White Paper 16

digital challenges for international law

ADI/ILA 150 ANS/YEARS

2023 PARIS

coordinators

Anne-Thida Norodom
Professor of Public Law at University of Paris, France

Aude Géry
Postdoctoral Researcher at GEODE, University of Paris 8, France

François Delerue
Assistant Professor in Law, IE University, Spain

assistant / rapporteur

Stefanos Argyros
Research assistant at GEODE, University of Paris 8, France

steering committee

(in alphabetical order)

Eyal Benvenisti
Whewell Professor of International law and Director of the Lauterpacht Centre for International Law, University of Cambridge, United Kingdom

Nehal Bhuta
Professor and Chair of Public International Law, University of Edinburgh; Co-Director of the Edinburgh Center for International and Global Law, United Kingdom

authors informations

Duncan B. Hollis

Laura H. Carnell Professor of Law at Temple Law School and non-resident scholar at the Carnegie Endowment for International Peace, United States

Zhixiong Huang

Changjiang Outstanding Young Scholar, Professor and Vice Dean of the Law School as well as Executive Director of the Institute for Cyber Governance, Wuhan University, China

Nnenna Ifeanyi-Ajufo

Senior Lecturer of Law and Technology at the School of Law, Swansea University, United Kingdom

Eduard Ivanov

Professor of International Law at the National Research University Higher School of Economics, Moscow, Russia;

Joanna Kulesza

Professor of International law and Internet Governance, University of Lodz, Poland

Clea Strydom

Independant researcher, postgraduate student, University of Johannesburg, South Africa

Jennifer Tridgell

Senior Researcher for the UN Special Rapporteur on Freedom of Religion or Belief (External Office), Media Officer of the International Law Association (Management Committee), United Kingdom

Robert Young

Legal Counsel, Criminal, Security and Diplomatic Law division, Global Affairs Canada, Canada

Introduction

Objectives and Structure

The celebrations for the ILA’s 150-year anniversary are articulated around two guiding questions: firstly, in which international society do we want to live in by 2050? And, secondly, to achieve this international society, what international law do we need? The French branch of the ILA, responsible for organizing the celebrations, has selected a variety of subject areas through which to explore these questions, among which the challenges presented by emerging digital technologies for international law. The White Paper on Digital Challenges for International Law aims to provide an overview of existing rules and principles of international law within the fields of digital data, digital security and artificial intelligence (Part 1, Statement of facts), identify some of the main factual challenges likely to emerge in the future (Part 2, Challenges) and reflect on whether and how international law can or should be used in response (Part 3, Questions). The White Paper is not an academic exercise, but rather an attempt to highlight some of the key digital challenges of the future and their potential implications for international law.[1] Ideally, it serves to anticipate some of the international legal questions that will be raised by future technological developments, and make them intelligible to all interested stakeholders, whether or not they are specialized in international or digital law.

The Topics of the White Paper

The Committee has articulated its work on digital challenges around three interrelated topics - data, security and artificial intelligence - based on a twofold rationale: firstly, these topics encompass some of the main challenges emerging from the dawn of information and communication technologies (ICTs). At the same time, they raise a variety of legal questions on international law that are of interest to international lawyers and other key stakeholders. The committee does not aim to provide an exhaustive list of challenges. The topics are approached mostly from a public law perspective, although some private and commercial uses of emerging technologies (e.g., the com-

Note 1 Typical academic requirements, including in terms of doctrinal referencing, will thus not be met. A bibliography will be made available on the ILA 150-year anniversary website.

mercialization of data) may also be considered. Many emerging technological trends, such as the metaverse or the development of digital currencies for example, may only be discussed insofar as they relate to the three main topics identified above. Some of these new developments may also come up in the White Papers of other committees, given the prevailing use of digital technologies and their impact on a variety of international legal fields.

1. Digital Data

Digital data is undoubtedly one of the most important issues in cyberspace but also for international digital law. First and foremost, it forms the indispensable basis of many digital technologies and innovations, such as AI, for example. It is what private actors such as digital platforms or social networks have built their economic model on. The power of these private actors has made digital data a political issue, as it is considered a resource that can be exploited but must also be protected. It has become a strategic issue insofar as it lies at the heart of the power relations between private and public actors and within each of these categories. The importance of digital data, particularly for the protection of privacy, justifies its being an object of law and particularly of international law. Digital data can also be a legal tool facilitating the collection of evidence of state practice or legal opinion, for example. Digital data is multifaceted due to its nature (personal, sensitive, public, etc.) and especially to its uses (open data, commercial purposes, research, etc.).

2. Digital Security

Even if the development of information and communication technologies is put forward to increase the security of States and citizens, it has rapidly led to their exploitation for malicious activities by both States and non-state actors, ranging from spreading manipulated information to launching destructive cyber operations. Indeed, ubiquity and the ability to move forward while hiding one's identity have been exploited for different ends: espionage, destabilization, sabotage, economic profit. Relations between States and non-state actors are also sometimes hard to distinguish. The interconnection of networks and the role of non-state actors in their development and management makes digital security an international issue by nature, of interest to citizens, the private sector and States. As such, digital security has become a major concern for international security, economic and social development and human security and it constitutes a condition to achieving the Sustainable Development Goals.

3. Artificial intelligence (AI)

Artificial intelligence can be understood as a learning method underpinning heterogeneous technologies (facial recognition, lethal autonomous weapons, etc.) and uses (i.e., commercial or military purposes). One of the important aspects of AI is Machine Learning, through which algorithms improve themselves automatically through experience. Such a changing dimension may create some challenge on the compliance of these algorithms with international law. The rapid development of artificial intelligence is accompanied by numerous challenges, some also concerning international law and international relations. Contrary to the development of cyberspace, artificial intelligence is not perceived as a new domain in itself and the applicability of international law in general is not questioned. Nevertheless, it raises numerous questions, notably in terms of attribution, responsibility, and compliance with the rules and principles of international law. Interestingly, some questions have received a lot of attention while others remain relatively unexplored. For instance, Lethal Autonomous Weapon Systems (LAWS) have been heavily discussed in the literature and have also been the subject of various inter-states processes, while there have been fewer discussions about the impact of artificial intelligence on acts and behaviors taking place in cyberspace. Additionally, there are overlaps and cross-fertilization between the ethical and legal approaches to the regulation of AI. Yet, a clear distinction is relevant in numerous cases. Moreover, AI technologies also offer new ways to contribute to the development and enforcement of international law, and they are thus likely to have an impact on the substance of the law.

1.

state of the art

Over the past few decades, States and international organizations have increasingly focused their attention and resources on the challenges and opportunities emerging from the use of new digital technologies. In this first Part, we provide an overview of the most important international rules and processes in the fields of digital data, digital security and artificial intelligence. For each of these three topics, we identify the main applicable rules and processes of international law and offer a brief commentary on their key characteristics (e.g., their geographical distribution, their legal status & content, the branch of law to which they belong, etc.). The examples we picked are not an exhaustive list of instruments and are only meant to provide a sample of some of the most salient existing rules.

Given the fact that many current debates and international processes already focus on how international law applies to cyberspace and on the development of norms for responsible State behavior, we decided to give an overview of the existing controversies on the application of international law (e.g., the disagreements over the meaning of sovereignty, due diligence, non-interference) by distinguishing between globally accepted concepts and those that are still controversial, without attempting to resolve them. The aim is to give readers an idea of what rules, if any, exist for each topic, and to take note of the existing disagreements on their application. Considering the large number of rules of international law applicable to digital data, digital security and AI, the overview provided here does not aim at being exhaustive but rather provides a general knowledge of the current debates. The resulting "state of the art" provides a basis upon which to evaluate the adequacy of existing rules and processes considering the challenges and questions identified in Parts 2 and 3.

The main takeaway from the rules and processes identified in the statement of facts is one of geographical, technical and legal fragmentation. While there is substantial agreement on the applicability of international law in the digital domain, there are significant disagreements on the status, interpretation and application of existing rules. Moreover, specific rules on each of the three topics are often non-binding, unequally distributed or tied to specific branches of international law.

1. Digital Data

1.1. Main Principles and Rules of International Law

As a matter of principle, all general international law applies to digital data, as well as any relevant branches of international law, such as international humanitarian law, international human rights law (especially the rights to privacy, freedom of expression and access to information), and international trade law.

Various technical and political processes specifically dedicated to digital data have also been completed or are underway in many international organizations. The United Nations, European Union, Organization for Economic Cooperation and Development, African Union, Economic Community of West African States and other sub-regional organizations in Africa, the G7 and G20, the World Trade Organization are all addressing issues pertaining to digital data in accordance with their respective mandates.

Examples of Texts Adopted by International Organization or Processes

- African Union: the African Union Convention on Cyber Security and Personal Data Protection.
- ASEAN: ASEAN model contractual clauses for cross-border data flow.
- Bilateral and multilateral free trade agreements: EU-Japan FTA, EU-Canada Comprehensive and Economic Trade Agreements, etc.
- European Union: General Data Protection Regulation.
- Council of Europe: The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).
- OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Declaration on Transborder Data Flows; Recommendation on health data governance; Declaration for the Future of the Internet Economy (The Seoul Declaration).

- G7: Declarations on the free flow of data, including the UK 2021 G7 Roadmap for Cooperation on Data Free Flow with Trust, the UK 2021 G7 Digital Trade Principles, the G7 2022 Action Plan Promoting Data Free Flow with Trust.
- G20: 2019 G20 Osaka Leader's Declaration;
- Executive agreements on transborder access to e-evidence, e.g., the U.S./UK and U.S./Australia agreements; laws on the protection of military data and a great number of other national laws, etc.;
- Ibero-American Data Protection Framework: e.g., the guide on international data transfers.
- WTO: see the work program on electronic commerce.
- United Nations General Assembly: see the resolutions on the right to privacy in the digital age.

1.2. Overview of Existing Rules

Existing international law on digital data is still at a burgeoning stage. With the exception of EU law, there are few binding rules of international law specifically dedicated to digital data. Indeed, most of the universal, regional or bilateral instruments addressing digital data do so either through interpretation or by subsuming digital data within a larger material scope, for example within the right to privacy enshrined in human rights instruments. Although international data protection frameworks exist since the '70s through the work of the OECD and the Council of Europe, most rules specifically dedicated to digital data have been adopted in narrow contexts, mainly in the fields of data protection, cybercrime and trade law (e.g., through the General Agreement on Trade in Services, or the Agreement on Trade-Related Aspects of Intellectual Property Rights).

Contrary to the field of digital security, there is a progressive shift from early non-binding (e.g., the OECD privacy guidelines) toward biding instruments (e.g., the GDPR), even though most rules can still be found in national law. At the international level, there are very few instruments specifically dedicated to digital data. Most of the existing international rules on digital data can be found in the regional law of the EU, the African Union (e.g., the Malabo Convention, even though it has not yet come into force), the Council of Europe (Convention 108 on data protection; Cybercrime Convention), the OECD, ECOWAS and other regional or sub-regional international organizations in Africa and Asia. Bilateral executive agreements and treaties are also an important source of existing rules.

1.3. Overview of Consensual vs. Contentious Rules

In principle there is widespread agreement on the applicability of general international law and of the various relevant branches of international law (international human rights law, international humanitarian law, law of international responsibility, etc.) to the digital domain, including issues pertaining to digital data. There is also a relative agreement on the main parameters of data protection (right of rectification, oversight bodies, etc.).

There are, however, many cultural and legal differences in conceptualizing personal data, the notion of privacy and on the application of existing human rights law. National and regional approaches to data protection vary greatly among jurisdictions, which contributes to increasing the legal fragmentation. There are also many disagreements on transborder access to data in the field of cybercrime and jurisdiction, especially regarding the appropriate data protection standards (e.g., Schrems cases) and jurisdictional criteria (e.g., Cloud Act, e-evidence, European, Chinese, and Russian laws). Finally, the ideal of a free flow of data is facing a growing number of pushbacks which raise significant challenges from the perspective of trade law.

2. Digital Security

2.1. Main Principles and Rules of International Law

As a matter of principle, all general international law applies to digital security, as well as any relevant branches of international law.

Various technical and political processes specifically dedicated to digital security have also been completed or are underway in many international organizations, among which the UN (UN Global Programme on Cybercrime under the auspices of UNODC; the UN OEWG and GGE processes, the Open-ended Ad Hoc Intergovernmental Committee of Experts to elaborate a comprehensive international convention on "countering the use of ICTs for criminal purposes"), the ITU (ITU Regional Cybersecurity Centre; ITU-T Study Group in the telecommunications standardization sector, Global Cybersecurity Index, etc.), the OECD (working party on security and privacy in the digital economy), the OSCE, regional and sub-regional organizations (OAS, UA, ASEAN). Multistakeholder initiatives are also underway in fighting terrorism, hate speech, or in reinforcing cybersecurity, for instance (Tech Against Terrorism, Global Internet Forum to Counter Terrorism, Paris Call for Trust and Security, Christchurch Call).

Examples of Texts Adopted by International Organizations or Processes

- ASEAN: Declaration to fight cybercrime; ASEAN Leaders' Statement on Cybersecurity Cooperation.
- Arab League: Arab Convention on Combating Information Technology Offenses.
- Council of Europe: Cybercrime Convention and its additional protocols; Declaration by the Committee of Ministers on the financial sustainability of quality journalism in the digital age Decl(13/02/2019)2; Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of Internet intermediaries; Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes Decl(13/02/2019)1).
- G7: Charlevoix commitment on defending democracy from foreign threats, G7 Actions for Enhancing Cybersecurity for Businesses.
- ITU: resolutions, e.g., Resolution on Strengthening the role of ITU in building confidence and security in the use of information and communication technologies REV. DUBAI, 2018, and recommendations, e.g., Recommendation ITU-T X.1500—Amendment 12 (2011) "Overview of cybersecurity information exchange."
- OSCE: confidence-building measures, documents PC.DEC/1106 and PC.DEC/1202.
- Paris Call for Trust and Security in Cyberspace.
- United Nations General Assembly resolutions: on the Creation of a global culture of cybersecurity (e.g., A/RES/59/239); on Countering disinformation (e.g., A/RES/76/227), on the

Promotion and protection of human rights and fundamental freedoms (e.g., A/RES/75/176); on Developments in the field of information and telecommunications in the context of international security and on States' responsible behavior (e.g., A/RES/76/19).

- United Nations Security Council resolutions: on terrorism, especially on terrorist propaganda and hate speech online (e.g., resolution S/RES/2354 (2017) on the implementation of the Comprehensive International Framework to Counter Terrorist Narratives), on the security of critical infrastructures (S/RES/2341(2017)).
- UN GGE and OEWG reports: A/65/201, A/68/98, A/70/174, A/75/816, A/76/135.
- UNHRC: resolutions on the promotion, protection and enjoyment of human rights on the Internet, e.g., A/HRC/RES/38/7 and A/HRC/RES/47/16.
- WHO: Joint declaration of the WHO et al. on managing the COVID-19 infodemic, promoting healthy behaviors and mitigating the harm from misinformation and disinformation.
- Shanghai Cooperation Organization: Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.
- OAS: see the work of CICTE, the Inter-American Committee against Terrorism; the resolutions of the General Assembly, e.g., AG/RES. 1939 (XXXIII-O/03) and AG/RES. 2004 (XXXIV-O/04)); the work of the Inter-American Judicial Committee on International law and State cyber-operations.
- Wassenaar Arrangement: provisions on intrusion software on the list of dual-use goods and technologies.

2.2. Overview of Existing Rules

There are few binding international rules specifically dedicated to digital security except in the field of cybercrime and in EU law. However, many binding instruments not specifically dedicated to digital security are also applicable. Non-specific rules on digital security can be found both at the universal (e.g., prohibition on the use of force, international humanitarian law, international human rights law, international space law, international telecommunications law) and the regional level.

Cybercrime and international security are the two main domains in which we find provisions dedicated to digital security. Relevant provisions can also be found in the instruments dealing with terrorist activities. Trade law may also be increasingly concerned with digital security, especially since the imposition of security requirements in the field of ICTs may impose barriers to trade and violate existing trade rules. Unlike the field of cybersecurity, information operations have not yet been addressed by most normative initiatives, except from the perspective of countering terrorist propaganda, and perhaps also from the perspective of human rights law (especially the rights to free and fair elections and freedom of information/access to information) and sovereignty (destabilization of political regimes).

2.3. Overview of Consensual vs. Contentious Rules

In principle there is widespread agreement on the applicability of general international law and of the various branches of international law (international human rights law, international humanitarian law, law of international responsibility, etc.) in the field of digital security. Yet, despite a relative consensus about the applicability of international law, many questions on its interpretation and application to cyberspace remain contentious.

There are unresolved disagreements on issues concerning the substance of international law (e.g., on the existence of certain rules or principles of international law in cyberspace, such as due diligence and sovereignty), the interpretation of its rules and norms (thresholds, coercion element and non-intervention, data as a protected object under IHL, non-physical effects and use of force/armed attack) and on their implementation in cyberspace (attribution, etc.). The extension of the law of State responsibility to digital activities, in particular, has been the subject of many disagreements, especially on the issues of attribution, countermeasures and defenses. Overall, the treatment of the application of international law to digital security has been uneven: there has been considerable focus on resolving disagreements on some international legal rules (e.g., on the prohibition on the use of force) while others have had a much more cursory treatment (e.g., human rights).[2]

Note 2 For instance, of the 184 rules of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017), only five were devoted to human rights questions.

3. Artificial Intelligence

3.1. Main Principles and Rules of International Law

International discussions and normative instruments on AI focus to a large extent on ethical questions, which are often conflated with legal ones. UNESCO's recommendation on the ethics of AI is a prime example of an instrument looking at AI through an ethical lens, while at the same time containing detailed legal provisions in substance. The following sections will provide an overview of existing international legal instruments on AI, without delving into their ethical implications.

At the international level, there are few, if any, binding rules specifically devoted to AI. There are however international human rights law standards that can be directly applied to AI. Relevant rights may include freedom of thought, privacy and non-discrimination (e.g., rights enshrined in the International Covenant on Civil and Political Rights, the International Covenant on Economic and Social Rights, the European Convention on Human Rights, the Inter-American Convention on Human Rights, the African Charter of Human and People's rights, the Istanbul Convention Against Violence Against Women, etc.), as well as other broad international rules that cover the use of technologies by States. AI technologies are already deployed in the context of hostilities, questions pertaining to the prohibition of the use of force and the law of armed conflicts, as well as other related rules of international law, are thus also relevant.

In addition to these general instruments, a growing number of international organizations are adopting rules specifically dedicated to artificial intelligence, among which the Council of Europe, the OECD (Council Recommendation on Artificial Intelligence), UNESCO (Recommendation of the General Conference on the Ethics of AI), the ITU (especially through its AI for Good summits). At the United Nations, discussions on the international security implications of artificial intelligence have been focusing on the development of lethal autonomous weapons systems (LAWS). The issue was placed on the agenda of the Meetings of High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW) in 2013. After a few informal meetings, the discussions took a similar shape to those on international cybersecurity: a Group of Governmental Experts (GGE) was established in 2016 and adopted 11 guiding principles on LAWS in December 2019. Through these principles, the GGE affirmed the applicability of international law and international humanitarian law in particular, as well as a set of ethical and non-binding principles. In the context of this White Paper, it is worth highlighting that the LAWS principles make no mention of autonomous cyber capabilities.[3]

Examples of Texts Adopted by International Organization/Process

- Benguerir Declaration: Final Declaration of the Forum for Artificial Intelligence in Africa.
- Council of Europe, Parliamentary Assembly: Recommendation 2102 (2017) on the brain-computer interface: new rights or new threats to fundamental freedoms? ; Recommendation 2185 (2020) on Artificial intelligence in healthcare: medical, legal and ethical challenges ahead; Recommendation 2182 (2020) on justice by algorithm—The role of artificial intelligence in policing and criminal justice systems; Recommendation 2102 (2017) on Technological convergence, artificial intelligence and human rights. Resolution 2346 (2020) on the legal aspects of "autonomous" vehicles; Resolution 2345 (2020) on Artificial intelligence and labor markets: friend or foe?; Resolution 2343 (2020) on Preventing discrimination caused by the use of artificial intelligence; Resolution 2341 (2020) on the Need for a democratic governance of artificial intelligence.
- Council of Europe, Committee of Ministers: Declaration on the risks of computer-assisted or artificial-intelligence-enabled decision-making in the field of the social safety net Decl(17/03/2021)2; Declaration on the manipulative capabilities of algorithmic processes Decl(13/02/2019)1; Recommendation CM/Rec(2019)1 on preventing and combating sexism.
- Council of Europe, Conference of Ministers responsible for Media and Information Society: Resolution on Artificial intelligence—Intelligent politics Challenges and opportunities for media and democracy.

[3] **Note 3** Cybersecurity is only briefly mentioned in the sixth principle, principle (f), as one of the "appropriate non-physical safeguards [that] should be considered [w]hen developing or acquiring new weapons systems based on emerging technologies in the area of lethal autonomous weapons systems".

- Ibero-American Data Protection Network: General Recommendations for the Processing of Personal Data in Artificial Intelligence.
- UNESCO: Recommendation on the Ethics of Artificial Intelligence; Beijing Consensus on Artificial Intelligence and Education.
- United Nations: 11 Principles on Lethal Autonomous Weapons Systems adopted in 2019 by the GGE on LAWS, CCW/MSP/2019/9, Annex III, p. 10.

3.2. Overview of Existing Rules

AI may be one of the few digital subject areas where most States are willing to adopt new instruments, as evidenced by the Recommendation on the Ethics of AI adopted by UNESCO in November 2021. Attempts to regulate AI are highly fragmented and vary depending on which of its technologies or uses is taken into account. Existing international law on AI is at a very early stage of development, even though there are multiple initiatives and processes currently taking place with sometimes a certain degree of overlap regarding their content.

The limited number of specific international rules on AI does not suggest, however, that AI is not regulated by international law. Indeed, existing rules and principles of international law are relevant to regulate AI technologies and their different uses. Yet, there is still a level of uncertainty as to how exactly these rules could be applied to AI. There is no binding rule of international law specifically dedicated to AI; there is, however, an increasing number of non-binding norms adopted on AI in general or on certain specific applications (e.g., on AI in health, labor markets and education, on autonomous vehicles, on the use of AI in the criminal justice sector, etc.).

3.3. Overview of Consensual vs. Contentious Rules

In principle there is agreement on the applicability of general international law and of various branches of international law (international human rights law, international humanitarian law, law of international responsibility, etc.) to AI. However, there is still no defined or conceptually clear position on AI in international law, and it is unclear whether current rules are sufficient or effective, and whether there is a need for new rules, for instance, in the context of human rights. In that vein, an important topic of uncertainty and discussion concerns whether and how humans will be able to retain control over AI and thus whether there is a need for new rules in that perspective.

1.3.4. The Impact of AI on International Law

The previous paragraphs outlined how international law is regulating different dimensions of AI. Yet, it is important to note that the development of certain applications of AI may impact the substance of international law, decision-making processes related to international law, law-making processes as well as for the implementation and enforcement of its rules and principles. Machine learning and computational text analysis may be used, for instance, for dispute settlement mechanisms, treaty negotiations and international adjudication. The capacity to collect and process important dataset may be used to identify violations of rules or principles of international law.

1.4. Conclusion

This "state of the art" leads to a twofold conclusion. There is, firstly, a consensus on the applicability of international law to all three topics and on the existence of a great diversity of normative instruments relevant to the issues at hand. The binding instruments are rather general in scope, without specifically addressing any of the three topics. On the other hand, at the regional and global levels, there is also a plethora of non-binding instruments specifically dedicated to digital data, digital security or AI.

The second observation concerns the existence of common challenges across the three themes. It was possible to observe unresolved disagreements on issues of general international law, and on the relevance, interpretation and implementation of international legal rules and norms to cyberspace. These disagreements could partly be attributed to the different cultural approaches of the digitally powerful states and regional groups weighing in the current negotiations. Three key challenges will be presented in the next Part.

2.

challenges

The emergence of new technologies in the fields of digital data, digital security and artificial intelligence has profound political, social and economic implications, both positive and negative. While some of the challenges and opportunities arising from the use of digital technologies are sector-specific, we have identified three common challenges cutting across all three topics under consideration: the relationship between public and private actors, the political instrumentalization of international law on digital issues, and endemic digital inequalities. Indeed, despite the technical, legal and geographical fragmentation of the digital sphere (as observed from the rules and processes gathered in the statement of facts), these challenges are pervasive and raise difficult questions for policymakers, international lawyers and researchers working on all three topics.

While the challenges identified here are not exhaustive, they are likely to shape debates on digital technologies in the coming years. They may also be relevant beyond the digital domain, for example in the context of some of the other topics being considered by the ILA for its 150th anniversary, as international law grapples with increasing political polarization, persisting inequalities and an increasingly complex landscape of non-state actors. Crucially, these challenges are often interdependent: the relationship between public and private actors, for example, implicates the often-unequal distribution of digital capacities, and both challenges are subsumed within the broader politicization of international legal debates on digital issues. Any assessment of proposed solutions must therefore consider their externalities, positive or negative, on the other challenges and opportunities. In this Part, each of the three challenges will be discussed and illustrated with examples from the fields of digital data, digital security and AI. The aim is to understand the difficulties and opportunities they raise.

1. Boundaries of the Public/Private

Debates on the appropriate allocation of roles and responsibilities between public and private actors have been a recurring feature of globalization. In the digital field, the development and use of new technologies by private actors have raised both enthusiasm and concerns about the capacity of States to effectively regulate access to information and online speech, and to ensure the security of the digital environment while not inhibiting innovation. Multinational corporations, especially large online service providers, control and exploit vast amounts of digital data that are integral to public governance, economic activity and individual rights, and they are at the forefront of the development of artificial intelligence technologies. Their data protection capabilities are also a key component of cybersecurity efforts, and they enjoy a prominent role in the prevention, detection and response to malicious cyber operations. These technologies and data are a source of revenue for these companies but also a valuable tool for serving the public interest. Conversely, other non-state actors, whether groups or individuals, are also responsible for conducting malicious operations, sometimes in close collaboration with States. The parameters of the relationship between States and a great variety of private actors, between the private and public spheres, are therefore an integral part of debates on digital data, artificial intelligence and digital security, and the following sections provide an overview of some of the main challenges ahead.

1.1. Digital Data

- Data Collection, Storage and Analysis by Private & Public Actors

Private companies analyze huge datasets, often containing personal data, and use them to develop new applications and technologies, but also for various business activities like advertising or the development of products or services targeting specific individuals and groups. Governments are also interested in digital data, whether for surveillance or for improving public administration purposes, and international organizations have also identified data as a strategic asset.[4] Producing, controlling and using the digital has thus become of utmost interest for a wide range of actors, including States and international organizations. Most digital data, however, is in the hands of private actors, on which citizens rely almost entirely to protect their data and associated rights. Many private actors have more data on citizens than governments, generating dependencies on the

Note 4 See, for instance, the U.N. Secretary General, *Data strategy of the Secretary-General for action by everyone, everywhere with insight, impact and integrity* (2020) ; I.T.U., 'New UN targets chart path to universal meaningful connectivity' (19 April 2022) <https://www.itu.int/hub/2022/04/new-un-targets-chart-path-to-universal-meaningful-connectivity/>.

private sector for the realization of governmental functions. During the COVID-19 crisis, for instance, companies from the surveillance and tech industry have expanded their services toward the health sector to offer big data analytics as a tool to deal with the challenges of the pandemic. In the context of the war in Ukraine, digital data held by Clearview, an American company known to have collected billions of photos of individuals online, has been used by the Ukrainian government to identify the dead and combat misinformation.[5] Similarly, the creation, use and detection of deep fake technologies involves both private and public actors.

Another aspect of the blurring lines between public and private actors and responsibilities concerns the cooperation required to enforce jurisdiction. In the context of criminal investigations, for instance, States often need to cooperate with the private sector to collect digital evidence. To counter disinformation and hate speech, they are also often compelled to collaborate with digital platforms. In France, for example, around 2015, the French government had to negotiate with Twitter to take content down after the company initially refused to comply with French law. Conversely, sometimes, digital platforms can also facilitate international law violations carried out by the State itself, as was perhaps the case when Meta (Facebook at the time) was accused of not doing enough to prevent the incitement to genocide carried out by public authorities of Myanmar on its platform.

International organizations and courts are facing similar challenges, an observation which has been highlighted by the UN Secretary General in the *UN Data Strategy*. The outcome of the ICJ case on the *Application for the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar),* for example, may depend on the ability to compel Meta to hand over relevant data.[6] If the ability to collect digital data may offer new opportunities for fact-finding missions and the realization of international justice, it also raises new challenges

Note 5 Paresh Dave, Jeffrey Dastin, 'Exclusive: Ukraine has started using Clearview AI's facial recognition during war' (*Reuters*, 14 mars 2022) <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>.

Note 6 Michael A. Becker, 'The Gambia v Facebook: Obtaining Evidence for Use at the International Court of Justice (Part I)' (*EJIL: Talk!,* 5 October 2021) <https://www.ejiltalk.org/the-gambia-v-facebook-obtaining-evidence-for-use-at-the-international-court-of-justice-part-i/>.

regarding the chain of evidence and probative value of such data, including when it is collected by non-state actors and outside a formal process of inquiry.[7]

Finally, private actors compete directly with States by taking part in activities that were previously the sole prerogative of public authorities. A good example is the development of cryptocurrencies which, to this day, largely escape the purview of most national laws and States' sovereign right over currencies. These developments question the roles and responsibilities of private entities toward citizens but also their relationship with States in the realization of governmental functions.

- Data & the Digital Economy

Data is at the heart of the economic systems developed by the private sector around new technologies: electronic currencies, platforms and new payment services, digital assets, etc. Four types of problems may arise from the control of private actors over data: 1) the confrontation between a commercial logic and a logic of security, including legal security, in the way data is being handled. Concerning legal security, different issues are being raised, from individual ones in the context of the application of the law to collective ones in that of national security; 2) a geopolitical approach vs. a commercial approach of the way data issues should be regulated; 3) a risk of divergence and a lack of communication and dialogue between economic players and regulators, as the former do not necessarily understand the interest of new rules produced by the latter, which may impact both the content and application of the law; 4) the question of what needs to be regulated, taking into account that it might not be essential to integrate everything into the law.

The strong private dimension of the economic sector might suggest that normative efforts should mostly focus on conflicts of law issues. But there is also a need to work on the substantive provisions of new instruments, as UNIDROIT does for example through its Digital assets and Private law project. Some sectors have already started to evolve. The banking and finance sectors that are particularly regulated, have already accepted that risk can exist without calling into question the integrity of their practices. To adapt to new challenges, States and international organizations have for example developed common

Note 7 The open-source investigations from Bellingcat, most recently in the context of the conflict in Ukraine, are a good example: https://www.bellingcat.com/tag/ukraine/?fwp_categories=news&fwp_tags=ukraine.

approaches to prevent the misuse of cryptocurrencies for criminal purposes.[8] In the field of cybersecurity incident reporting, the European Union's General Data Protection Regulation (GDPR) is, for example, a starting point for the obligation for private actors to do so.

The data of the digital economy does not only call for changes in what the law says but also in the way it is made. All this data can be used to gain a better understanding of practice and thus to develop the law in line with needs, or even to anticipate them. The role of private actors in the collection and analysis of this data leads us to wonder about the role that could be assigned to them in the development of standards. The public-private nature of this sector encourages further reflection on "collaborative international law,"[9] that is on improving the mechanisms for elaborating, applying and interpreting the law in order to make it more effective and efficient.

In sum, there are two main challenges here: on the one hand, the need for regulation to take technological neutrality into account and, on the other hand, the need to develop a common set of minimum standards that protect individual and collective interests but also promote technological development. In order to preserve economic stability, the law must not radically change, but it must evolve according to real-world needs.

- Data and Normative Plurality

Another dimension of the challenges associated with the question of public/private boundaries is the normative plurality that flows from the growing role and importance of private actors. The norms being set by the terms of service/community guidelines of major online platforms (regarding, for instance, the regulation of speech) serve as the basis for platforms to take actions and regulate content, becoming the *de facto* norms applicable in the "virtual territory" of the platforms and competing with the laws applying in a country. Interestingly, the terms of service are integrating things that are normally within the province of public legislation. For example, Meta's oversight board has been referring to international law in several of the

Note 8 See, FATF, *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Assets Service Providers* (2021), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

Note 9 See Catherine Kessedjian, *Le droit international collaboratif* (Pedone 2016).

decisions it has rendered since its creation.[10] This leads to a situation of both competition and complementarity between private norms and public ones.

1.2. Digital Security

In the field of digital security, the foggy distinction between the public and the private is apparent from the threat landscape itself. Firstly, States, including those with advanced capabilities, may allow, if not facilitate non-state actor activities in a way that is carefully designed not to exercise the level of control that would trigger their own responsibility. The line can also be blurred between activities conducted in the interest or upon more or less explicit requests from a State and activities conducted for the threat actor's own interest. In terms of capacities, code can be leaked, and tools can be reused by many actors, as evidenced by the Shadow Brokers leaks and their reuse by both States and non-state actors. Conversely, tools can be developed and implemented to disguise their authors' identity and complicate their identification. Secondly, the impact of digital threats further blurs the line between the public and private spheres. The effects of malicious activities can disseminate far further than the initial targets as shown by many malicious cyber activities in the past. Information operations, by their very nature, also transcends all the lines (public/private, civil/military). Finally, non-state actors can exercise prerogatives usually dedicated to States in order to defend themselves or others in the digital space. The blurring of all these lines has, however, one advantage: any effort to increase the level of security of an actor is likely to benefit others, and thus to make it harder for anyone to exploit existing vulnerabilities and conduct malicious activities.

The relationship between the State and non-state actors is also relevant in the context of ensuring a State's security and, more globally, international security. The importance of ensuring the security of the digital domain has immensely increased the power of private cybersecurity companies and Computer Emergency Response Teams (CERTs). Their collaboration and relationship with States has already become an important topic of discussion, particularly in the context of the attribution of cyber-operations, the security of critical infrastructure and the fight against cybercrime. States increasingly rely on private companies to store and protect sensitive data and critical in-

[10] For a list of these decisions, see https://www.oversightboard.com/decision/.

frastructure, and they are also often compelled to collaborate with cybersecurity companies to prevent, identify and respond to cybersecurity threats. So do international organizations such as Interpol. Private companies, especially digital platforms, also enjoy a particularly prominent role in efforts to curtail harmful information operations, with States heavily relying on them. The EU's Code of Practice on Disinformation and the proposed Digital Services Act (DSA) are key initiatives in that regard, as well as a variety of national processes (e.g., current negotiations on the UK's online Safety Bill, debates in the U.S. on reforming section 230 of the communications Decency Act, various national laws to curb disinformation, etc.). Ultimately, the relationship between the State and private companies on content moderation and information operations will define who has control over speech on the Internet.

The respective roles of private companies, NGOs & individuals in international negotiations on digital security has become a prominent subject of debate. For example, the rules on the participation of civil society at the UN GGE and OEWG processes and at the ad hoc committee on cybercrime have been the source of many disagreements among participating States.[11] Private companies (especially Microsoft) are also very interested in negotiations at the UN and international negotiations more generally although their involvement varies greatly. Discussions on the respective roles and responsibilities of States and civil society/private companies raise significant questions on the legitimacy of international lawmaking and the balance of power between relevant stakeholders, that may vary at the different stages of the norm-creation process. One of the challenges will be to design institutional structures capable of accommodating the participation of all relevant actors, while preserving the State's key prerogatives on norm creation and decision-making. If multilateral and state-centered processes do not succeed, there is also a possibility that other actors and processes will fill the gap. Processes like the Oxford Process on International

[11] **Note 11** See the resolution on multi stakeholder participation at the OEWG recently proposed by the UK: U.N.G.A., "United Kingdom of Great Britain and Northern Ireland: draft resolution. Modalities for the participation of non-governmental organizations, civil society organizations, academic institutions and the private sector in the open-ended working group on security of and in the use of information and communications technologies 2021–2025" [7 April 2022] A/76/L.49; or the debates about multi stakeholder participation at the *Ad Hoc* Committee on cybercrime: "General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations" [26 May 2021] GA/12328.

Law Protections in Cyberspace[12] or the *Tallinn Manual* (frequently cited and debated by States, sometimes even in their national positions on the application of international law in cyberspace) have already shown they can be effective if they succeed in getting buy-in from enough states. Private companies have also initiated various processes in the field of digital security, such as the Charter of Trust (Siemens), the Cybersecurity Tech Accord (Microsoft), and in the context of the fight against terrorism (see esp. the Global Internet Forum to Counter Terrorism).

Finally, the relationship between the State and non-state actors manifests itself in the field of normative plurality. For both the physical and logical layers, security is largely defined by non-state actors. Global standards like ISO shape the future of technologies and the architecture of the Internet is managed by non-state actors. Since security is either not always a priority for technical requirements or is being lowered for national security issues,[13] technical requirements and security procedures, such as in the case of vulnerability disclosure, can impact, directly or not, the level of security. Even if States can influence these norms, they are deprived of great power in this field, having to deal with private technical regulation. In the field of disinformation, different efforts of co-regulation or self-regulation exist.

1.3. Artificial Intelligence

Today, non-state actors, are the leading actors in the development of AI technologies and applications, in particular private companies and research institutions. Even when States are developing their own AI applications, they are mostly based, at least partly, on technological solutions developed by non-state actors. An AI application may be the result of different solutions developed by different actors, either State-related or non-state actors, and thus contributing to blurring the boundaries between these different actors. In this context, questions related to the relationship and allocation of responsibilities between public

[12] **Note 12** Oxford Process on International Law Protections in Cyberspace, <https://www.elac.ox.ac.uk/research/the-oxford-process-on-international-law-protections-in-cyberspace/#:~:text=The%20Oxford%20Process%20on%20International%20Law%20Protections%20in%20Cyberspace%20is,2020%20in%20partnership%20with%20Microsoft>.

[13] **Note 13** See the Snowden revelations on cryptography and the US.

and private actors are particularly relevant regarding AI. Moreover, the development of AI requires access to data which is often held by private actors, raising concerns similar to the ones already discussed in the context of data collection, storage, and analysis by private and public actors which will thus not be restated in this section.

The role of non-state actors in State-sponsored uses of AI as well as their relationship with States take very different forms. In order to perform certain tasks, including functions that are integral to the exercise of public authority, state agencies and other entities acting on behalf of States have been using AI applications developed by private actors. There is, for instance, a growing use of AI solutions in border and immigration controls,[14] criminal and financial investigations, or in the context of a conflict.[15] The development of the so-called e-health sector can also illustrate how the relationship between public and private actors can be challenging, as data collected by privately developed applications may be used by public health institutions. The conduct of a specific activity using an AI technology may be the result of different activities performed by both States and non-state actors, to develop certain technologies, transform and then use them. Such a diversity of roles played by non-state actors also challenges the way these relationships may be grasped by international law.

2. The Politics of Law in Cyberspace

Given their significant social and economic implications, international debates on the governance of digital technologies are often contentious and politically fraught. The development of legal rules and non-binding norms has become an object of political debate and strategizing, an avenue for States and other interested stakeholders to promote their vision of Internet governance, and even perhaps governance more broadly.

Note 14 See for example European Parliament, *Artificial Intelligence at EU Border. Overview of applications and key issues* (2021).

Note 15 The US-based company Clearview AI offers a relevant example, as its facial recognition application has been used by law enforcement authorities in the US and has more recently been provided to the Ukrainian Government for the purpose of identifying Russian soldiers killed in Ukraine.

2.1. Digital Data

There are currently several different models of data protection. By way of example, and at the risk of oversimplifying them, we can highlight a European model considering data as an attribute of the person worthy of the strongest protection, an American model considering data as an asset and favoring its free collection and use, particularly on a commercial basis, and an emerging Chinese model focused on the preservation of sovereignty and security. These three models have common characteristics but also very different underlying logics, which lead their proponents to diverge in their interpretation of internationally established standards and to envisage different, even opposing, methods of data protection and control.

The confrontation between these different models materializes through the issues surrounding the extraterritoriality of normative instruments, but also the operational competence of states and international organizations. More generally, we are witnessing an opposition between two competing logics, one prioritizing the free flow of data, another its protection. It is legitimate for States and regional groups to defend normative instruments based on their own values, but their extraterritorial effects may lead to an increase in conflicts of norms and jurisdiction. The solution lies not only in the development of rules on conflict of norms and jurisdiction but also in the substantive rules of public and private international law.

It also depends, above all, on developing the appropriate mechanisms for dialogue, cooperation and even complementarity between the different normative systems, whether at the stage of law formation or at the stage of its implementation. The inscription of the *Protection of personal data in transborder flow of information* in the United Nations International Law Commission (ILC) long-term program of work[16] could be an interesting prospect in this sense, if it is realized. A reflection on the politics of law leads us to think about how to improve legal mechanisms to develop a genuine *international* law and also to respond to the digital divide as discussed later in this report.

2.2. Digital Security

There is a widespread agreement on the fact that digital threats (cyber and informational) will continue to increase in number and sophistication. According to several expert interviews, the

Note 16 International Law Commission, *Report on the work of the fifty-eighth* session [2006] A/61/10, Annex D.

nature of malicious activities (cybercrime, cyberterrorism, attacks against critical infrastructure, cyber espionage, mass surveillance, information operations, etc.), which range from sophisticated state-sponsored cyber activities to low-level threats, will likely remain the same while their sophistication, scale and pace of execution will increase. The rising instability and insecurity in the digital sphere have been and will thus continue to be the subject of much legal and political debate. Indeed, while many actors spend tremendous resources to counter those threats, both States and non-state actors also benefit from the conduct of malicious activities and are unlikely to significantly restrict their options. This will impact both the content of the relevant law and the lawmaking process.

Today, the main challenges in international negotiations on cybersecurity are not legal but geopolitical. Through international negotiations on digital security, States compete to impose different conceptions of Internet/ICT governance: some see the digital sphere primarily as an opportunity to advance economic prosperity, others focus on its potential to ensure human prosperity, and yet others prioritize state security. These different visions coexist and sometimes conflict within one State. Each of these visions impacts the way States think and talk about international law, the choices made about its interpretation and the kind of international legal rules envisaged by States. For example, States that prioritize economic development look for international legal rules that preserve innovation, while those focusing on human rights emphasize privacy/encryption, and those preoccupied primarily with national security look to override cybersecurity protections in order to de-anonymize users and/or impose controls of digital content, etc. States can also voluntarily exploit the challenges in the interpretation of international law, generating new ambiguities, adding confusion and instability to the current situation. During the interviews conducted by the Committee to prepare the White Paper, it has been suggested that this situation does not necessarily imply that international law is at the root of the problems or the solution and that a lack of legal clarity is not the main obstacle to compliance. It is rather part of a larger crisis of multilateralism where international law has become a tool for political competition. While some States are interested in retaining the *status quo*, others see an opportunity to propose new rules and advance their own interests.

This political dimension of legal debates on digital security also manifests itself in the field of disinformation. If States managed to reach a consensus in fighting against terrorist propaganda, the development of information operations by States and non-state actors to achieve different ends, including to interfere in other States' internal affairs, is challenging the very foundations of western democracies. For decades, western democracies have cautiously avoided including information operations in international discussions while States such as China or Russia that defended the concept of information security have tried to do so. Today, Western States are struggling trying to find the right balance between content control and the protection of human rights. The phenomenon of information operations is fueled by States themselves as more and more States are developing military doctrines to legitimize and conduct these operations, creating vulnerabilities for their own societies and increasing the dilemma they are facing.

The geopolitical challenges encountered by digital diplomacy also touch upon the model of cyberspace itself. The debates about the role of the International Telecommunication Union (ITU) during the 2000s have reemerged as the fragmentation of cyberspace and the political control of its infrastructure increase. This reinforces the debates on the multistakeholder model of Internet Governance and sharpens a bit more the split between different visions of the formal and material regulation of cyberspace.

In the field of cybercrime, the politics of law has similar consequences with distrust when trying to achieve a consensus in the ad hoc committee in charge of elaborating a new cybercrime treaty within the framework of the UN, the fragmentation of international regulation on cybercrime, and the impact on human rights. Indeed, we're witnessing a situation where the fight against cybercrime is increasingly framed through the lens of national security and not criminal justice, threatening human rights and fundamental freedoms and limiting any willingness to cooperate.

The consequences are threefold. Firstly, it directly impacts the ability of States to reach any meaningful agreement to better ensure the security and stability of cyberspace within the framework of international security. Secondly, it exacerbates disagreements between States, reinforcing the logic of coalitions of like-minded States aggregating around common values and thus contributing to fragmented regulations. Finally, it leads to a situation where we see some security issues being framed under an economic lens to overcome current blockages. For example, the OECD, an international organization with a mandate focused on economic development, has started working on security issues such as vulnerability disclosure, the security of the ICT supply chain or the use of hack back by private actors.

While there are many contentious discussions on the content of international negotiations on digital security, the various processes under which these negotiations are conducted also raise significant political implications. This is especially true in the context of UN negotiations, the highest profile of which have been conducted through the UN GGE (the last one solely sponsored by the U.S. and its allies) and the Russia-sponsored OEWG processes. These processes have acquired an important political significance and their reports are vigorously negotiated and discussed by States and all other interested stakeholders. Crucially, questions of international law and its application in cyberspace were central to both processes.

States have been reluctant to share precise views on the application of international law in the context of digital security (thus hindering the clarification of the law, whether treaty-based or customary) although the final 2021 GGE report (A/75/135) was notably accompanied by the publication by certain States of national statements on the application of international law in cyberspace (A/76/136). The value and political significance of these statements will be the subject of much debate: while they could be considered as a tool to clarify the law and get buy-in from States, they may also be perceived as a form of unilateralism further eroding already-fragile multilateral processes.

Ultimately, one of the key challenges in the coming years will be to identify the appropriate forums to discuss sensitive digital security issues and their interaction with international law: while UN processes are very likely to remain relevant, especially through the most recent mandate of the OEWG and the *Ad Hoc* Committee tasked with elaborating a cybercrime treaty within the framework of the UN. Over the coming years, there will be much focus on the cybercrime negotiations at the UN, as they may revisit the norms discussed at the GGE/OEWG and/or expand the understanding of what constitutes a "cybercrime" to encompass information operations and may even touch topics such as attribution to States. Other international organizations with more specific mandates may also play a prominent role, especially the ITU, the OECD (already working on cybersecurity through an economic lens, see section 1 above), regional human rights and economic integration organizations (Council of Europe, OAS, AU, ASEAN, etc.), and even the WTO (security concerns and technical barriers are increasingly being invoked and raised to limit trade of digital products and services). The choice and coordination (or lack thereof) of those processes may depend on the political interests and the antagonism of the most powerful States and is likely to influence the content of the negotiated rules. Regarding the interpretation of international law, no traditional organ, such as the UNGA's 6th Commission, the International Law Commission or the International Court of Justice, is for now in a position to be tasked with clarifying it. This leaves an important role to play for non-multilateral institutions such as the Institute for International Law[17] or the International Law Association. In the meantime, other initiatives such as the *Tallinn Manual* or the Oxford Process have stepped in.

The universal forums and processes in which international negotiations on digital security will be conducted also have profound implications for the active participation of developing countries. There is a risk that a lack of participation of developing countries may lead to the adoption of rules and principles reflecting the interests of powerful States, which could further erode the perceived legitimacy of international law on digital security in the coming decades. Instead of bringing more developing countries into the conversation and reducing digital inequalities (see section of endemic digital inequality), adopted rules may either be irrelevant or harmful to developing countries if their perspectives are not integrated. Yet, it should be noted that there is an important difference between the level and impact of participation in universal processes and the strong normative production at the sub-regional level. In the field of the interpretation of international law in cyberspace, efforts are also being made at the regional level as illustrated by the work of the Organization of American States Inter-American Juridical Committee project on improving transparency regarding state views on international law in cyberspace.[18]

2.3. Artificial Intelligence

There are two core challenges on the politics of law in cyberspace which concern AI and that have already been discussed in the previous sections. Firstly, there is an important degree of conflation between legal and ethical matters, which is not a problem in itself but still raises some questions. The discussions and initiatives seem to be focusing predominantly on ethical questions at first sight. A closer look at those discussions shows, however, that legal matters and norms are at the center of these discussions and fundamental to comprehend the adopted instruments. Ethics thus seems to be more a point of entry to

Note 17 In 2021, the IIL has created a commission on the applicability of international law to cyber activities.

Note 18 Organization of American States Inter-American Juridical Committee, *International Law and State Cyber Operations* [2020].

advance matters related to the application of international law to AI. The boundaries between ethical questions and legal questions are thus not always clear. It should be noted that this may be a matter of concern as it could affect the value or substance of the legal rules. Secondly, in the field of international security, most of the attention has been focused on LAWS and, therefore, other forms of unfriendly or hostile conducts using AI applications tend to be absent from the existing discussions, which can increase their polarization. In multilateral forums, for instance, there has been almost no discussion on autonomous cyber operations and how to regulate them, while they are already a reality.

A third important challenge concerns the identification of the right balance between approaching AI as a whole or choosing a more focused approach on specific technologies and uses of AI. Different technologies and applications raise different legal questions. This challenge creates a twofold difficulty. On the one hand, there are very limited, if any, overarching legal questions about AI but rather numerous questions on specific uses and consequences of AI-based products. In some ways, this challenge relates to the difficulty of clearly defining what should be understood as AI and how this should be approached by international organizations and processes. On the other hand, this also has a practical consequence, as there are different discussions and processes going on at the same time, each focusing on a rather limited set of questions and domains of application and with very different objectives. Finally, in some cases, the discussions on AI are incidental. In these situations, AI is not being tackled as such, but decisions are made on issues that may impact AI. This is, for instance, the case in the fields of violent extremism and terrorism where preventive measures can be recommended with an implied use of AI. Yet, these very general discussions on AI related to other topics might offer very interesting contributions that would contribute to similar discussions on other topics. Thus, some of these different discussions should be more connected in order to facilitate cross-fertilization, but also to avoid overlaps and contradictions. In adopting a more granular approach to the different AI-related technologies, it would be easier to identify similar discussions taking place in different fora.

A last remark on the politics of international law and AI concerns the approach that has been adopted. Generally, AI is approached from a reactive perspective, aiming at preventing possible (negative) uses of these technologies. The discussions on LAWS is a good example, as is the discussion on the respect of fundamental rights by new AI applications. Yet, as discussed in different parts of this report, AI also offers positive solutions for the development and enforcement of international law, the implementation of human rights or the reduction of the digital divide. This issue has been little tackled in the context of fact-finding missions and human rights but it remains underexplored.

3. Digital Divide

3.1. Digital Data

ICTs are a great way for people in developing countries to access information and participate in the development of greater cultural diversity in the digital age. However, in its 2021 report *Measuring digital development. Facts and figures*, the ITU stated that 63 percent of the world's population had access to the Internet but that "96 percent of the 2.9 billion still offline [were] living in the developing world."[19] Digital development isn't just a matter of connectivity. It also includes meaningful access to the Internet, that is, the ability to benefit from ICTs services, in urban and rural locations and without gender barriers. According to the ITU, there is both a generational gap and a gender one. This results in a "connectivity Grand Canyon" or "digital divide" that directly impacts the development of States and the ability to achieve the UN Sustainable Development Goals.[20] Although capacity-building programs in the field of connectivity are being implemented by international organizations and many States,[21] this "digital divide" is far from being closed and will increase development inequalities. These inequalities in connectivity are also impacted by the concentration of the networks in the hands of a few actors in a monopolistic position. Added to the failure or manipulation of the architecture of the Internet for geopolitical ends, this threatens the decentralized nature of the Internet and thus its resilience, impacting connectivity as a whole.

This "connectivity Grand Canyon" reinforces the digital data divide, a growing concern that concerns developing countries but also those that do not have powerful companies collecting

Note 19 I.T.U., *Measuring digital development Facts and figures 2021* (2021), 1.

Note 20 U.N. Secretary General, *Roadmap for Digital Cooperation* (June 2020); U.N.G.A., "Resolution on information and communications technologies for sustainable development" [17 December 2021] A/RES/76/189.

Note 21 For a list of such programs, see https://cybilportal.org/es/projects/.

and processing data for economic purposes (e.g., European countries). The "data value chain" has become key in the development of the digital economy and requires capacities to produce, store and process data in order to monetize it. It constitutes a prerequisite to develop and sell Internet of Things (IoT) products and AI applications and systems and will in return produce data that will be used for future products and services, increasing the cost of entry on the digital market. As pointed out by a recent report from UNCTAD, "[a]s the data-driven digital economy has evolved, a data-related divide has compounded the digital divide. In this new configuration, developing countries may find themselves in subordinate positions, with data and their associated value capture being concentrated in a few global digital corporations and other multinational enterprises that control the data."[22]

Apart from economic consequences, these technical inequalities have direct consequences on the ability to enforce data protection mechanisms as data is stored and processed by powerful actors often located in other jurisdictions. They also constitute a driver for further fragmentation and limitations on data flows insofar as, in order to ensure the application of their laws and regulations on data, States can be tempted to limit data flows, thus impacting the development of digital products and services. There are also social and cultural consequences flowing from these technical inequalities. Products and services based on digital data won't reflect the moral and cultural values and beliefs of a given population, adversely impacting individuals and the society they live in. Conversely, the limitation of data flows is likely to increase "data bubbles" which in turn could be used to implement greater control and surveillance.

Finally, as technology can also further the implementation of international law, including human rights and fundamental freedoms, the rule of law and the administration of public services, the lack of digital data limits the ability of States to fulfill these key objectives and responsibilities, impeding the enhancement of human security and democracy.[23] In the same way, data accessibility is useful to face the major challenges of to-

Note 22 U.N.C.T.A.D., *Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow* (2021), xvi.

Note 23 In the field of preventing, detecting and countering corruption, this has been highlighted by the UN General Assembly: U.N.G.A., "Our common commitment to effectively addressing challenges and implementing measures to prevent and combat corruption and strengthen international cooperation" [2 June 2021] A/RES/S-32/1.

morrow, such as global warming or the problem of connectivity and the provision of humanitarian services. Promoting access to data and effectively sharing it will be one of the key challenges for the coming years, for States, as well as international organizations. And yet several factors can explain the relative lack of data sharing so far, including national security, confidentiality and privacy concerns.[24] Data accessibility is not only an economic problem but also a problem for achieving the SDGs.

3.2. Digital Security

The digitization of societies has been accompanied by the development of malicious activities from both States and non-state actors. As more and more services depend on connectivity, as products are increasingly connected (Internet of Things) and new technologies are developed (quantum computers, AI, etc.), the number of exploitable vulnerabilities as well as the means to exploit them will consequently increase. The rising number of cyberattacks has become a key concern for a wide range of actors. Countering these threats requires human, technical, organizational and legal capacities that are unequally distributed across the globe and that even the most developed countries lack. In that sense, there is today a global gap between the level of connectivity and the level of security. Inequalities in terms of access and transfer of digital data are also compounded by significant inequalities in digital security capabilities. The stakes are high as already-fragile developing countries are likely to be the most affected by endemic digital insecurity. Besides, the resulting vulnerabilities are capable of increasing instability at a global scale. But the most developed countries tend to be the most connected, which also makes them highly vulnerable to digital threats. The digital security of States is thus highly dependent on the actions of all others in this field. There is thus a common interest between all States, but more globally of all actors, in closing the digital security divide.

Apart from national security interests, digital security is also a requirement to ensure the protection of human rights. A lack of cybersecurity poses great danger to users' data, their right to privacy, freedom of expression or freedom of assembly and association. Without security, States are limited in their ability to protect and defend human rights. This extends to the security of technologies designed to advance human rights and

Note 24 O.E.C.D., *Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use across Societies* (2019).

international law or that can be used to do so.[25] Information operations have also been described as a threat for democracy. Countering these operations will benefit democracy and the rule of law. The same logic applies to businesses and human rights and due diligence.[26] Ensuring security is a way for them to prevent and address the risks that a lack of security can have on human rights. Digital security thus enables the respect and implementation of international law.

Since the late 1990s, as efforts to increase access to data and accelerate the digitalization of emerging economies have intensified, the international community has progressively created cyber-capacity building initiatives aiming to improve the security of the digital environment.[27] These initiatives involve a broad range of actors and communities (States, international organizations, NGOs, cybersecurity companies, etc.), focusing on a variety of topics (access to data, cybersecurity, etc.) and objectives (raising awareness, sharing knowledge on technical capabilities, policies, adapting the legislation, etc.). Although their common aspiration is to facilitate the circulation of knowledge and capabilities on digital security, their content and form vary significantly.

Given the collective importance of protecting the security of the digital environment, the coordination, effectiveness and legitimacy of these initiatives has become a prominent topic of discussion. However, behind their apparently technical nature, capacity-building initiatives also raise important political questions, especially regarding the relationship between developed and developing countries, but also among developing countries themselves. While sharing knowledge and skills has the potential to strengthen cooperation and improve technical, political and legal capabilities on digital security, it could also reproduce or even compound existing inequalities and dependencies, reproducing existing power hierarchies in the international arena. It has also been pointed out that duplicating existing legislations without considering the local context could lead to greater control over citizens, putting human rights at risk. Without sufficient coordination and adherence to overarching

[25] **Note 25** See *supra* on the role of data and AI to advance human rights and international law.

[26] **Note 26** See e.g., the B-Tech project conducted by the UN Human Rights Office of the High Commissioner: https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/BTechprojectoverview.pdf.

[27] **Note 27** For an overview, see https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf and https://www-tandfonline-com.ezp.lib.cam.ac.uk/doi/full/10.1080/23738871.2017.1294610.

principles, these capacity-building initiatives risk becoming short-term and self-serving projects.

In that context, the sustainability of cybersecurity capacity-building efforts has emerged as a key topic of concern and will likely constitute one of the most important challenges moving forward. Cybersecurity capacity-building initiatives will have to encourage the adoption of measures to promote the security of the digital environment without unduly restricting access to data and security tools and opportunities to use them (e.g., through greater requirements to register and record data). In other words, it will be important to ensure that cybersecurity measures do not hinder the digital, social and economic development of the least developed States, who are not always able to bear the high costs of achieving digital security as quickly as possible. Striking the right balance between cybersecurity and development will be a key factor in future efforts to reduce the digital divide.

3.3. Artificial Intelligence

Data is the prerequisite necessary asset to develop and use AI. The inequalities in terms of access to digital data and digital security capabilities also translate and are amplified in the field of AI. This observation has two primary consequences.

Firstly, most of the data is collected and stored by a limited number of actors operating from certain regions of the world, which makes it more difficult for other actors to emerge and develop their own AI applications. Thus, already-existing inequalities in terms of data collection and storage have consequences on the capacity to develop AI applications both in terms of the actors involved but also in terms of their geographical location.

Secondly, there are significant inequalities regarding the amount of data collected and processed by different population groups around the world. This has a direct impact on the development of AI applications, which tend to rely on the data of Western countries, creating significant biases. These biases affect the legitimacy of AI applications, especially when they are used for law enforcement purposes.

Besides, AI has the capacity to transform law-making processes, the substance and the enforcement of international law, as already discussed. This may have two opposite consequences for the digital divide. On the one hand, the digital divide, and in particular the unequal access to data, affects the capacity of States and other actors to benefit from AI solutions on international law. It might be a matter on which States could reinforce their capacity-building efforts as well as the sharing of data, in order to allow more States to access this data and use AI applications. Such an approach would be beneficial for the implementation of the rules and principles of international law as well as for the international rules-based order in general. On the other hand, AI-based solutions may help States with more limited capabilities to process a larger amount of data and foster their ability to participate in lawmaking and interpretative processes. This last comment will depend on the willingness of States to cooperate and share data and AI solutions in this context.

AI may also play a role in bridging the digital divide and its international legal consequences. AI applications can be used to collect and process large datasets on different matters and thus help identifying possible solutions, such as on how a specific international legal obligation is enforced at the domestic level. In that perspective, AI may offer relevant solutions for treaty verification and enforcement mechanisms. .

4. Conclusion

The challenges posed to international law by data, digital security and AI are threefold. They relate to the relationship between public and private actors, underlining the difficulties of adapting interstate mechanisms of international law in favor of a new way of looking at normativity, but also to the way in which law is produced and implemented. The second challenge concerns the politics of law, which opposes cultural, political and legal models that international law must strive to bring into a dialogue. Finally, these digital issues have highlighted the digital divide from an economic but also from a sustainable development point of view.

But these challenges also correspond to the opportunities offered by digital technology. Data and AI are also ways of bridging inequalities between the states and improving the human condition. Moreover, if international law sometimes seems to be affected by technological developments, these developments can also help it to progress, or even modify it. Data collection allows for a better understanding of the practice of actors in international relations and AI can facilitate the implementation of international law.

Both the challenges and opportunities that digital technologies constitute for international law highlight the relevance of legal capacity-building. Legal capacity building has two main objectives. On the one hand, it contributes to a better understanding of the substance of the law and how it applies in specific contexts, for instance, as with the different technologies discussed in this White Paper. On the other hand, it contributes to the development of domestic and regional regulations and policies in compliance with international law obligations, and to their implementation. Hence, sharing good practices is an important element in the legal capacity building.

This second part thus shows the interrelated relationships between data, digital security and AI between the challenges they raise, the opportunities they present, and, finally, between each of these elements. Incidentally, it raises substantial questions, that could feed our future debates and research.

3.

questions

Confronting the legal instruments outlined in Part 1 with the main challenges highlighted in the Part 2, this last Part identifies some of the most salient questions about the future development of international law on digital data, digital security and AI. Indeed, the adequacy of existing legal rules is constantly being evaluated in light of the conceptual and real-life impacts of new technological developments. Existing academic and policy discussions often debate whether current international legal rules are sufficiently clear, precise and complete to keep up with the rapid pace of digitalization even though there is also skepticism that digital technologies give rise to fundamentally distinct legal challenges and have a more significant impact on international law than other technological or social developments. The following sections will provide a brief and non-exhaustive overview of some of the main legal questions emerging in the fields of digital data, digital security and AI. But, beforehand, it is worth outlining the cross-cutting and common issues that digital activities will pose for international law.

1. Cross-Cutting Legal Questions

Because of the difficult dialogue between States to respond legally to the needs of the digital sector, numerous non-state initiatives have emerged to propose interpretations of international law or even new standards (e.g., the *Tallinn Manual*, the Global Commission on the Stability of Cyberspace, etc.). Groups of legal experts are also dealing with the digital sector (e.g., the Commission on International Law on the protection of personal data in transborder flow of information; the Institute of International Law on the applicability of international law to cyber activities). Without doubt, the ILA has a role to play in envisioning the evolution of international digital law.

It is nothing new to say that non-state actors should be considered in the ways in which law is formed and applied, and even more so in the context of digital law. It could be useful to think of a typology of the different ways in which the relationship between the private and the public can or does operate in relation to international law. At a more theoretical level, this would question whether digital issues change the way international law traditionally deals with non-state actors. At a more practical level, it could offer suggestions to better implement international law. For example, we could differentiate whether private companies are: 1) as agents for states to fulfill their sovereign responsibilities (i.e., to protect, respect and fulfill human rights on behalf of a state); 2), completing the State's fulfillment of its functions/responsibilities/obligations (Facebook's Oversight Board has integrated the IHRL into its decision-making process); 3) as competitors to States in the exercise of their sovereign rights (e.g., by designing their own digital security standards that resist state demands for decryption, etc.); 4) as substitutes for functions traditionally under the jurisdiction of a State (whether in terms of data or defense); or 5) as autonomous actors that intersect with public actors while defending their own interests (e.g., deciding whether to cooperate with law enforcement requests; devising their own interpretations of international law and, on occasion, enforcing them).

It also seems necessary to consider how ICTs are changing international law. Thinking about the adaptations of international law to meet the needs arising from technological developments is unproblematic. These debates must lead us to think or rethink institutional and substantive international law, the evolution of norms but also of sources, the processes of international law formation and the products of these processes. But it is also necessary to understand what these ICTs can bring to international law. We know that technical solutions can complement legal solutions (e.g., privacy by design or by default). But the law can also use new technologies in the field of evidence, in identifying State practice or *opinio juris,* for example, but also in the field of e-justice or legal tech. How can the interrelations between international law and ICTs be considered?

2. Digital Data

Clarification of existing law. The identification of rules applicable to digital data and the clarification of their interpretation will be one of the key legal challenges of the coming decades. There is a need to develop more precision as to how international law applies to digital data, all the while shaping the development of the law to reflect a wide range of legitimate interests and objectives, especially the sometimes-conflicting imperatives of human rights and privacy, law enforcement and national security. According to several expert interviews, the interpretation of privacy provisions in international human rights law will be of particular importance as the right to privacy is one of the most rapidly evolving and malleable fundamental rights. The ECtHR and the CJEU in particular are at the forefront of international privacy and data protection litigation, having to adjudicate increasingly complex and contentious cases, for example on mass and targeted surveillance by public and private actors, on the interception and storage of personal data to combat cybercrime, on the extraterritoriality of data protection regimes and on the main parameters of data protection itself (the notion of data, the right to be forgotten, the right to rectification, etc.).[28] Aside from the coordination or conflict between the ECtHR's and CJUE's approaches, the extent to which other regional organizations and courts are able to develop their own understandings of data protection will also be significant, especially given the growing influence of the EU's GDPR. The clarification and interpretation of existing rules will also be an area of concern in other fields of international law which involve issues pertaining to digital data, in international humanitarian law for instance, where there is considerable uncertainty as to whether digital data should be classified as an object or non-object during an armed conflict, and in international trade law (is data a good like any other, capable of being apprehended through existing rules, perhaps with slight modifications? How do we take the data produced by international trade into account?)

Regulatory fragmentation. Clarifying the law will be particularly difficult given the relative lack of harmonization of existing initiatives. States and international organizations often advocate for competing conceptions of data protection, which is reflected in the legal instruments they adopt. The differences between the European Union's approach to data protection, which is focused on fundamental rights and personal autonomy, and the approaches of the United States and other powerful states such as China and Russia, will likely be the source of significant political confrontations in the coming decades (see section above on the politics of law in digital data). Even though the GDPR already enjoys a considerable influence on many national and regional data protection policies, there is a growing trend toward the nationalization of norms and laws for the protection and security of the digital environment, which could further fragments and undermines the legal interoperability of relevant international, regional and domestic legal regimes. The private sector has already started to engineer the infrastructure to deal with this fragmentation (e.g., Microsoft developed the sovereign cloud model).

[28] **Note 28** ECtHR, *Guide to the case-law of the European Court of Human Rights - Data Protection* (ECtHR, updated on 31 December 2021); CJEU, *Factsheet on the protection of personal data,* (updated on 11 November 2021).

Extraterritorial jurisdiction. The fragmentation of existing norms and the trend toward their nationalization is accompanied by attempts to ensure the extraterritorial application of national or regional instruments. Given that data plays an important role for digital cooperation, evidence, and mutual legal assistance, regulatory conflicts arising from trans-border flows of data and the extraterritoriality of data protection regimes (e.g., the *Schrems II* case) will likely give rise to some of the main legal challenges in the field of digital data. The growing assertion of extraterritorial jurisdiction may be structural. As less technologically dominant states struggle to catch up, they are likely to resort to unilateral and extraterritorial regulations to try and keep control over their digital data; this holds for the EU and developing countries alike.

Human rights implications. Collecting, sharing and selling digital data, especially personal data, has significant human rights implications, both positive and negative. Practices such as targeted advertising, content curation, private and public surveillance, espionage, the collection of data for criminal investigations, Internet filtering, the use of biometric data, etc. can put privacy and freedom of expression at risk. But digital data and AI can also help improve the human condition. From the perspective of individuals, one of the main challenges of the coming decades will be to ensure that they can keep track and maintain control over their data.

Key Questions

- What are the different kinds of legal instruments and mechanisms that could be developed in order to ensure the effective protection of digital data by tech companies? How can the relationships between private and public actors be designed to promote both the circulation and protection of digital data?
- How will the international community deal with the legal ramifications (regulatory fragmentation, extraterritoriality, etc.) of pervasive political confrontation between states advocating for competing models of data protection?
- How could the international community prevent and mitigate the adverse effects of unequal access to digital data, especially big data? How to build a truly international data law?
- How can data bridge the digital divide, facilitate the achievement of OODs, and improve the human condition?

3. Digital Security

Regulatory fragmentation. Very few laws and regulations are harmonized across the world. This is the result of both a lack of universal instruments but also of different visions of cyberspace. In the field of cybercrime, and despite efforts to facilitate cooperation, cooperation remains complicated, the regulatory fragmentation and lack of cooperation slow down and even impede criminal investigations. Another aspect of the regulatory fragmentation deals with security requirements. The security requirements and legislation to strengthen security are being elaborated all around the world. Apart from the resulting fragmentation of law, there is a great risk of developing contradictory obligations (for example in the field of cryptography or in disclosing vulnerabilities) or obligations that could create vulnerabilities for everyone and threaten legal security. The regulatory fragmentation also challenges the implementation of measures to counter disinformation operations, hate speech and more globally the fights against harmful content.

Human rights implications. Countering digital threats has both positive and negative impacts on human rights. On the one hand, as the digital space is increasingly used to conduct information operations and disinformation proliferates, States and non-state actors involved in content takedown are putting pressure on several rights, including freedom of speech, the right to an effective remedy or the prohibition of discrimination. In the same vein, the extension of surveillance programs, whether targeted or not, and the success of the surveillance industry, challenges many rights and fundamental freedoms. The digitalization of societies has also mainstreamed the use of electronic evidence in criminal investigations. The need to access electronic evidence in a very short amount of time can challenge the obligation for States to protect human rights, especially in the case of extraterritorial requests to a service provider about data concerning a foreign citizen. The difficulties encountered in attempting to access electronic evidence can be an incentive for States to opt for bulk surveillance, eroding trust in public institutions, the rule of law and fundamental freedoms. As the sheer amount of data increases more rapidly than the pace of legal cooperation, the trends described above are likely to continue. On the other hand, the respect and protection of human rights will necessarily require greater digital security. This questions the role of digital security in the definition and assessment of States, international organizations and non-state actors' obligations.

Multilateralism and international law. Digital security questions the ability of multilateralism to deal with new issues and constitutes a condition to ensure its future. The verification of commitments has been highlighted as one of the main challenges to ensure compliance with new binding rules in the field of ICTs in the context of international security, something that could also explain the reluctance of States to publicly agree on most issues. But the issue of verification has broader implications than the verification of potential new obligations. The increasing number of malicious activities online, the multiplication of sources of information and the manipulation of information itself challenge the ability to verify online information, increasing distrust and conflictuality. As an object of multilateralism, digital security also keeps questioning the place and role of non-state actors in its elaboration. As a requirement, digital security will play a key role in the modalities of negotiation (protection of the information) but also in the ability of international organizations to ensure the relevant level of protection for their information.

Extraterritorial jurisdiction. Considering the very nature of malicious digital activities and the characteristics of the digital space versus the territoriality of the law, extraterritorial jurisdiction has been and will be a key legal challenge for the coming years. This is especially true as threats will increase in number and sophistication while cooperation will likely remain strained in many fields considering the level of distrust between States and the lack of capabilities to counter emerging threats.

Key Questions

- Does the role of private actors in initiating or responding to malicious activities call into question how international law deals with private actors?
- Will the international community be able to develop a consensus on the application and meaning of existing international law rules and concepts relevant to the field of digital security, or will new ones be developed?
- Is there any role, and if so, what will be the role of digital security in itself in relation to other international obligations?
- How can cyber capacity building and technology sharing be optimized to ensure that developing states are able to achieve digital security?

4. Artificial Intelligence

A first legal challenge, which has been highlighted earlier, concerns the conflation between legal and ethical matters, and the fact that most of the current processes and initiatives tend to focus predominantly on ethics rather than law. As discussed in the previous sections of the report, this is not a problem in itself and the work on ethical questions has also been beneficial to legal discussions. Yet, in some circumstances, such an approach may affect the content of international legal norms.

The absence of a clear and consensual definition of AI and most of its related notions (autonomous, machine, robot, system, etc.) creates important legal challenges. This definitional challenge amplifies another related challenge: the fact that there are several parallel processes and initiatives going on at the same time. Since these different initiatives and processes may use a different vocabulary to describe similar issues, it is more difficult to identify possible overlaps or divergences.

There is also uncertainty as to whether and how states should apply traditional rules of international law to AI. This challenge is related to the definitional challenge, for two reasons. Firstly, it becomes difficult to identify the object of the discussion and the potential consequences of the regulation. Secondly, some discussions on AI tend to be very general, while, for legal purposes, it may be necessary to adopt a more granular approach on the different forms of AI applications and their consequences on society.

There is currently no general understanding on how international law should regulate the application of AI in unfriendly or hostile State conducts. This observation has important consequences for different aspects of international law, such as the attribution of the relevant conduct, the determination of its lawfulness and the invocation of the responsibility of the different actors involved. These difficulties affect two branches of international law in particular: international human rights law and the law of armed conflicts. With respect to human rights law, key challenges include the determination of the human rights implications of facial recognition software, discriminatory bias in algorithms, attribution and responsibility for human rights infringements occasioned by the employment of AI. From the perspective of the law of armed conflicts, there are challenges concerning the regulation of certain means and methods of warfare as well as the appraisal of the technical evolution of weaponry and their legal consequences. All these challenges are exacerbated by the relations that may exist between States and non-state actors in the development and use of AI technologies. The recourse to AI solutions developed by different actors for decision-making as well as in autonomous systems may raise questions related to attribution and individual responsibility, notably regarding command responsibility and individual criminal responsibility. Intertwined activities performed by both non-state actors and States may also raise questions related to their accountability and to how to repair injuries caused by AI-based technologies even in the absence of a wrongful behavior. Finally, this situation also raises the question on how non-state actors, in developing certain AI technologies, should and can consider possible international legal obligations, notably related to human rights.

AI raises important challenges for international law, but it also offers new solutions for lawmaking and interpretative processes as well as for the enforcement of international law. More generally, AI also offers new solutions that may have a positive impact on challenges already faced by the international community, for instance, in helping reduce the digital divide.

Key questions

- How to navigate and take the diversity of AI-related technologies and applications and the diversity of legal questions they raise into account?
- How to navigate the diversity of actors involved in the development and deployment of AI technologies, notably in terms of responsibility and accountability? Should future legal instruments on AI focus on sector-specific applications or on attempt to address the issue holistically,
- How will states apply traditional rules of international law to AI-related technologies and solutions, especially human rights law and humanitarian law?
- How to bridge the divide among States on the access to data for the development of AI technologies and more generally access to AI?
- How are AI-based solutions contributing, and how will they contribute, in the development, interpretation and enforcement of international law?

Conclusion

Beyond the three themes dealt with (data, cybersecurity and AI) and the three challenges identified (boundaries of the public/private, the politics of law in cyberspace, the digital divide), it was possible to raise a certain number of questions that could feed our future debates and research around already known legal themes:

- Sources of law, the formation of law, its interpretation and progressive development, the need for new rules;
- State competences, extraterritoriality;
- Proof and evidence;
- Liability and accountability;
- And, more theoretically, the nature and formulation of international law.

Digital issues and technologies are both a challenge and an opportunity for international law. The different subthemes highlighted some specificities for each of them. However, the technicalities of each issue should not be overestimated as many challenges and legal questions are shared by the three sub-themes.

annex 01

list of experts interviewed

(in alphabetical order)

- Ian Barber, Senior Legal Officer, Global Partners Digital.
- Rogier Creemers, Assistant Professor in Modern Chinese Studies, University of Leiden.
- Bertrand de la Chapelle, Cofounder and Director, Internet & Jurisdiction Policy Network.
- Viola de Azevedo Cunha, Senior Research Fellow, Unicef Office of Research.
- Carlo di Nicola, Senior Legal Officer, UNIDROIT—International Institute for the Unification of Private Law.
- David Emm, Principal Security Researcher, Kaspersky.
- Sherif Hashem, Professor of Information Sciences and Technology, George Mason University.
- Kubo Mačák, Legal Adviser, International Committee of the Red Cross.
- Angela McKay, Director of threats and risk mitigation, Google.
- Marko Milanovic, Professor of International law, University of Nottingham.
- Folake Olagunju, Program Officer of Internet and Cybersecurity, ECOWAS.
- Patryk Pawlak, Brussels Executive Officer, European Union for Security Studies & Project Director, EU Cyber Direct
- Kavé Salamatian, Professor of Computer Sciences, University of Savoie, & Head of European ERA Chair in CyberSecurity, Tallinn University of Technology.
- Alexander Seger, Head of the Cybercrime Division, Council of Europe.
- Johanna Weaver, Director of the Tech Policy Design Centre, Australian National University.
- Richard Wingfield, Head of Legal, Global Partners Digital.
- Moctar Yedaly, Deputy Minister, Ministry of Transport and Infrastructure of Mauritania.

The interviews

The content of the White Paper draws on a series of interviews, held between November 2021 and January 2022, on the issues of interest to the Committee (digital data, digital security, artificial intelligence and digital challenges in general). The Committee has selected legal and non-legal experts from a variety of professional backgrounds (academia, government, civil society, the private sector, *etc.*).

Each interview lasted 50 minutes and entailed a 10-minute presentation by the interviewee, followed by 40 minutes of discussion with the Committee. There were no strict requirements as to the content of the presentation.

IN THE SAME COLLECTION

Food / Agriculture

Anthropocene

Fight Against Corruption

Mass Crimes and Impunity

Law In Support of Democracy

Human Rights

Energy

Business and Human Rights

Outer Space

Civil Status

International Finance

Taxation

Global Governance / Multilateralism

International Investments

Migration

Digital Challenges for International Law

Ocean

Sdgs beyond 2030

Cultural Heritage

Intellectual Property

Dispute Resolution

Health

Labour

Cities in International Law

White Paper n° 16 - Digital Challenges for International Law
realisation: 23 July, 2022
graphic design: clémence hivert - *bluclemence@gmail.com*

www.ilaparis2023.org/en

Public consultation from September 1 to December 31, 2022

adi-ila2023-dinum@laposte.net

ADI / ILA 150 ANS/YEARS

2023 PARIS