International Rule on Cyber Governance

Pardis M Tehrani
University of Sunderland
University of Malaya

Introduction

Cyber activities have become an integral part of international relations.

The vast interconnectedness of networks, technologies and cyber processes across borders has brought societies and individuals from different nations closer together

Has opened up new opportunities for cooperation among both State and non-State actors.

This has created new vulnerabilities.

Applicability of international law

- Unlike many other international issues, the governance of cyberspace did not originate with states, but with the academic institutions and private actors who constructed the internet

- International law, however, is primarily a legal order for states (and their creations, like international organizations).

- International law does not hold a monopoly on the regulation of cyberspace . Given industry and civil society players, other regulatory regimes (for example, industry self-regulation) offer alternative vehicles.

- Necessity of the Geneva Convention

Existing position of the application of international law to cyber operations

- Both **global leaders** and **international legal experts** agree to the position that existing international law applies to cyber operations.

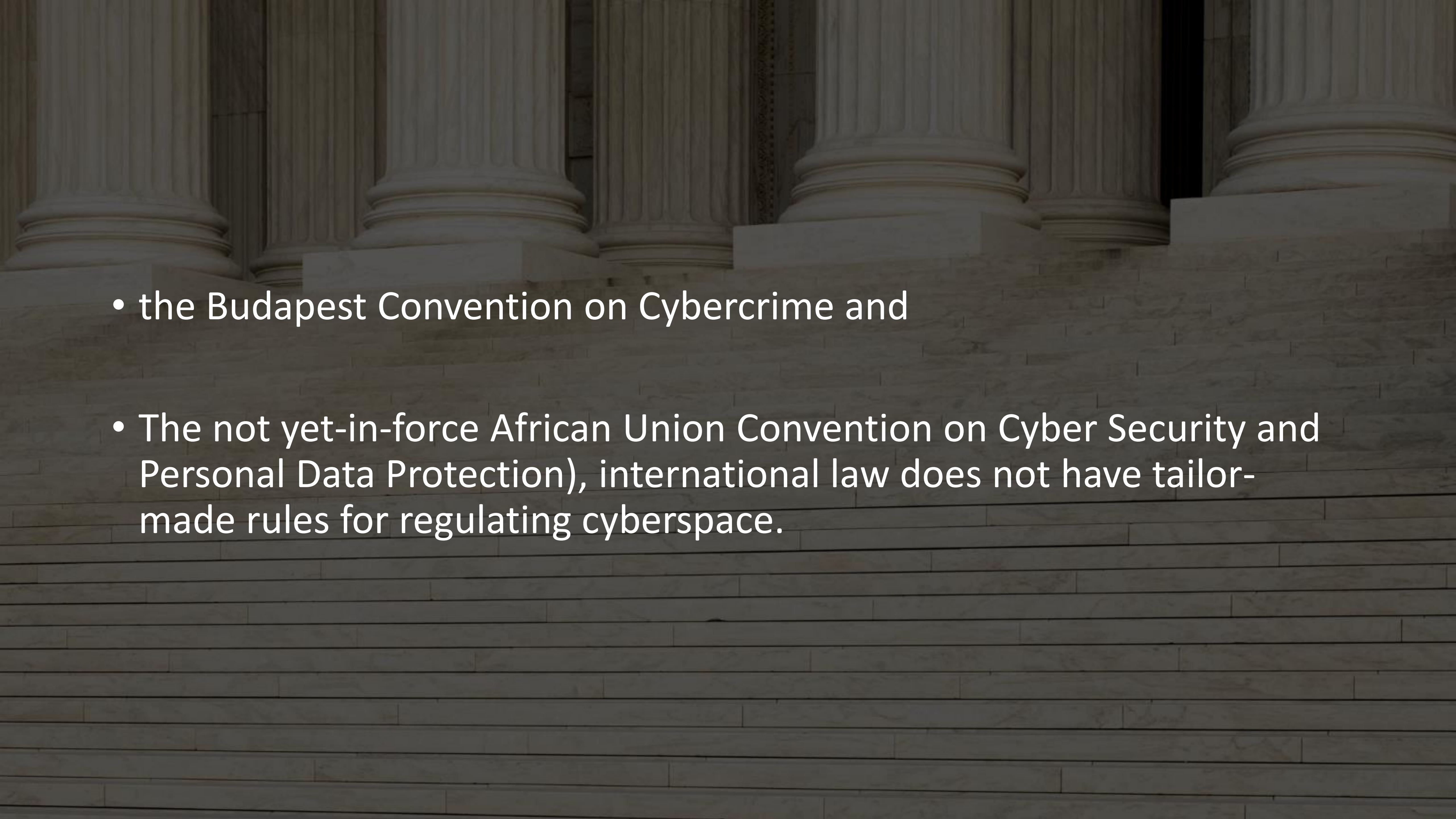
Today, most states and several international organizations have affirmed that existing international law applies to the use of information and communication technologies (ICTs) by states.

- UN General Assembly's First Committee on Disarmament and International Security,
- the G20
- the European Union
- ASEAN
- the OAS

The final **reports of the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace** manifest the commitment of global leaders towards the application of various express provisions and customary practices of international law to cyberspace

Two Tallinn Manuals: express the position of **international legal experts** on the international law applicable to cyber operations.

Additionally, case law and advisory opinions derived from the International Court of Justice have proved useful as precedents determining the future debates on the matter.



- the Budapest Convention on Cybercrime and

- The not yet-in-force African Union Convention on Cyber Security and Personal Data Protection), international law does not have tailor-made rules for regulating cyberspace.

- Not every single detail of how international law and its specific bodies apply to cyber operations is figured out today

- The sixth **UN GGE** on Responsible State Behaviour in Cyberspace, which concluded with a final report adopted by the UN General Assembly in July 2021, addressed many such divergences by allowing for closed-room deliberations and negotiations amongst 25 countries—including India and the five permanent member countries of the UN Security Council.

- On a larger scale, **the Open-Ended Working Group (OEWG)** on developments in the field of information and telecommunications in the context of international security—the final substantive report for which was released in March 2021—allowed for the participation of over 140 countries in deliberations surrounding the cyber applicability of international law.

General international law Applicable to Cyber space

- So many countries affirm that international law applies to the activities of every State in cyberspace. This includes the United Nations Charter (UN Charter) in its entirety and customary international law.

- They recognize the obligations of every State flowing from the
- principle of sovereignty to:
- refrain from the threat or use of force;
- settle disputes peacefully; and
- refrain from intervention in the internal affairs of other States.
- Some countries further recognize the obligations arising, in a non-exhaustive manner, from international human rights law (IHRL), international humanitarian law (IHL) and in relation to the law of State responsibility.

- Australia, Brazil, China, Czech Republic, Estonia (2019, 2021), Finland, France, Germany, Iran, Israel, Italy, Japan, Kenya, Netherland, New Zealand, Norway, Pakistan, Poland, Romania, Russia, Singapore, Sweden, Switzerland, UK (2018, 2021, 2022), US (2012, 2016)

Obligations of States under UN Charter

- Sovereignty

- Right to freely choose its political, social, economic and cultural system.
- No independent 'cyber borders' incongruent with a State's physical borders
- 'due diligence principle' : States are under an 'obligation not to allow knowingly their territory to be used for acts contrary to the rights of other States
- Attribution is another challenge as the threshold of physical harm needs to be fulfilled: physical effects and functional impairments

- Prohibition of wrongful intervention

- Not explicitly mentioned in the UN Charter. However, can be derived from art. 2 para. 1 UN Charter and is grounded in customary international law.
- Criteria for wrongful intervention, the conduct must (1) interfere with the domaine réservé of a foreign State and (2) involve coercion.
- Malicious cyber activities will only in some cases amount to direct or indirect use of force. However, measures below this threshold may also qualify as coercive. campaign

• Prohibition of the use of force

- The vast majority of malicious cyber operations fall outside the scope of ‘force’. However, cyber operations might in extrem is fall within the scope of the prohibition of the use of force and thus constitute a breach of art. 2 para. 4 UN Charter.
- Cyber operations can cross the threshold into use of force and cause significant damage in two ways.

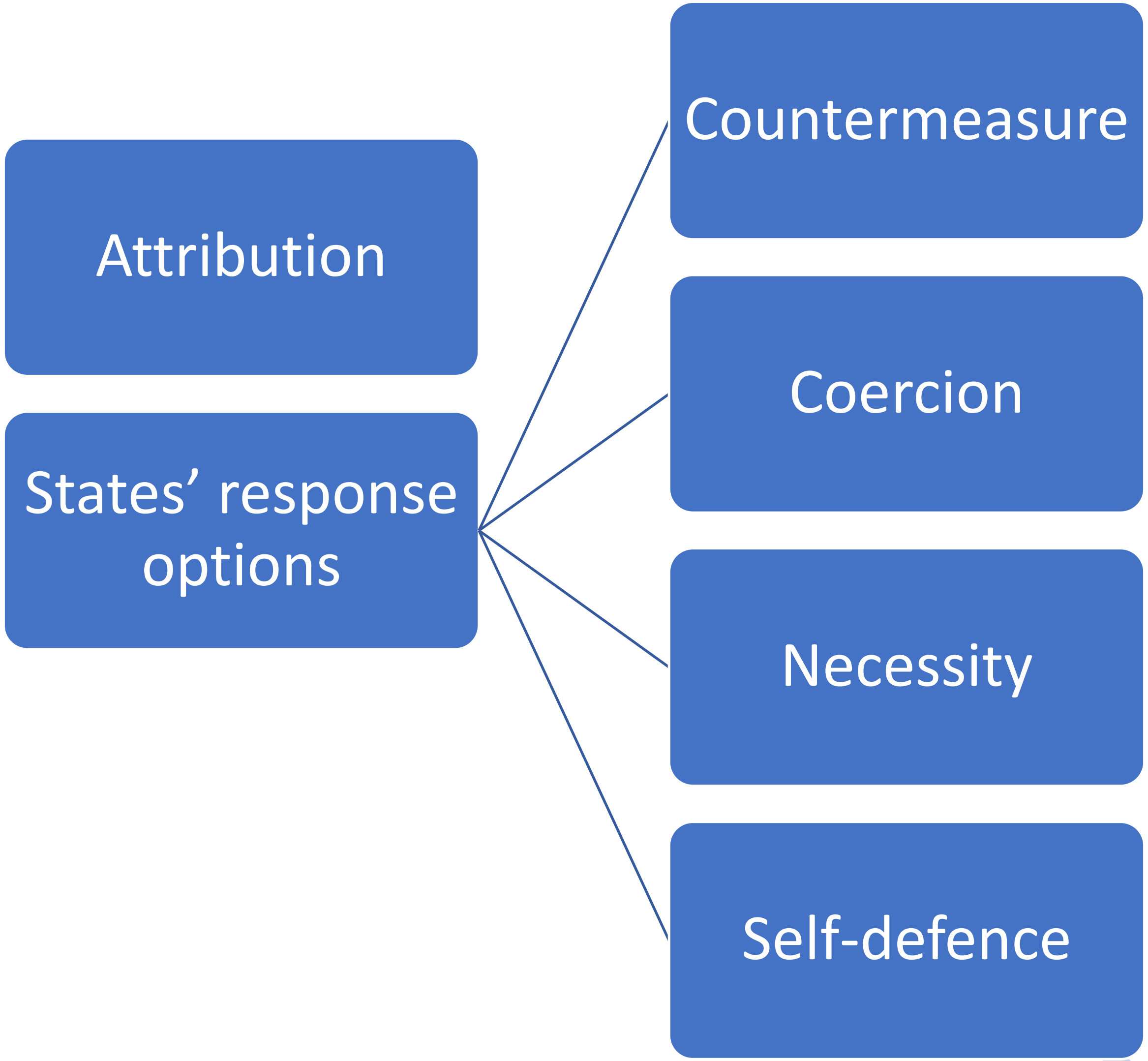
  1) They can be part of a wider kinetic attack
  2) Outside of a wider kinetic military operation, can cause serious harm and may result in massive casualties

- Tallin Manual 2 is on the view that the threshold of use of force in cyber operations must analogised to the ICJ’s Nicaragua Judgement; by the scale and effects of such a cyber operation
- and if it’s comparable, it would constitute a breach of art. 2 para. 4 UN Charter.
- The determination that if cyber operation having crossed the threshold of a prohibited use of force is a decision to be taken on a case-by-case basis.
- Based on the assessment of the scale and effects of the operation, the broader context of the situation and the significance of the malicious cyber operation will have to be taken into account.

- Qualitative criteria which may play a role in the assessment are
- the severity of the interference,
- the immediacy of its effects,
- the degree of intrusion into a foreign cyber infrastructure
- the degree of organization and coordination of the malicious cyber operation.

Obligations of States under international humanitarian law (IHL)

- Applicability of IHL in the cyber context
- The fundamental principles of IHL limiting the recourse to cyber operations in the context of an armed conflict
  - The prohibition of indiscriminate attacks and cyber operations
  - The obligation to take precaution in planning and executing a cyber attack
    - ✓ Take all feasible precautions in the choice of means and methods
    - ✓ Gathering intelligence on the network to assess the attack’s likely effects.
    - ✓ Inclusion of a deactivation mechanism or a specific configuration of the cyber tool which limits the effects on the intended target
    - ✓ obligation to conduct weapon reviews of any new means or method of cyber warfare



Attribution

States' response options

- Countermeasure
- Coercion
- Necessity
- Self-defence

Challenges of international law’s application to cyberspace

- (i) no specific treaty on cyber issues ;
  - Not all states have the legal capacity
  - No state practice
  - No customary international law on cyber space
  - Many states lack the personnel or resources to understand the issues involved in applying international law to cyberspace
- (ii) existential disagreements;
  - Disagreements: Among those states that have taken positions on international law’s application to cyberspace, there are a number of “existential” disagreements
  - Competing on inclusion exclusion of a particular international legal rule or regime
- (iii) interpretative challenges;
  - International legal regimes like nonintervention, sovereignty, and human rights

- (iv) Attribution:
  - International law only regulates its subjects of international law
  - It does not usually direct the behavior of ICT companies or individuals
  - Difficulty in identification of responsible body
  - More complicated where states employ proxies
  - International law has yet to fully Resolve how much control is required or what evidence must be shown to demonstrate it).

- (v) Accountability:
  - Although attributions of state and state-sponsored cyber operations may be on the rise, accountability has proved challenging.

Data governance issues in multidisciplinary ways

- The new data governance gradually developing, the maturity can be seen a departure from the one-size-fits-all approach towards conversations on how to regulate the different types of data, such as personal, corporate, public, health, etc.
- This will require a holistic approach that takes into account the standardisation, security, human rights, and legal perspectives.

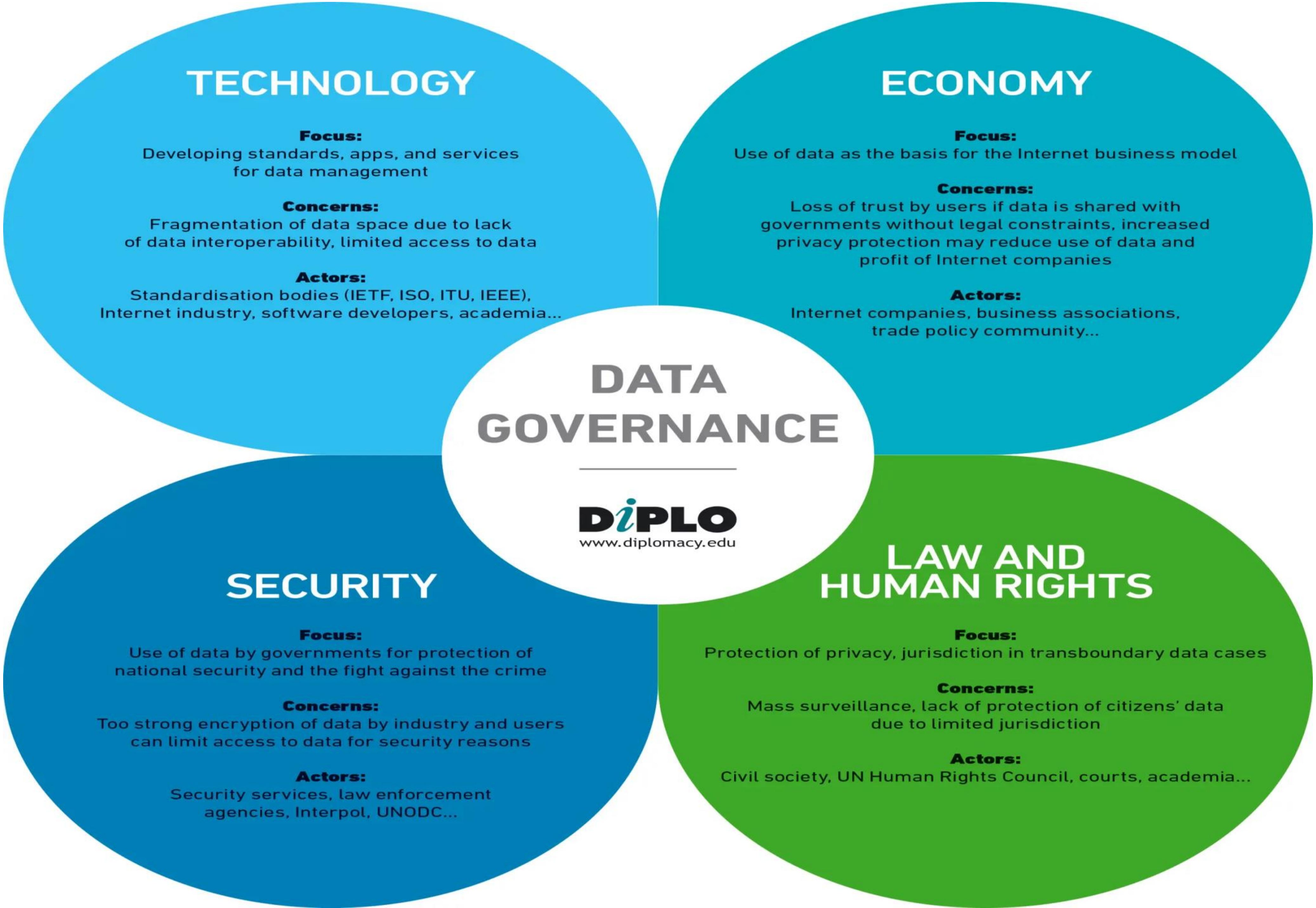
- Two aspects must reconcile by states:
  - ✓ The need to ascertain sovereignty over critical and sensitive data that needs to be stored physically on national territories
  - ✓ The fact that free flow of data across national and corporate borders facilitates economic development and contributes to the public good

- Win-win solutions are of course ideal, but realistically, governments will have to make optimal trade-offs between the two.

- We tend to group all kinds of data into one basket, but in reality, there are different kinds of data – from personal data to sector-specific and open data – all of which need a dedicated data governance approach.

- In 2023, data governance will mature with the realisation that we need as many governance approaches as there are types of data. Thus, the way we govern personal data needs to be different from the way we tackle scientific, business, or communal data.

- In 2023, countries, companies, and international organisations will have to address the multidisciplinary nature of data governance in holistic ways.



DATA GOVERNANCE

DiPLO
www.diplomacy.edu

TECHNOLOGY

Focus:
Developing standards, apps, and services for data management

Concerns:
Fragmentation of data space due to lack of data interoperability, limited access to data

Actors:
Standardisation bodies (IETF, ISO, ITU, IEEE), Internet industry, software developers, academia...

ECONOMY

Focus:
Use of data as the basis for the Internet business model

Concerns:
Loss of trust by users if data is shared with governments without legal constraints, increased privacy protection may reduce use of data and profit of Internet companies

Actors:
Internet companies, business associations, trade policy community...

SECURITY

Focus:
Use of data by governments for protection of national security and the fight against the crime

Concerns:
Too strong encryption of data by industry and users can limit access to data for security reasons

Actors:
Security services, law enforcement agencies, Interpol, UNODC...

LAW AND HUMAN RIGHTS

Focus:
Protection of privacy, jurisdiction in transboundary data cases

Concerns:
Mass surveillance, lack of protection of citizens' data due to limited jurisdiction

Actors:
Civil society, UN Human Rights Council, courts, academia...

Framework Suggestions

- Each country participating in the OBOR initiative may have its own set of laws and regulations related to cyberspace governance and development. These laws can vary significantly from one country to another.

- In the absence of a comprehensive regional framework specifically addressing cyberspace development in the OBOR countries, it is likely that each participating country would follow its existing domestic laws and regulations regarding cyberspace governance. These laws typically cover areas such as data protection, cybersecurity, electronic transactions, intellectual property rights, and online content regulation.
- It is important for businesses and individuals operating within the OBOR countries to be aware of and comply with the relevant domestic and international laws and regulations pertaining to cyberspace governance. As cyberspace is a rapidly evolving domain, countries may also be in the process of formulating or updating their legislation to address emerging challenges and technologies.

- Information and communication technologies are evolving fast, and so is the need to provide adequate legal assessments and to find responses to novel factual situations.

- While international law provides a sufficient framework to cope with the fast pace of technological change and remains applicable also to new developments**, its interpretation and effective application in the cyber context will increasingly be dependent on an in-depth understanding of technological intricacies and complexities**.
- This may require an intensified pooling of technical and legal expertise.
- How international law applies to State activity in the cyber domain, remains in significant ambiguity.
- International law as it stands is capable of providing essential guidance on state behaviour in and with regard to cyberspace.
- Uncertainties as to how international law might be applied in the cyber context can and must be addressed by having recourse to the established methods of interpretation of international law.
- Efforts and attempts to clarify the modalities of the application of international law in cyberspace are based on international exchange and cooperation.
- United nations' working groups on cyber and international security.
- these groups elaborate voluntary, non-binding norms for responsible State behaviour in cyberspace which may fulfil an important function in supplementing the existing 'hard' rules of international law.
- importance of States' reflecting and taking heed of the multifold and rich academic and civil society debates worldwide on the role and function of international law in the cyber context.