EXECUTIVE SUMMARY

TOWARDS RULE OF LAW IN THE DIGITAL ENVIRONMENT

Prepared by the
NATO Strategic Communications
Centre of Excellence

The digital environment enables instantaneous, cross-border exchanges of information, which has made possible innovative business models and new ways to communicate. But the digital environment also harbours novel threats to individuals' human rights and to security interests of nations across the globe. Recognising these developments, the NATO StratCom COE organised an invite-only workshop with representatives from industry, academia, and government to discuss what regulation is needed in the digital space. We summarise the key take-aways from the workshop below.

IN ADDITION TO 'ETHICS', FUNDAMENTAL RIGHTS IS A POSSIBLE FRAMEWORK ON WHICH TO BASE COMPREHENSIVE REGULATIONS FOR DIGITAL ACTORS AND ARTIFICIAL INTELLIGENCE

The act of regulating new technologies is simpler once questions of ethics, values, and morals have been resolved, as drafting technical legislation or regulations requires clarity about the aims of the regulation. In this regard, it may be helpful to base regulations for new technologies on the concept of fundamental rights and to benefit from the institutions already developed to uphold those rights.

A similar framework that could be used as a basis for regulatory intervention is that of international human rights. The United Nations Universal Declaration on Human Rights establishes a vision of the rights to be enjoyed by all peoples across the world. And while the main signatories to the declaration have been countries, the same principles apply directly to private entities through the UN Guiding Principles on Business and Human Rights.

Particularly in the context of artificial intelligence, many entities hope to regulate this technology with private law through contractual relationships with data subjects or between organisations. Yet it can be argued that digital technologies such as AI, and content personalisation in particular, should be regulated by public law.

The power imbalance between the companies employing AI to make decisions and the data subject makes it unlikely that the terms of any interaction would be truly fair; consumers may be unable to detect when their rights have been violated, either because the technology and underlying decisions are too complex or because the technologies are used without warning or transparency. Lawmakers could also mandate that data subjects 'own' their own data and have the right to direct how other entities use it, even after the data has been collected and manipulated.

Industry has been promoting the conception of an ethics-based framework.

'Ethical technology' has long been the language used by engineers contemplating the impacts of their technologies. At the highest level, creating ethical technology means settling on ethical principles to govern the technology, but this concept lacks the robust international consensus and institutional support for both the interpretation and enforcement that undergird the international human rights framework.

MULTILATERAL AND MULTISTAKEHOLDER INPUT SHOULD INFORM COMPREHENSIVE LEGISLATION

Multilateral agreements would be the most effective at promoting human rights and the rule of law in the digital environment. Protections under national legislation vary by country, and national legislation may be difficult to enforce against foreign actors that operate in the digital world. Unless there are international agreements in place, national legislation applies to the actions of only persons registered in or residing in that country, and even when legislation applies to entities 'doing business in' a country, there is no guarantee that a government can meaningfully penalise violations of local law.

Smaller countries (whether by population or by economy) have been left in a particularly precarious situation. While a country may be of little significance in terms of revenues and user-base for a multinational company, that company may be a dominant service provider in that country and decisions made by the company may substantially impact the country's population, policy, or politics. Many countries are consequently less able to effectively regulate their internal affairs now than before the digital revolution. Even when those affairs relate to fundamental institutions, such as preserving the integrity of the democratic process or protecting the nation's vital interests against an aggressor.

In the European legal framework, the European Union and its member states have shared competence in the area of freedom, security and justice. EU member states have the obligation to maintain law and order and to safeguard their internal security. With the digital environment, member states face practical challenges in meeting their security obligations when the threats come from technologies registered and led from beyond a country's borders yet operating within them, as is allowed by EU Single market rules.

The digital environment is all-embracing, it is a successful and promising space for entrepreneurs, individual users, civil activists, states, and the free media. Accordingly, discussions focused on creating a digital environment based on rights and liabilities should include representatives of all stakeholders and should expressly consider what checks and balances are needed to prevent an abuse of power by governmental or private entities.

STANDARD LEGAL DEFINITIONS ARE NEEDED

The panellists identified practical limits on enforcement as a crucial shortcoming of existing regulations. Many laws use definitions that do not clearly apply in the digital environment, making it difficult for governments to enforce them without additional judicial interpretations. This is likely because the laws were passed before cross-border digital technologies became ubiquitous.

Policymakers and the international community need to work towards standardising the legal definitions of emerging technologies or, alternatively, revising existing definitions to accommodate these new technologies. Standard legal definitions would promote meaningful and informed debates about the societal impacts of new technologies and would lead to the development of better policies both nationally and internationally.

Common definitions for many technologies already exist,[1] but they do not always transpose neatly into legal definitions. While regulations imposed on 'social media'[2] (as defined in the footnote) would appropriately apply to businesses commonly conceived of as 'social media', they might be too restricting for other types of websites that allow users to create and share online content, including newspapers that support comments sections and e-commerce websites allowing product reviews. Overbroad definitions may place unnecessary regulatory burdens on companies, potentially hampering innovation.

In Lithuania, for example, 'social media' is presumed to be any platform where people can share and disseminate information and their beliefs. And, in its Online Harms White Paper, the United Kingdom proposed a regulatory framework that would apply to 'companies that provide services or tools that allow, enable, or facilitate users to share or discover user-generated content, or interact with each other online'.[3]

'SOCIAL MEDIA' COMPANIES ARE NOT TRADITIONAL MEDIA

'Social media' companies differ substantially from traditional media such that new or bespoke regulations are needed to address the potential harms without unnecessarily burdening individual rights or impairing innovation.

The term 'social media' implies that these entities are somehow regulated by traditional media laws that promote

[1] Merriam-Webster Dictionary: social media are 'forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)'.
[2] This report will place the term 'social media' in quotation marks because the term has no widely recognised legal meaning.
[3] Online Harms White Paper, United Kingdom, p. 49.

accountability and protect the public good. But 'social media' companies are not news, radio, or television, and are rarely subject to the corresponding regulations and liabilities for these media.

One way to solve the problem would be to update the platform immunity framework to recognise 'social media' companies as distinct actors in the media ecosystem. Two prominent examples of platform immunity laws include the United States' Communications Decency Act of 1996[4] and the European Union's e-Commerce Directive 2000/31/EC.[5] Platform immunity laws protect companies from legal claims arising from user-generated content in certain circumstances, such as when the company merely delivers or stores information at a user's request, but may not shield companies from liability in all circumstances, especially when companies exert more active control over the content on their site.

Unlike traditional media organisations, 'social media' companies do not create the content found on their sites nor do they review or edit content before it is published. In fact, 'social media' companies would likely be unusable and may not be economically viable if required to authorise every post, comment, or message. And, unlike companies that simply transport or passively store content, 'social media' companies employ sophisticated algorithms that tag, curate, organise, and emphasise user content. 'Social media' companies are neither traditional media nor passive conduits in light of the above discussion; formalising the unique activities of 'social media' companies in legal frameworks is recommended. Along these lines, the EU has recognised that 'social media' companies differ from traditional media in the amendments to the Audio-Visual Media Services Directive (AVMSD) in which the EU created a separate classification for 'video sharing platforms'.

GOVERNMENTS NEED MORE TECHNOLOGICAL COMPETENCE TO LEGISLATE AND TO ENFORCE IN THE DIGITAL ENVIRONEMENT

Governments need to become increasingly sophisticated in their understanding of cyber and digital technologies as legislators, regulators, consumers, and law enforcers. Technological competence is not the same as technical expertise. Government officials do not all need to know how to develop machine learning technologies or design a blockchain; yet they should understand—at least broadly—how such technologies function, the business models that support their existence, how they collect, use, and protect data (especially personal data), and how market power is distributed throughout the digital ecosystem.

[4] 47 United States Code § 230

[5] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Arts. 12, 14.

With a more nuanced understanding of these technologies, government officials and legislators can design thoughtful regulations, provide meaningful guidance to companies, and can, where appropriate, engage industry stakeholders as partners to solve problems.

One proposal is to create a sort of 'super regulator' to advise other governmental agencies on new technologies and the internet without directly overseeing compliance. Similar structures have been already established or considered. For example, the Computer Crimes and Intellectual Property Section (CCIPS) of the US Department of Justice advises and partners with federal prosecutors to charge and litigate computer- and internet-based crime, and the United Kingdom has proposed establishing an 'internet regulator' to advise UK agencies dealing with these issues.

LEGISLATION COULD REGULATE VARIOUS ASPECTS OF DIGITAL ACTIVITY

To minimise harms associated with the digital environment, countries could choose to regulate one or more aspects that make the most sense to supervise given their national laws, constitutions, and traditions. Various views about the pros and cons of regulating a particular aspect have been identified.

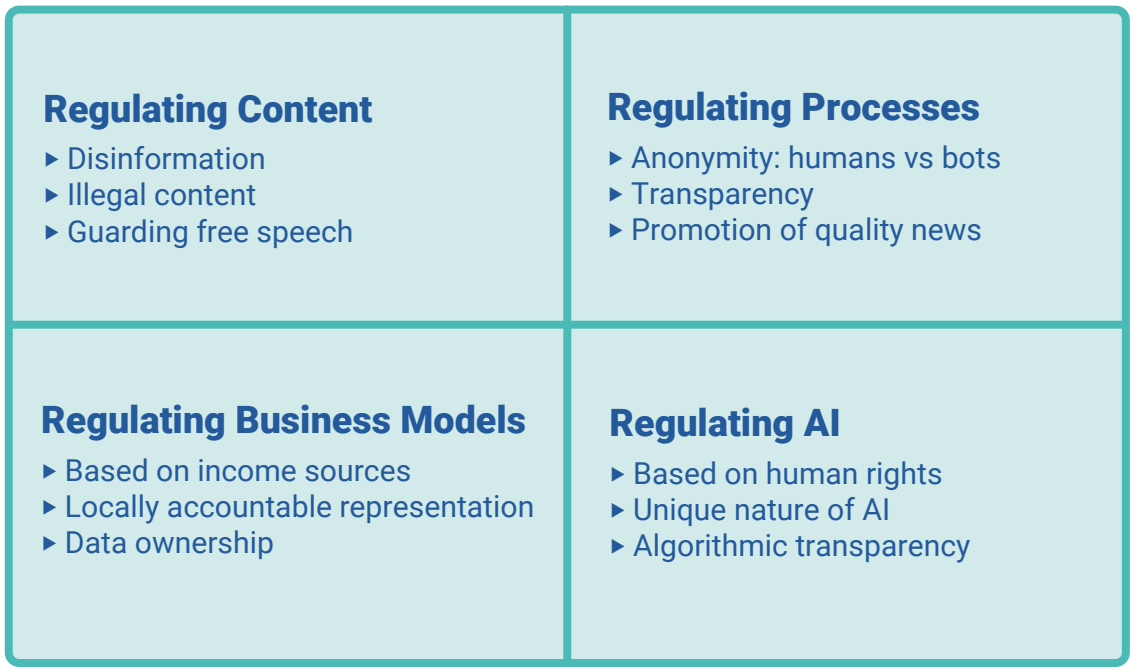
Society needs comprehensive legislation that sets out the rights and duties of 'social media' companies and other digital actors. The comprehensive approach contrasts with the current approach, which focuses on incremental and gradual adjustments to existing law in an attempt to catch up to new threats from the digital environment. One of the ideas discussed was the adoption of high-level legally binding principles that regulators specialising in certain aspects of the digital environment could flexibly apply.

- **Content regulation:** To establish the rule of law via regulating the digital content, a country should provide more guidance on the meaning of hate speech, misinformation, and illegal content, and draft legislation that clearly describes the responsibilities of 'social media' companies to moderate this content, as well as the penalties associated with failure to do so. Any legislation should ensure that human rights are protected from overzealous enforcement by 'social media' companies.

- **Processes regulation:** The activities and behaviours of digital actors online should be legislated, for instance determining when anonymity is inappropriate and requiring greater transparency in the digital business' services to users. Additional transparency is needed to protect human rights and national security interests. In order to accomplish this, national and international oversight of the operations of digital actors could be considered.

- **Business model regulation:** Regulations could be based on the harms associated with a digital actor's particular business model. For example, advertising-driven 'social media' use algorithms to achieve high engagement. Researchers are increasingly recognising these algorithms as contributing to the proliferation and distribution of extremist content. Thus certain business models may negatively impact national security and social cohesion more than others, and for that reason legislators may wish to create regulations that impose different obligations on 'social media' companies based on their sources of income. Some business models require vast amounts of personal data and, in some jurisdictions, it is clearly stated that a person owns their own data and is in control of that data regardless of which entities may have received them. Legislators may also include a requirement for digital actors to have a meaningful presence in regions where they serve a significant number of users.

- **Artificial Intelligence regulation:** Due to the rapid evolution of technology, comprehensive legal framework for AI development and application will likely be necessary as narrow regulations could become quickly outdated. A global treaty for artificial intelligence may be sought; the starting point for such a treaty could be the international human rights regime. Governments that seek to regulate artificial intelligence must acknowledge the unique characteristics of technology that complicate efforts to regulate it . Additionally, AI-based decisions frequently lack the transparency needed to confirm that rights are being respected.



THIS IS AN EXECUTIVE SUMMARY FOR THE REPORT
"TOWARDS RULE OF LAW IN THE DIGITAL ENVIRONMENT"

REPORT ISBN: 978-9934-564-52-9

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org