe the norms.[5] Last but not the least, establishing or amending cyberspace and cybersecurity legislation, policies and strategies for cyberspace and cybersecurity governance can serve as a more comprehensive and cohesive way to ensure observation of laws and human rights in cyberspace within the realm of a respective state.

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

- It should be sufficiently (technology-wise) neutral to cater for the constant evolution of technology and crime as it otherwise risks becoming obsolete already by the time it enters into force.

- Law enforcement powers should be subjected to safeguards in order to ensure the rule of law and human rights requirements are met.

- It should be sufficiently harmonized or at least compatible with laws of other countries to allow for international cooperation, for example, meet the dual criminality condition.

2 ITU National Cybersecurity Strategy Guide 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

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

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

EXAMPLE OF GOOD PRACTICE

Cybercrime is a key area where national legislation and policies are critical. 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 means to combat cybercrime. The result is legislation that is largely adapted to the fight against crime in accordance with many fundamental principles, although weaknesses persist in both respects. Algerian law accommodates most of the provisions of the Budapest Convention, in some cases with alternative wording. It includes the following offenses: fraudulent access and retention in a system; capture of communications and words spoken privately or confidentially; deletion or modification of data contained in the system following fraudulent access or retention; alteration of the functioning of a system following fraudulent access or retention; 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 in line with current cyberspace challenges

In drafting and adopting national legislation on cyberspace and cybersecurity (be it by updating existing legislation or creating a new one), law- and policymakers need to keep in mind a number of current challenges.

Firstly, progress of innovation in cyberspace is much faster than national legislative processes. Therefore, even the most modern pieces of cyber legislation can – and likely will – lag behind the latest technologies. Secondly, legislating on cyberspace 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 swift progress in technology innovation stands in stark contrast with slow and often protracted national legislative processes.[7] For this reason, a lot of technologies and cyber tools are being used without necessary regulation. A typical example of such regulatory vacuum is the use of artificial intelligence (AI). While a large majority of states has not managed to adopt appropriate legislation on the content regulation

by social media companies employing human content moderators, AI-powered tools

6 African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (2017) https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2-1.pdf

7 European Court of Auditors, Challenges to effective EU cybersecurity policy – Briefing Paper, (2019): 18.

are already being deployed to replace humans in this job[8].

Nevertheless, states shall avoid legislating in a fast and uncoordinated manner. Although the public concerns related to the speedy technological progress might constitute a political incentive to adopt legislation in order to demonstrate the competence and reactivity of state institutions, a large number of swiftly adopted norms can be more disruptive than letting private companies operate without complete 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 deliberative process encompassing all stakeholders, including the private sector and civil society.

Moreover, when adopting legislation on the matter, states shall avoid being overly prescriptive as this might impede the process of innovation and research as well as disincentivize smaller ICT companies on the market that might be unable to fulfill high standards of over-prescriptive legislation. This said, when deciding whether to legislate on a specific cyber-related matter, states shall consider other options beyond legislation: for example, sometimes adoption of voluntary codes of conduct or set of non-binding guiding principles might fulfill a desired regulatory objective. Also, such soft law instruments are easier to amend and thus more apt to reflect the latest trends in technology.

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

EXAMPLES OF GOOD PRACTICE

In Ghana, specific regulations for banking and financial institutions - which form the sector most affected by cybercrime – were adopted by a 2018 Cyber Security Directive for Financial Institutions of the Bank of Ghana. The Directive requires active involvement of senior executives and the board to strengthen cybersecurity. All banks in the country are required to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cybersecurity issues, and also formulate adequate measures to manage cyber and information security risks.

(Source: https://www.bog.gov.gh/wp-content/uploads/2019/09/CYBER-AND-INFORMATION-SECURITY-DIRECTIVE.pdf)

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

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

Good Practice 3: Governments should enhance cyber expertis.

Lack of IT expertise and knowledge in the public sector is another serious obstacle for states in adopting legislation on cyber-related issues.[9] The only solution to this problem is that states should find ways to accumulate more subject-matter expertise. There are many ways to how this objective might be attained, the most straightforward being for a state to employ necessary number of IT experts. However, states tend to have much more limited financial and other resources than private ICT companies and might face problems in attracting and retaining experts on such high-profile issues as cybersecurity, AI or data analytics.

A partial remedy might be via alternative regulatory schemes, which would offer access to private sector expertise by letting it participate to some extent in the regulatory process but without removing the state's overall responsibility. Given that private companies have a high-level expertise and necessary know-how on the issues pertaining to cyberspace, the rules adopted in cooperation with the private sector may overcome a traditional gap between advancement of technology and national legislations. In addition to this, such co-regulatory schemes might be much less politicized than national legislative processes alone.

9 Raymond, Mark. "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot." Strategic Studies Quarterly10, no. 4 (2016): 137, (http://www.jstor.org/stable/26271532).

EXAMPLES OF GOOD PRACTICE

National cyber expertise has been increased in 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 Center provides an environment for firms to experiment and test their cybersecurity capabilities. It also provides educational facilities to develop cybersecurity professionals. A similar center 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 cybercrimes and create economic opportunities. The country's Economical and Financial Crimes Commission (EFCC) announced in October 2009 that it shut down about 800 websites associated with cybercrimes and arrested 18 cybercrime gangs. The EFCC noted that "smart technology" provided by Microsoft helped.

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

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

Protection of privacy and personal data is essential for cybersecurity and is an area with a concrete progress being made in terms of implementation when it comes to the right to privacy and protection of personal data, 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 with objectives of giving control to individuals over their personal data. This Regulation has also spawned a number of privacy and data protection laws on the national level.

In 2014, the African Union adopted the Malabo Convention on cyber security and personal data protection (see Chapter 3). However, the Convention has not entered into force yet. 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 arena. Although only a handful of African nations have directly signed it or been invited to accede, it has been used as a guiding framework for the creation of the African Union's Convention on Cybersecurity.

10 Nir Kshetri, Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, (2019), 77-81, DOI: 10.1080/1097198X.2019.1603527 (Sajber kriminal i sajber bezbednost u Africi, Žurnal za rukovođenje globalnom informativnom tehnologijom)

EXAMPLES OF GOOD PRACTICE

In Kenya, a new data protection bill was tabled for review in the Parliament in November 2018. The bill incorporates many elements of Europe's General Data Protection Regulation (GDPR). For instance, the bill requires organizations to inform users about the reason for collection of their data, the purpose data will be used for and for how long the organization will store them. The bill also includes a provision giving consumers the right to request organizations delete their data. In addition, it requires organizations have a certain level of security standards for storing 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 law in line with the EU's General Data Protection Regulation (GDPR). Building on the French Data Protection Act of January 1978, the 2018 Law expands the data protection authority of the Commission national de l'informatique et des libertés (CNIL), empowering it in the following ways:

• Increased regulatory authority to implement security regulations, codes of conduct, and develop reference documents and recommendations. Furthermore, the CNIL will have the power to approve certifying bodies as well as the authority to certify as per the GDPR and the French national law products, persons and procedures.

• Oversight powers are strengthened, allowing CNIL agents to make requests for any documents not protected by legal privilege. Additionally, CNIL agents are allowed to use new types of sanctions and administrative fees have been significantly raised. In case a company fails to protect personal data, fees can go 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)

Dobre prakse 5: Governments should develop and update laws protecting critical infrastructure.

Critical Infrastructure Installations, also known as CIIs, are essential to well-being of the general population. CIIs are assets, systems, networks (both physical and virtual) that are essential for vital societal functions, including health, security, and economic and social well-being, and disruption or destruction of which would have a significantly negative impact on the population.

Examples of critical infrastructure installations include:

- Power plants
- Water and Food supplies
- Public Safety: security forces, emergency organizations, civil defence
- Public Health: hospitals and medical care, laboratories
- Public Administration
- Transport (e.g. road, rail and air transport)
- Waste Disposal (waste and wastewater)
- Financial Services (e.g. banking, insurance companies)
- Information and Communication Technologies networks

A significant proportion of critical infrastructure installations (CII) have incorporated 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 weaknesses that might have devastating effects on the local population.

States have a duty to protect CIIs from cyber-attacks within their respective borders. Protecting CIIs from cyber-attacks should be a priority issue in a state's cybersecurity strategy. To this end, states need to develop and implement cyber defence measures protecting vulnerable areas in CIIs information systems. These measures should be able to detect, defend against, and neutralize cyber-attacks.

EXAMPLES OF GOOD PRACTICE

The Parliament of South Africa, in March 2019, adopted CII legislation aiming, inter alia, to provide for identification and declaration of infrastructure as critical infrastructure; provide for guidelines and factors to be taken into account to ensure transparent identification and declaration of critical infrastructure; and make sure measures are put in place for the protection, safeguarding and resilience of critical infrastructure. The legislation also establishes the Critical Infrastructure Council and gives the interior minister a discretion to declare certain installations 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 laws, policies and strategies to regulate cyberspace and meet current challenges in cyberspace, including areas of privacy and personal data and critical infrastructure protection.
- Increasing cyberspace expertise through education and knowledge sharing, particularly through Private-Public Partnerships (PPPs) is essential for good cybersecurity governance.

Resources

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

Cybersecurity Policy Framework. A Practical guide to the development of national cybersecurity policy. Microsoft (2018).

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

African Union Commission and Symantec, Cyber crime and cyber security trends in Africa Report (2017). https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2-1.pdf

CHAPTER 5
NATIONAL CYBER SECURITY STRATEGIES

OBJECTIVES

This chapter seeks to provide users of this guide with an introduction to national cyber security strategies (NCSS). It specifically aims to increase users' knowledge of NCSS's main elements and share examples of good practices.

The learning objectives of this chapter are the following:

- Increased knowledge of national cyber security strategies in general.
- Increased knowledge of main elements of a national cyber security strategy.
- Increased awareness of available resources supporting national law and policy-makers in developing national cyber security strategies.

Introduction

Since its advent, cyberspace has provided a variety of opportunities for economic, technological and social development. However, at the same time, transnational threats – such as state-sponsored cyber espionage, military cyber activities, cybercrime, cyber terrorism and terrorist use of Internet – have been on the rise as well. When these security risks associated with or facilitated by cyberspace are not appropriately covered by comprehensive strategies and action plans, States fail to protect national and human security or maintain economic growth.

In response, states around the world develop and adapt strategies to address this evolving security threat landscape, including adoption of new or amending existing national security policies. National security policies focusing on the threat landscape in cyberspace are called national cyber security strategies (NCSS).

NCSS can take various forms and, depending on a country's cyber-readiness, vary on the level of detail. Having in mind that NCSSs are context-specific, it is not possible to have a blueprint for an effective NCSS. Nevertheless, we can identify a set of strategy priorities that are integral part of most NCSSs. These are regulatory frameworks, protection of critical infrastructure, international cooperation, and public-private collaboration, as well as research and development.

While there is no commonly agreed definition of a NCSS, the International Telecommunications Union (ITU), defines a national cyber security strategy 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 cyber security of the nation and their respective roles and responsibilities.
- A description of the steps, programmes and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience[1].

As cyber threats are evolving fast, the scope of NCSS has been following up, from solely protecting individuals and organizations actors to safeguarding society as a whole.

NCSS seeks to achieve two interrelated objectives:

1. Strengthening cybersecurity for the benefit of the Internet economy so that it can further drive economic and social prosperity, and
2. Protecting cyber-reliant societies from cyber-threats.

1 ITU, Guide to developing a national cybersecurity strategy, 2018, p. 13

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

Good Practice 1: National Cyber Security Strategy is embedded in a broader national security policy of a Government.

NCSS should be seen as an additional tool to achieve strategic national priorities. Therefore, it is important that a country considers NCSS a part of its general security strategy. This further contributes to a comprehensive approach to national security.

Incorporation of cyber security, as an important element in a national security strategy and vice versa, demonstrates that a Government understands cyberspace makes a critical part to practically every aspect of national security.

EXAMPLES OF GOOD PRACTICE

The Swedish national cyber security strategy states that its strategy 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 follows for the implementation of its national cyber security strategy the principles and procedures established in the Security Strategy for Society.

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

When developing a comprehensive NCSS, it is important to translate a country's vision and objectives into concrete actions that ultimately contribute to achieving the goals and objectives identified in the first place.

The following NCSS lifecycle, developed by the ITU, aims to help guide user's strategic thinking on a national level.

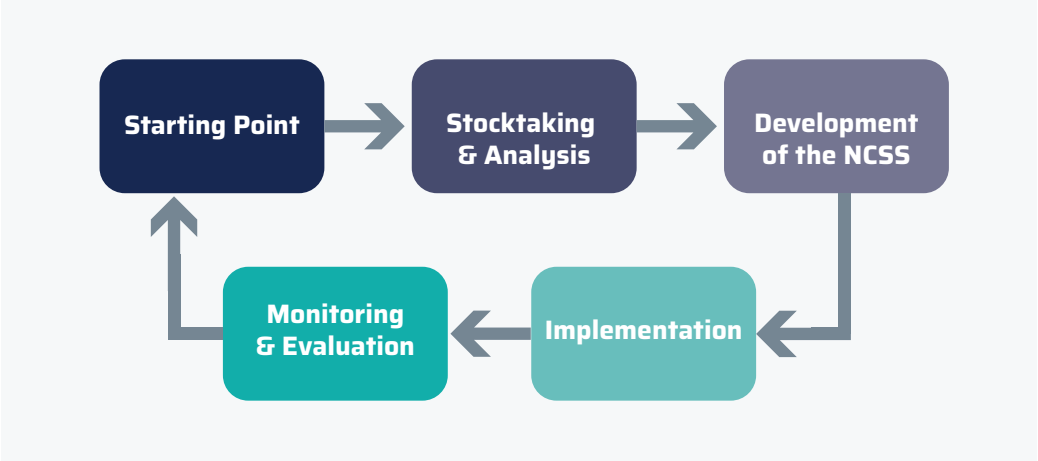


Figure 1: Lifecycle of NCSS based on the ITU Guide to developing a national cybersecurity strategy

Before developing a NCSS, it is essential that a Government identifies the objectives and purpose of such a strategy and clearly articulates its vision in the context of cyber security.

CASE STUDY: OAS TECHNICAL ASSISTANCE MISSION TO MEXICO

In 2017, the Organization of American States (OAS), through its Cyber Security Programme, and upon request of the Government of Mexico, convened a commission of international experts to share best practices with Mexican entities to understand the current state of cyber security in Mexico, to identify the current state of cyber security maturity as well as to advance a national cyber security framework.

Experts in the commission hailed from the private sector, other governments, the technical community, international organisations, 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: Drafting National Cyber Security Strategy should be steered by a lead authority and involve a wide range of stakeholders.

In order to start with developing a NCSS, a lead authority should be identified. This can either be a pre-existing entity or a newly established agency. One of the key responsibilities of this lead authority should be to coordinate the process in a neutral manner. It should be responsible for identifying key stakeholder involved in the development of NCSS and ensuring continuous exchanges with stakeholder to ensure that pertinent knowledge and expertise have been utilised in the process itself. In

addition, the leading authority should also be in charge of defining and stipulating clear roles and responsibilities of respective key stakeholders.

CASE STUDY: CHILEAN INTER-MINISTERIAL COMMITTEE

In Chile, an inter-ministerial committee consisting of the Ministry for Interior and Public Security and the Ministry of National Defence steered the process of developing a national cyber security strategy.

This inter-ministerial committee organised and coordinated working group sessions corresponding to topics identified for the national cyber security strategy. The different subjects of the working groups were: information infrastructure, prevention and sanctions, education and awareness raising, cooperation and international relations, institutionalisation. Permanent members of these working groups were the under secretariats for interior, defence, general presidency, justice, economy, telecommunications and national intelligence agency.

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

While it is a truism that the private sector plays a special role in ensuring cyber security, cooperation between public and private sector is not always institutionalised.

Public-private cooperation is furthermore important for critical infrastructure protection, as most critical infrastructure is owned and operated by private entities. Hence, they should be actively involved in the planning process aimed at protecting national critical infrastructure against cyber threats.

Involving as many stakeholders as possible in the process of developing a NCSS is essential to promote ownership of the strategy. Ownership is critical in the implementation phase. In addition, including all relevant stakeholders further ensures that they contribute with their expert knowledge to a higher success rate.

EXAMPLES OF GOOD PRACTICE

In order to ensure the optimal outcome of its NCSS, the UK had an open consultation process available on its website for everyone to provide feedback on the strategy.

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

The Canadian government initiated an online public consultation process that sought the views of Canadians, the private sector, academia, and other informed stakeholders on the cyber security landscape in Canada. A report of this review process has been published accordingly and made available online.

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

The UK Cyber Security Strategy states that achieving the goal of a safe, secure internet will require everybody, the private sector, individuals and government to work together. Just as we all benefit from the use of cyberspace, we equally have responsibility to help protect it.

While public-private partnerships are the most common format of institutionalising cooperation between the public and the private sector, challenges remain. Especially as per the mandate of a public-private partnership, lack of clarity regarding roles and responsibilities, mistrust between the stakeholders, obstacles in information-sharing, lack of incentives for working together, and a lack of effective oversight and hence accountability.

Typical mechanisms to involve different stakeholders may take the form of committees, round-tables, workshop, expert interviews, consultations, etc.

CASE STUDY: IDENTIFYING RELEVANT STAKEHOLDERS

While not all stakeholders need to be involved in every discussion, it is important to identify the relevant stakeholder that have a direct interest and expertise and hence can contribute to the discussions.

The following provides a list of relevant stakeholders in the development of a NCSS. Although the list is non-exhaustive, it should nevertheless provide a good overview of the relevant stakeholders.

- **Government:** relevant ministries (ICT, Economy, Communications, etc.), regulatory agencies, judiciary and law enforcement, defence and security services.
- **Private sector:** ICT companies, information security companies, business association.
- **Civil society:** interest-driven groups (such as human rights or child online protection), identify-based groups (faith, minority, women's rights), civil society organizations networks.

- **Academia:** universities, research entities, think tanks, independent researchers.
- **Technical community:** Computer Emergency Response Teams, Computer Security Incident Response Teams, domain name system standardisation organizations.
- **IOs:** regional and international organizations (such as AU, OSCE, OAS, CoE), international institutions (e.g. World Bank, ITU).

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

Good Practice 3: Drafting National Cyber Security Strategy should incorporate country's cybersecurity strengths and weaknesses.

As a next phase in the development process, it is important to note that the cyber security landscape in a specific country should be assessed and analysed in order to identify country's cyber security strengths and weaknesses. As a part of this stocktaking, national regulatory framework (including laws, regulations, policies and programmes related to cyber security), national critical infrastructure and public-private partnerships, as well as technical and institutional capabilities used to prevent cyber security risks (such as Computer Emergency Response Teams) and protect against cyber security threats (such as data protection officers) should be mapped and analysed.

Stocktaking and analysis process assesses the cyber maturity level of a country to further ensure that a NCSS is tailored to actual needs of the country.

CASE STUDY: CYBER SECURITY CAPACITY MATURITY MODEL, GHANAIAN MINISTRY OF COMMUNICATIONS

The cyber security capacity of Ghana was assessed through the Cyber Maturity Model developed to support the review of cyber security capacities in Ghana in relation to five dimensions:

- Cyber security policy and strategy
- Cyber culture and society
- Cyber security education, training and skills
- Legal and regulatory frameworks
- Standards, organisations and technologies.

The objective of this assessment was to enable the Ghanaian government to gain a better understanding of its strengths and weaknesses with regard to cyber security, and consequently increase effective investment into capacity building.

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

Building on this assessment, a NCSS can be developed under the lead of a dedicated authority and with extensive engagement of key stakeholders. Ideally, working groups are established to draft specific sections of the NCSS subject to the working group's relevant expertise. A good practice implies, that before adopting a NCSS, there is a review process of the NCSS, in form of online consultation or workshop, amongst as many stakeholders as possible. This will contribute to ensuring that the NCSS is based on a shared vision.

Depending on a concrete adoption process in place, either the parliament or the government are authorised to adopt a NCSS. The adopted NCSS should be published in an official gazette or on a ministry's website, to ensure that the population is aware of its existence and content as well as the Government's priorities concerning cybersecurity, and can actively contribute to achievement of strategic priorities identified by the respective strategy.

There is no single approach when it comes to structuring the drafting process of a NCSS. Good practices will differ depending on the scope of the NCSS, the range of stakeholders involved, and the available technical requirements.
In Chile, Kenya, and Mexico the draft version of the NCSS was also published online to allow different stakeholders provide comments thereto and create ownership.

Good Practice 4: NCSS incorporates following strategic priorities: enhanced governmental coordination at policy and operational levels, reinforced public-private cooperation, improved international cooperation, and respect of fundamental rights.

Most NCSSs underline importance of international cooperation for promoting cyber security and the need for creation of more effective alliances and partnerships with like-minded countries, including capacity-building. In addition, most NCSSs recognise the respect of fundamental rights, in particular the right to privacy and freedom of expression and opinion, as well as free flow of information, as indispensable for a secure cyberspace.

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

EXAMPLES OF GOOD PRACTICE

Canada's national cyber security strategy reflects Canadian values such as the rule of law, accountability and privacy.

(Source: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/canadas-cyber-security-strategy/@@download_version/5a41f8f967154454a13d71acc40a8f28/file_en)

Malawi's national information and communication technology strategy underlines that the Government will continue to provide a conducive environment for both public and private sector participation in the development, deployment and utilization of ICT in both urban and rural communities.

(Source: https://www.macra.org.mw/?wpdmpro=malawi-ict-policy-2013)

Good Practice 5: Identify national critical infrastructure to be incorporated in NCSS.

Identifying national critical infrastructure is essential for developing policies on how to protect the latter from cyber threats. Without a clear definition and list of what constitutes critical infrastructure, it is difficult to secure these critical assets from cyber risks.

An increasing proportion of critical infrastructure depends on information communication technology in order to operate and function. Protecting national critical infrastructure from cyber threats is vital since it may have worldwide effects – consequently, it is commonly included as a priority in national cyber security strategies of many States.

An increasingly growing number of States therefore identify their national critical infrastructure. The majority identifies water, electricity, hospitals, as national critical infrastructure.

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, this European Union 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 Bill lists factors to be taken into account in declaring of critical infrastructure. These factors are for instance: the sector in which the primary functions of such an infrastructure take place; the strategic importance, including the potential impact of destruction, disruption, failure or degradation of such an infrastructure or the interruption of a service which might affect the South African Republic's ability to function, deliver basic public services or maintain law and order; the risk category of such an infrastructure; the resources available to the person in control of the infrastructure; the effects or the risk of a destruction, disruption, failure or degradation of such an infrastructure; the size and location of any population at risk; historic incidents of destruction; the level of risk or threats to which such infrastructure is exposed; special characteristics or attributes of such an infrastructure; the extent to which the declaration as critical infrastructure will promote the interests of the public; and any other factors which may be determined by the Minister.

Source: https://pmg.org.za/bill/644/

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 for example.

Source: http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf

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

Source: https://www.babs.admin.ch/fr/aufgabenbabs/ski.html

Good Practice 6: National Cyber Security Strategy provides an implementation and R&D plans.

A NCSS is only as effective as its implementation. Therefore, the effective implementation of a NCSS relies on adoption of an implementation plan (sometimes also referred to as action plan) to turn the strategy into concrete actions and policies, by coordinating efforts and resources.

A crucial part of an implementation plan is development of key indicators to monitor and evaluate the success of the NCSS. In the monitoring process, the government should ensure that the NCSS is implemented in accordance with its action plan. In the evaluation phase, it should assess whether the NCSS is still reflecting its objectives and priorities – and if not, to reassess these.[2]

An implementation plan should furthermore include the establishment of an incident reporting mechanism and work out how to raise peoples' awareness of risks and threats in cyberspace. Reporting computer security incidents plays an essential role in enhancing national cyber security overall. Such reporting contributes to adjusting and tailoring the list of cyber security measures to the changing threat landscape. A necessary prerequisite for reporting is cooperation between the public and the private sector. Hence, confidence and trust are vital to support open information sharing with regards to risks and threats in cyberspace. Establishing a computer incident response team (CSIRT) is considered to be a cornerstone in effectively coordinating incident management.

In order for an implementation plan to be effective there needs to be awareness-raising initiatives as regards the individual user and her / his knowledge about cyber security threats and vulnerabilities. This is vital to ensure that the individual user knows how to protect herself / himself from risks in cyberspace that can potentially affect the national cyber security of a country.

Investing in and fostering Research & Development (R&D) is furthermore essential for developing new tools for deterring, protecting, detecting and adapting to and against all kinds of cyber threats.

2 ITU Guide on developing a cybersecurity strategy, p. 26

EXAMPLES OF GOOD PRACTICE

Kenya's NCSS sets the following objective "[t]he 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." (p. 4)

Nigeria's national cyber security strategy identifies the individual user as the weakest link within the cyber security chain. Therefore, the strategy provides "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 ICT policy is also monitored and evaluated for effectiveness and responsiveness on an annual basis or as may be determined. (Source: Malawi, National ICT Policy, 2013, p 11)

The National Cyber Security Strategy of Mauritania includes in the policy a detailed implementation plan for the policy itself. (Source: Maurétanie, Stratégie Nationale de Modernisation de l'Administration et des TICs 2012-2016)

Poland's national cyber security strategy identifies increasing user awareness on the methods and safety measures in cyberspace as a critical component of its strategy (Poland, National Cyber Security Strategy, 2013)

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

Good Practice 7: Provide sufficient resources to develop cyber security awareness-raising campaigns aimed at the public following on the implementation of a NCSS.

Everyone on Internet – from a Government official, business owners, the financial and trading sector, to the public as well as children – is vulnerable to cyber security threats.

Generally, there is a common understanding that cyber security is a not responsibility of a single agency, entity or individual but a shared responsibility of everyone connected to the Internet or using applications that are linked to this online realm.

According to the Organization for 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].

Everyone can be effected by various kinds of cybercrime, it is therefore a paramount to educate the public on the risks and threats in cyberspace.

CASE STUDY: OAS CYBERSECURITY AWARENESS CAMPAIGN TOOLKIT – SITUATION ANALYSIS

A good understanding of the current context as regards the cyber security threat landscape is paramount to developing a successful awareness raising campaigns.

In this respect the OAS developed some guiding questions that seek to help to analyse a 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?
- 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 2016, available at https://thegfce.org/wp-content/uploads/2020/06/2015-oas-cyber-security-awareness-campaign-toolkit-english-1.pdf

3 OAS (2016) : Cybersecurity Awareness Raising Toolkit, p8, available at 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, target-specific, and planned and developed in a multi-stakeholder process, involving Government officials, private companies such as internet service providers, telecommunications companies, etc.), as well as civil society representatives, such as non-governmental organisations, the media and academia.

EXAMPLES OF GOOD PRACTICE

In 2015, Jordan passed a law on combating cybercrimes and a specialized unit "Cyber-Crime Unit" was established. This Cyber Crime Unit, assisted by 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

KStaySafeOnline which is powered by the National Cyber Security Alliance seeks to encourage a culture of cyber security. To this end, it published on its website an infographic on how to make certain that everyone in a household – 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

- In order to meet current and emerging cyber security threats, States have to continuously monitor and adapt their national cyber security strategies to the evolving threat landscape.
- It is essential to set specific objectives and strategic priorities for a national cyber security strategy to be successful.
- Cyber security strategies should recognise the respect of fundamental rights, such as privacy and freedoms of expression and belief, as well as the free flow of information in order to promote a free and open cyberspace.
- Cyber security has an impact on a large number of different sectors and across different public agencies. Therefore, close cooperation between all governmental authorities as well as with the private sector is an important pillar of successful implementation of a national cyber security strategy.
- In order to develop new tools for deterring, protecting, detecting and adapting to and against new kinds of cyber threats, governments should invest more resources into Research & Development.
- In order to protect national critical infrastructure from cyber threats, it is important to define what is considered to be “national critical infrastructure” in a given context.

RESOURCES

ITU Guide to National Cybersecurity Strategies, available at https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018

https://www.enisa.europa.eu/publications/ncss-good-practice-guide

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

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

Organization for American States, Cybersecurity Awareness Campaign Toolkit, 2016, available at 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 seeks to provide users with an overview of strengths and challenges pertaining to private-public partnerships in cyberspace, between law enforcement agencies and private companies in particular when investigating crimes and unlawful content on Internet.

Learning objectives of this chapter are the following:

- Increased knowledge of concepts of multi-stakeholder initiatives and public-private partnerships.
- Increased awareness of cooperation between law enforcement agencies and private companies.
- Increased understanding of elements needed for creation of effective multi-stakeholder approaches to cybersecurity.

Introduction

Cybersecurity is a cross-sectional area, and therefore a common objective of every National Cyber Security Strategy (NCSS) is collaboration between public and private cyber actors in order to enhance cybersecurity. Multi-stakeholder approaches on cyberspace and cybersecurity, also referred to as Public-Private Partnerships (PPPs), are becoming increasingly vital to cybersecurity governance, partly due to an important role played by private companies and transnational characteristic of cyberspace itself. Effective cooperation among all stakeholders – notably governments, the ICT sector, academia, and civil society – has become an essential element of implementation of international standards and norms and effective NCSS.

Ever increasing efforts in relation to cybersecurity combining the public, public-private and private mechanisms are symptomatic of a more fundamental shift in the way business is carried out on a global scale. In light of this trend, cooperation across a variety of stakeholders – states, business and civil society – can be seen as a pragmatic response to fill certain governance gaps found in traditional regulatory approaches. Indeed, such initiatives aim to support effective governance by ensuring commercial actors operate within a framework of rule of law and respect for human rights. Groups composed of diverse stakeholders can together craft better approaches and solutions than one stakeholder group alone.

1. Understanding public-private partnerships

Overview

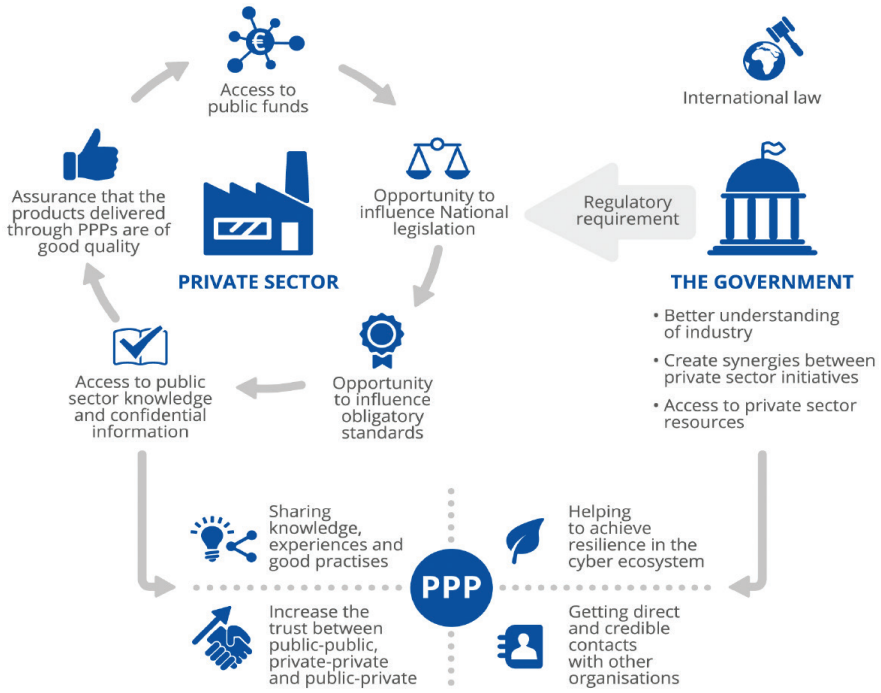
Public-Private Partnerships imply sharing of resources (assets, skills, expertise, and financing), risks and rewards among stakeholders. In the area of cybersecurity, PPPs signify collaboration between government and public institutions on one side and ICT industry, academia, and civil society on the other in order to increase cybersecurity awareness, mitigate cybersecurity risks, and ensure robust national cybersecurity capabilities. This cooperation is multi-faceted and may involve enhancing cyber defence capabilities 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 increasing cybersecurity awareness or ensuring robust national cybersecurity capabilities.

PPPs can be beneficial to cybersecurity for a number of reasons:

- To encourage improvement of cybersecurity awareness and understanding across organisations and throughout society;
- To improve a national pool of cyber skills through creations of initiatives designed to identify, inspire and enable more people become cybersecurity experts;
- To endow cybersecurity professionals with required financial and technical resources, through dedicated initiatives;
- For research and development in the sphere of cybersecurity;
- For crime and fraud prevention;
- For cyber security certification and accreditation;
- To connect and foster collaboration between public and private entities dealing with cybersecurity.

PPPs in the cybersecurity area can be categorized in line with the following four types:

- Institutional PPP: formed under a legal act linked with critical infrastructure protection. They usually cooperate via working groups, rapid-response groups and long-term communities.
- Goal-oriented PPP: created to build a cybersecurity culture through a platform or a council bringing private and public sector together to exchange knowledge and good practices. It focuses on one subject or a specific goal.
- Outsourced cybersecurity services: created when governments fail to effectively address private sector needs they have identified. These PPPs act as an autonomous third party, but actively address needs of the industry and support the government in policy-making or implementation.
- Hybrid PPP: Computer Emergency Response Teams (CERTs) operating under a PPP framework. Governments assign these PPPs with a task of delivering CERT services to the public administration or the whole country.



Reasons and incentives for Public-Private Partnerships

Source: Public-Private Partnerships in Cyberspace, ENISA, November 2017, p. 14

2. Roles of governments and other stakeholders

A Key Role of Public Institutions in Multi-Stakeholder Collaboration

VGovernments hold a primary responsibility for development of effective NCSS. Law and policy-makers are thus responsible for creation of adequate framework in compliance with state's obligations under international and national legislation. Governments engage with private actors such as ICT companies to ensure that co- and self-regulation is consistent with international human rights law and national law as well.

Beyond this purely legalistic approach, governments can play an important role in coordination and engaging with the ICT sector and civil society by creating and supporting collaborative platforms. These are of a particular relevance to national referral units, which search for and flag 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. In addition, open communication channels among relevant stakeholders help identify and fill in critical gaps in cybersecurity, and prevent from

potential conflicts of interest. Institutionalised and coordinated efforts can also promote complementary actions of, and better channelling of human and financial resources among stakeholders.

CASE STUDY: COMPUTER EMERGENCY RESPONSE TEAMS

Computer Emergency Response Teams (CERTs) are units of experts mandated with aiding individuals or institutions that fall victim to a cyberattack. Their main tasks are to identify hostile malware and prevent it from spreading further in the network while mitigating the consequences of the attack. Such units are often incorporated within private companies or public institutions but may also exist on a national level as separate government agencies offering their assistance to a wide range of private and public entities.

Although national CERTs are public agencies, they represent a good example of public-private cooperation. The basic function of every CERT is to provide 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 a public online form. In addition, some national CERTs offer mobile teams that can be dispatched to an institution requiring assistance in the event of cyberattack.

Cooperation between the private and public sectors is essential for maintaining a stable and secure cyber environment. Public institutions cannot secure cyberspace on their own for two main reasons. Firstly, the private sector drives the innovation in the field and controls most of cyberspace. Secondly, even state-owned and state-controlled critical cyber infrastructure relies heavily on products and services of private companies for their protection.

Moreover, governments are obligated to respect and protect human rights of their citizens online and must therefore ensure that any actions by private companies and national CERTs are not in violation of human rights, especially the right to privacy and free expression. To fulfil this aim, CERTs should be independent from political influence and should not serve as governmental instruments to infringe upon computer system and network privacy or the privacy and secrecy of communication.

When establishing national CERTs, governments should keep in mind the human dimension of cybersecurity in all its three aspects: confidentiality, accessibility and integrity. One therefore has to understand that cybersecurity is, at its core, not about securing networks but about enhancing human security. As to the protection of confidentiality of information, the right to privacy should be a guiding standard of all operations protecting and enhancing confidentiality of data. As far as accessibility of data is concerned, it is essential that freedom of expression and information is respected and protected.

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

CASE STUDY: INTERNET REFERRAL UNITS AT THE EU AND THE NATIONAL LEVEL

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

- To support the competent 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 removal of internet content used by smuggling networks to attract migrants and refugees;
- To swiftly carry out and support the referral process, in close cooperation with the industry[2].

According to the EU IRU's transparency report in 2017, "cooperation with the private sector is fundamental in prevention".[3] Since its establishment in July 2015 until December 2017, the EU IRU has assessed 46'392 pieces of terrorist content that triggered 44'807 decisions for referral with a 92 percent rate of content removal.[4]

As outlined in the transparency report and in the EU IRU's mandate, the IRU is responsible for assessing online content and referring it to the respective ICT company hosting the content for removal. As such, the EU IRU focuses on content published by Al-Qaeda and Daesh and affiliated groups and assesses this content against Europol's mandate, in accordance with the principles set out in the EU Directive on combatting terrorism. The EU Directive on combatting terrorism provides safeguards with respect to content removal outlined 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]

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
5 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017L0541

In case the assessed content infringes Europol's mandate, the relevant content is referred to the ICT company on whose platform the content has been detected. Nevertheless, eventually it is left to the discretion of the company to remove this flagged content or not, after assessing it against its respective terms of service. The EU IRU has no legal power to take down content.

Similar referral units exist in the UK, France and the Netherlands, with statements by Europol indicating that parallel mechanisms have been established in Belgium, Germany, and Italy.[6]

In addition, the EU IRU organizes so-called joint Referral Action Days with ICT companies such as Google, Twitter and Telegram. The joint Referral Action Days bring together specialised law enforcement units from multiple national IRUs and the EU IRU and ICT Companies. The law enforcement specialists assess several hundred pieces 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 respective ICT company in attendance, which reviews the detected content against its own terms and conditions. The final decision to remove the content detected remains with the company. The joint Referral Action days promote a coordinated approach between governments and ICT companies in addressing violent extremist and terrorist content on the Internet.[7]

ICT Industry & Civil Society-led Initiatives

ICT companies quite often face co- and self-regulation challenges in relation to their platforms, particularly when it comes to protecting human rights, such as freedom of speech and the right to privacy. These challenges are exacerbated by the fact that social media platforms have become essential tools for society to discuss, share, and access information. In response, ICT industry-led initiatives such as knowledge and technology sharing between companies; creation of platforms for interactive content-moderation tools and resources; and training sessions run by larger companies for smaller ones on content removal approaches, can be effective tools for strengthening cybersecurity.

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

The International Association Of Internet Hotlines has a global presence in 43 countries and seeks 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 consists of 48 hotlines that provide a mechanism to the public to report content or activity online that is suspected to be illegal. INHOPE divides illegal activities into two different categories: criminally illegal activity that is investigated and prosecuted by Law Enforcement, which INHOPE hotlines focus on, and civil illegal activity that can be prosecuted by civilian bodies.

INHOPE's primary focus is child sexual abuse material, including online grooming but it also includes hate speech and xenophobic content online. While INHOPE does provide a definition for hate speech, it also acknowledges that hate speech is an "extremely complex" matter that is often not illegal under criminal law. Therefore, each report to a hotline concerning hate speech is assessed against national legislation, i.e. where the respective content is hosted.[10]

All anonymously reported content is reviewed by a Hotline Content Analyst to assess if the material is illegal. If the Hotline Content Analyst considers the reported content illegal, the location of this content will be traced. If the content is hosted in the same country, the material will be reported to national law enforcement agencies and / or the ICT company for removal. If the material is hosted in a foreign country, it gets forwarded to the hotline in the hosting country.

INHOPE further developed a Code of Practice for Internet Hotline Providers outlining that INHOPE members should regularly consult major stakeholders, including governments, law enforcement agencies, ICT industry, child welfare institutions and that members ought to apply the principles of transparency, accountability, responsibility and trustworthiness.

INHOPE also emphasises the importance of staff well-being for those who review the reported content and acknowledges the psychological toll content review of child abuse and violent extremist or terrorist content can have on reviewers. A white paper, developed and published by the French hotline Point de Contact, intends to develop a common set of best practices for the operational handling and processing of harmful and potentially illegal content that may endanger physical safety and psychological well-being of professional content reviewers[11].

8 https://www.inhope.org/EN
9 https://www.inhope.org/EN/our-story
10 https://www.inhope.org/EN
11 https://www.pointdecontact.net/wp-content/uploads/2020/11/Livre_blanc_EN.pdf

3. Creating cybersecurity PPPs

Good Practice 1: An enabling environment should be established as a necessary precondition for creation of effective PPPs

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

Creating an enabling environment should include agreement by stakeholders as to the legal basis of PPP. Public institutions should take the lead in creating PPPs or national action plans. In order to do so, adequate resources should be provided for PPP-internal coordination and collaboration, and a pragmatic approach adopted to resolve challenges in coordination and collaboration. Fostering private sector participation, particularly of small and medium sized enterprises, is also an important factor for ensuring enabling environment is created, which may further promote cooperation and collaboration among relevant stakeholders. Finally, PPP stakeholders should invest in open communication with the wider public.

Good Practice 2: Clear lines of responsibility and accountability should be set in order to protect human rights

Establishing clear lines of responsibility and accountability of all stakeholders is essential for ensuring that issues such as infringements of human rights do not occur. In context of NCSS, PPPs can be uniquely problematic for a number of reasons, including reluctance of politicians to take responsibility for stricter cybersecurity legislation, coupled with the private sector's aversion to accepting responsibility or liability for national security, which leaves this partnership without clear lines of responsibility and accountability. Incorporating clearly specified mechanisms of responsibilities and accountability in PPP agreements is therefore integral to mitigating risks and ensuring all stakeholders have adequate understanding of their roles and responsibilities.

Good Practice 3: Trust between stakeholders has to be built and maintained

IBuilding and maintaining trust between public and private entities is one of the biggest challenges for PPPs. Developing and maintaining trust 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

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

both public and private sector; insufficient public sector budget and resources failing to meet private sector's expectations; and lack of understanding and dialogue between the public and private sector regarding the concept of PPPs itself.

Public agencies and private entities need to build trust on principles of openness, fairness and mutual respect. In case of PPPs, a significant trust test is information-sharing. Participants need to feel they are gaining additional pieces of information by being a part of partnerships and, at the same time, that their data are safe and secure.

CASE STUDY: GLOBAL FORUM ON CYBER EXPERTISE

The Global Forum on Cyber Expertise (GFCE) is a platform for states, international organisations 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 platform for policymakers, practitioners and experts from different countries and regions to facilitate sharing experience, expertise and assessments on key regional and thematic cyber issues. Since its launch, the GFCE's focus has shifted to becoming a coordinating platform. The initial focus areas for capacity and expertise building were cyber security, cybercrime, data protection and e-governance. In 2019, the GFCE positioned itself to facilitate and coordinate knowledge and expertise sharing for the implementation of Cyber Capacity Building. Moreover, the different GFCE working groups are moving towards developing a clearinghouse mechanism.

Source: 'History', the GFCE

KEY FINDINGS

- In cyberspace and on cybersecurity related issues, groups composed of diverse stakeholders are often more likely to be more effective than one stakeholder alone. Multi-stakeholder approaches, also referred to as public-private partnerships (PPPs), can together craft better approaches and solutions, and are becoming increasingly vital 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 coordination 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 initiatives for cybersecurity.
- Governments should invest in pragmatic approaches towards building PPPs including open communication, inclusive participation, and motivating increased private sector participation.

RESOURCES

Public-Private Partnerships in Cyberspace, ENISA, November 2017, available at https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

Public-private partnerships in national cyber-security strategies, available at 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)

Public Private Partnerships in the EU: Widespread shortcomings and limited benefits http://publications.europa.eu/webpub/eca/special-reports/ppp-9-2018/en/

African CERTs https://www.africacert.org/african-csirts/

EU IRU, available at https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru

www.dcaf.ch