UNITED NATIONS UNIVERSITY
UNU-CRIS
Institute on Comparative Regional Integration Studies

LODZ CYBER HUB
University of Lodz

Summary Report from Sino-European Legal Workshop on

International Law of Critical Internet Infrastructure

edited by Joanna Kulesza and Berna Akçali Gur

On December 13, 2024, a workshop co-hosted by the Lodz Cyber Hub (LCH) at the University of Lodz Law School and the United Nations University – Comparative Regional Integration Studies (UNU-CRIS) was held to examine regional approaches to the governance of Critical Internet Infrastructure (CII). This event brought together speakers from European and Chinese universities to explore the application of international law to CII, with a particular focus on the rapidly evolving satellite systems in low Earth orbit (LEO) and the pressing challenges of safeguarding subsea infrastructure, such as telecommunications cables.

The workshop raised in-depth discussions on the unique legal frameworks adopted in Europe and China, analyzing the challenges and opportunities each region faces in the protection and management of CII. By comparing these governance models, the workshop sought to provide insights into their effectiveness and adaptability within the broader context of international law.

Key topics included the definition and significance of CII in both European and Chinese contexts, the legal frameworks governing CII in each region, and the role of regional cooperation in enhancing the security and resilience of CII. The event concluded with a Q&A session, where participants had the opportunity to engage with the panellists, deepening their understanding of the issues at hand. Through these discussions, the workshop contributed valuable perspectives on the evolving governance of critical infrastructure in the context of global technological advancement.

During the session, the following topics were discussed:

- Definition of CII: The concept and its significance in European and Chinese contexts were explained.
- Analysis of Legal Frameworks for CII in Europe and China: The legal frameworks governing CII in both regions were analyzed.
- Regional Cooperation: The role of regional cooperation in enhancing the security and resilience of CII was discussed, with a focus on existing international agreements, treaties, and platforms for collaboration.
- Q&A Session: Participants were given opportunities to actively engage with panelists, addressing their questions and reflections on the topics discussed.

This report is based on individual contributions from speakers, summarizing their interventions during the workshop. The workshop was hosted under Chatham House Rules, without recording, to facilitate open discussion.

Introduction

In the current climate of growing political tensions and shifting global power dynamics, it is more vital than ever to discuss the governance of CII. As digital technologies increasingly underpin national security, economic stability, and global communication, the management and protection of CII have become pivotal. Tensions between global powers, particularly in areas of cybersecurity, data sovereignty, and technological control, threaten to disrupt the stability of interconnected systems. By addressing these issues now, we can foster international cooperation, ensure resilient governance, and mitigate risks that could arise from politicized control over critical infrastructure in an increasingly fragmented digital world.

Both Europe and China are critical players in the global landscape of CII, with immense influence on the digital economy, cybersecurity, and the stability of global communications. Europe, with its regulatory frameworks such as the General Data Protection Regulation, has set standards for privacy, data protection, and multilateral governance, positioning itself as a leader in promoting digital rights and cooperation. On the other hand, China, as a major technological and economic power, plays a pivotal role in shaping the future of CII, particularly with its rapidly growing technological advancements and centralized governance model. Understanding the interplay between these two regions is essential for addressing the evolving challenges in global CII governance.

Section I: International Law and the Governance of LEO Satellites as CII

The Role of International Law in Governing LEO Satellites: A European Perspective

by Dr. Berna Akçali GUR, Lecturer in Space Law, Centre for Commercial Law Studies (CCLS), Queen Mary University of London; Associate Research Fellow, UNU - CRIS

The EU authorities' perception of satellite broadband services provided by mega constellations has shifted significantly in a short time, mainly due to the expanding applications of Starlink, the foremost operational satellite constellation deployed primarily in the LEO. Starlink has been crucial in reestablishing connectivity in various disaster zones, but its strategic value became especially clear to the EU through its deployment in Ukraine, a major and currently the only conflict area in Europe. As EU authorities monitored these developments, they recognised their need for autonomous access to space-based broadband infrastructure to protect their critical infrastructure and the risks associated with relying on external actors. Consequently, investment in an EU-based and EU-controlled satellite broadband infrastructure became a top priority. The EU Commission introduced the EU Secure Connectivity Programme, leading to the creation of the EU constellation Infrastructure for Resilience, Interconnectivity, and Security by Satellite (IRIS^2). In October 2024, the European Commission awarded a 12-year concession contract to the SpaceRISE consortium to develop, deploy, and operate IRIS^2.

The EU recognizes the importance of not only broadband services but also a broader spectrum of space-based infrastructures in safeguarding critical infrastructures. The ambitious IRIS^2 initiative underscores the importance of satellite systems to ensure the resilience of digital infrastructures and other critical infrastructures digitally connected, including energy and transport. The potential need to rely on satellite-based connectivity to ensure secure communication and support critical services during emergencies is concerning if the EU has to rely on external actors' services. Mitigating these security concerns demands urgent action, as the availability of resources necessary to establish such an infrastructure is limited. The radio frequency spectrum is essential for the space segment to communicate with the Earth, which is regulated at the domestic level by national authorities but coordinated at the international level by the ITU. It is a limited natural resource used by various communication systems, including radio and television broadcasting, mobile phones, and Wi-Fi networks. Like radio frequency, the LEO is not an endless domain. Its capacity is limited by physical availability, space traffic, and space debris. Broader international law recognises the limitations of these two resources.

These motivations are also reflected in the EU's regulatory and policy instruments. The Commission highlighted the need for more resilient and sovereign networks in the State of the Digital Decade Report 2023. The rationale for IRIS^2 is to establish a "sovereign, autonomous and secured connectivity infrastructure" to "support the autonomy and digital sovereignty of the continent." Consequently, the EU authorities, exercising their right under Article 189(2) of the Treaty on the Functioning of the EU to adopt measures related to European space policy, have initiated efforts to secure their presence in LEO and the new space race through investments in LEO-based broadband infrastructure to ensure protection of their critical infrastructure.

Comparative Legal Frameworks for Governing LEO Satellites in China: Challenges and Best Practices

based on presentation by Dr. LENG Xinyu, Associate Professor, China University of Political Science and Law

China's regulatory framework for the protection of Critical Information Infrastructure is structured through a tiered system of laws and regulations aimed at safeguarding vital sectors and ensuring resilience against threats. At the highest level is the Cybersecurity Law of the People's Republic of China, enacted by the National People's Congress in 2016. This law forms the cornerstone of the country's cybersecurity efforts, outlining foundational principles for the protection of critical infrastructure and securing networks vital to national security, economy, and public welfare.

Building upon the Cybersecurity Law, the Regulation on Protecting the Security of Critical Information Infrastructure, introduced by the State Council in 2021, provides specific guidelines for CII protection across key sectors such as telecommunications, energy, transportation, finance, public services, and national defense. It addresses risks such as physical damage, functionality loss, and data breaches, all of which threaten national security and public interests. This regulation establishes a framework for identifying and securing vital infrastructure.

Further elaborating on this framework, sector-specific measures were introduced to address the unique protection needs of particular industries. For instance, the Measures for the Administration of the Protection of Critical Information Infrastructure of Highways and Waterways, issued by the Ministry of Transport in 2024, focus on securing transportation and maritime infrastructure. These measures protect critical land and sea-based communication networks, including subsea cables and pipelines essential for global data transmission. Maritime security is further enhanced by the Provisions on the Administrative Law Enforcement Procedures of Coast Guard Agencies, granting maritime agencies authority to inspect critical infrastructure like submarine cables and pipelines. This reflects the increasing importance of undersea cables for telecommunications and data transmission, key to both global communication networks and national security.

Similarly, the Measures for the Administration of the Security Protection of Railway Critical Information Infrastructure, also introduced in 2024, address the security needs of the railway sector. These measures aim to protect the railway system, crucial for both domestic and international transportation, from cyber threats and physical disruptions.

As technology evolves, the scope of CII protection has broadened, especially with the rise of LEO satellite constellations. The G-60/Qianfan Project, for example, underscores the need for regulatory frameworks to secure satellite infrastructure, which is now considered critical. The risk of disruption to satellite systems, including telecommunication modules and remote sensing equipment, highlights the importance of robust legal safeguards.

Discussions on the application of International Humanitarian Law (IHL) to space-based infrastructure have gained traction. Concerns about the protection of space-to-ground intelligence systems from hostile actions have led to growing intersections between space law, IHL, and cybersecurity, emphasizing that CII protection is not only a national issue but also an international legal matter.

China's approach to CII protection is comprehensive, evolving from broad cybersecurity laws to sector-specific measures and addressing emerging technologies like satellite constellations. This ensures the security and resilience of the nation's critical infrastructure in the face of both traditional and emerging threats.

Section II: Governance of Subsea Infrastructure and Cross-Border Data Access – The Snowden Effect, Cybersecurity, and Jurisdictional Limits

Internet Infrastructure, Database Access, and Jurisdictional Boundaries in Chinese CII Governance

By Prof. PEI Wei, Professor, Beihang University

In China, Critical Information Infrastructure is defined by the Cybersecurity Law as network facilities and systems crucial to industries such as communications, energy, transportation, finance, and public services, where damage, malfunction, or data leakage could severely impact national security, economic operations, or public interests. This definition is based on a dual approach of assessing the industry significance and the potential consequences of disruptions. The 2021 "Regulations on the Security Protection of Critical Information Infrastructure" introduced a dynamic identification model for CII operators, which considers factors such as the importance of network facilities to industry operations, the potential harm of disruptions, and inter-industry dependencies.

China's CII framework employs a precise method for boundary determination, as outlined in the draft "Cybersecurity Technology – Method for Determining the Boundary of Critical Information Infrastructure." This approach classifies infrastructure into two categories: those providing common information services and those highly dependent on such services. It uses a systematic process based on the indispensability of software and hardware assets to critical business functions. To minimize the scope of CII designation, the framework adopts principles that limit operational elements, protect sensitive data, and reduce asset inclusion, ensuring a focused yet robust approach to identifying and managing CII components.

The governance of cross-border data transmission is a key element of the CII framework, with strict compliance obligations imposed on operators. These include data localization requirements, mandating that personal and important data collected domestically must remain stored within China, unless specific exceptions are met through rigorous security assessments. Personal data is categorized into general and sensitive information, with sensitive data—including biometrics, religious beliefs, and medical records—subject to heightened regulatory scrutiny. Important data is further classified based on its potential impact on national security, economic stability, or social order.

China's Data Security Law, Personal Information Protection Law, and Cybersecurity Law collectively form the foundation for regulating cross-border data flows, ensuring data sovereignty and security. Additionally, sector-specific regulations address unique compliance needs in areas such as healthcare, population genetics, and overseas securities issuance. For instance, companies seeking to list securities

abroad must adhere to stringent confidentiality and approval processes to manage sensitive or state-related data.

Strict restrictions are also placed on providing data to foreign law enforcement agencies, requiring prior approval from Chinese authorities. The framework's multi-layered approach to data classification and governance—spanning general, important, and core data—ensures proportionality in managing risks. Through its integrated legal regime, China aims to secure its Critical Information Infrastructure while addressing challenges posed by digital globalization and ensuring compliance with international standards.

Protection of Undersea Cables: Lights and Shadows of the International Legal Regime

By Dr. Annachiara ROTONDO, Junior Assistant Professor, Università degli studi di Napoli Federico II

Through an impressive infrastructure stretching around 1.3 million kilometres across the seabed, submarine cables form the backbone of the global telecommunications network enabling around the 99% of the world's voice, data and video traffic. However, they are extremely vulnerable being continuously exposed to natural hazards and anthropic threats, where the latter cause around the 80% of their faults. Hence, considering the extraordinary level of pervasiveness and interconnection reached by the submarine cables network and the number of interests at stake, it seems worth investigating the international legal regime applicable in case of breaking or injuring of such cables.

Sources of international law dealing with the breaking or injury of submarine cables are to be sought, prima facie, within international law of the sea and specifically in the 1982 United Nations Convention on the Law of the Sea (UNCLOS) that with regard to this specific subject matter encompasses the 1958 Geneva Convention on the High Seas and Continental Shelf and reflects, according to the prevailing opinion, customary law. Following its typical zonal approach, the said convention provides different legal regimes for the protection of submarine cables regardless their functions but according to their location.

Within maritime zones under states' sovereignty (either territorial seas or archipelagic waters) - where the most of faults occur since the shallow waters foster the much of human activities threatening submarine cables - cables' protection come into play in relation to the right of innocent passage. In particular, according to the Convention, States may adopt laws and regulations relating to innocent passage through their territorial sea in respect of the protection of cables. Thus, besides a general competence of enacting laws and regulations UNCLOS does not prescribe any positive obligation to prosecute submarine cables injuries in this area, with the consequence that such prosecution must be deferred to national legislation (eventually) adopted according to the prerogatives, needs and procedures of each single coastal State.

On the contrary, UNCLOS prescribes specific obligations in relation to criminal and civil liability for cable damages occurred within the high seas, the exclusive economic zone, and on the continental shelf. In particular, Article 113 extends - within given limits - the State's criminal jurisdiction on the basis of the 'flag-state principle' or the 'offender's nationality' principle, addressing legislative but not enforcement jurisdiction, i.e. avoiding prescribing prosecution or specifying minimum penalties. Moreover, Article 114 requires States to adopt laws and regulation on civil liability of cables owners under their jurisdiction for damages caused to another cable during laying or repairing their own one. Finally, according to Article

115 States must provide for an effective regime of civil liability aimed at ensuring that the ship owners who can prove to have sacrificed an anchor or any fishing gear for avoiding injuring a submarine cable shall be indemnified by the cable owner.

This legal framework, however detailed, is more than insufficient as it focuses on attributing responsibility for cable damage to the flag state or the offenders 'state, rather than giving jurisdiction to a coastal state or the cable user's state that are the real victims of cable damage. Therefore, considering that multilateralism is not (and never will be) a feasible solution to overcome the said enforcement gap, it seems worth reflecting on the role that international jurisprudence could play in updating the content of an old convention to the new challenges posed by the rise of a new global interest: i.e. undersea cables protection.

Section III: Application of International Law to CII – Recommendations and Challenges

The EU Renewed Approach for Improving CII Governance

By Prof. Paolo BARGIACCHI, Full Professor of International Law, Department of Economic and Legal Sciences, Kore University of Enna

The EU Directive 2022/2557[1] defines "critical infrastructure" as an asset, a facility, an equipment, a network or a system which is necessary for the provision of an essential service. CII describes both the essential Information Communication Technology (ICT) infrastructures and those essential for operating physical infrastructures.

In the EU legal system the concept of "critical" is linked to performing vital functions for the life of States, requiring a higher legal protection and being resilient from cyber incidents or threats.

In this field the latest EU legislation marks a significant change in at least two aspects: 1) previous Directive 2008/114[2] provided protective measures for infrastructure as object while new Directive 2022/2557 and Regulation 2022/2554[3] improve the resilience of the subjects, i.e. critical entities operating critical infrastructure, rather than of individual assets alone; 2) previous NIS Directive[4] only provided rules for cybersecurity while the NIS2 Directive[5] provides a horizontal legal framework for digital infrastructure sector's resilience.

[1] EU Directive EU 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[2] EU Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[3] EU Regulation EU 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.
[4] EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[5] EU Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

The EU legislation creates an enhanced and innovative ecosystem against cyber threats, applies an all-hazards approach, imposes comprehensive requirements on a large set of critical entities and calls for a solid level of harmonization among Member States' legislations in respect of the identification of critical entities.

Pursuant to Directive 2022/2557, critical entities are those public or private entities identified by a Member State as providing an essential service, i.e. a service which is crucial for the maintenance of vital functions, economic activities, public health and safety, or the environment. Critical entities, including third-country entities, are required to take technical, security and organisational measures in the name of resilience, describe and report them to the EU and its Member States, and undergo assessment, oversight and enforcement.

In particular, to strengthen financial entities' ability to monitor all ICT risks emerging at the level of third-party service providers, Regulation 2022/2554 provides that contractual arrangements on the use of ICT services must be harmonised to be tailored to the EU prudential standards and enable the rights of access, inspection and audit by the financial entity. Contracts can be terminated in case of breaches revealing a potential alteration of the performance or of evidence of weaknesses of the ICT third-party service provider in its overall ICT risk management.

The Eurosystem Oversight Policy Framework monitors the ICT third-party service providers' activities and exercise its powers also in third countries upon administrative cooperation arrangements. Penalties against designated critical ICT third-party service providers established in third countries are enforced and service providers have to establish a subsidiary within the EU if they want to provide ICT services to EU financial entities.

The spill-over effect of the EU legislation abroad requires an international framework of arrangements to be stipulated as soon as possible to guarantee both its effective implementation and the friendly development of international relations between the EU and the wider world.

The Role of International Law in Chinese Governance of Critical Internet Resources: Legal Solutions and Responses to Technological Challenges

By Dr. ZHU Lixin, Researcher and Director of the Institute of Cybersecurity Rule of Law, Institute of Technology and Education Development, Xi'an Jiaotong University

This presentation explored the intersection of international law, technology, and governance within the Chinese context, focusing on the management of Critical Internet Resources (CIR). It began by defining CIR, drawing from the perspectives of the Working Group on Internet Governance (WGIG) and Prof. Milton Mueller. WGIG encompassed the administration of the domain name system, IP addresses, root server system, technical standards, peering and interconnection, telecommunications infrastructure, and multilingualization. Mueller narrowed it down to the governance of internet standards, domain names, IP addresses, and interconnection and routing among service providers.

The governance of CIR was characterized by its unique, highly technical, and professional nature, with global and regional platforms typically adopting a multi-stakeholder approach. ICANN and RIR generally adopted a bottom-up, consensus-driven multi-stakeholder governance approach to control over these valuable resources. This involved a cooperative division of labor among community participants, decision-makers, and executors. However, traditional international law fell short in providing legal provisions for entities like ICANN.

Technological challenges loomed large in CIR governance. Cybersecurity threats were intensifying, impacting the security and stability of CIR. As IP and DNS-based services faced increasing attacks, DNS abuse was particularly difficult to contain. The rapid development of technologies such as big data, the Internet of Things, and IPv6 complicated IP address resolution, allocation, and management. AI technology introduced new governance challenges, enabling malicious actors to exploit it for cybersquatting, domain impersonation, and sophisticated attacks on IPs, domain names, and protocols.

China had implemented specific laws to govern CIR. The Measures for the Administration of Internet IP Address applied to units within China that directly obtained IP addresses from international institutions and those capable of allocating IP addresses for others. The state enforced record-filing management for IP address allocation and use, with the Ministry of Information Industry overseeing the filing process and managing a national internet IP address database.

The Measures for the Administration of Internet Domain Names aimed to regulate domain name services, protect user rights, ensure the safe operation of the domain name system, and promote the development of Chinese domain names and national top-level domain names. The Ministry of Industry and Information Technology supervised domain name services nationwide, formulating management rules, development plans, managing domestic domain name root servers and registration bodies, ensuring network and information security, protecting user privacy, and coordinating international domain-related matters.

International law played a role in China's CIR governance, with the country's Cybersecurity Law providing a legitimate basis for managing cyber power within an international law framework. The law sought to ensure network security, preserve cyberspace sovereignty and national security, protect the rights of citizens, legal persons, and organizations, and foster the healthy development of economic and social informatization. It encouraged international cooperation in cyberspace governance, technology R&D, standard formulation, and combating cyber violations and crimes, advocating for a peaceful, secure, open, and cooperative cyberspace and a multilateral, democratic, and transparent cyber governance system.

However, the multi-stakeholder governance model and international law alone could not effectively address the technical risks associated with CIR. Cooperation among countries based on cyber sovereignty, support for multi-stakeholder governance under international law, and transparent and democratic governance remained the primary approaches for CIR governance.

Summary and Recommendations

As global reliance on CII grows, further comparative studies between Europe and China are essential to understand the nuances of their respective legal regimes governing CII. While both regions face similar technological challenges, their regulatory frameworks, based on international law, exhibit significant differences in approach. Europe emphasizes multilateral governance and privacy protection, while China adopts a more centralized, state-driven model. Examining these contrasting frameworks will shed light on the strengths and weaknesses of each, offering valuable insights for improving CII governance and ensuring the security, stability, and resilience of global internet infrastructure.

Note on the Editors

Dr Joanna Kulesza is an Assistant Professor of International Law at the University of Lodz, Poland, specializing in internet governance, cybersecurity, and international human rights law. She has contributed significantly to research on the global regulation of the internet and the intersection of law and emerging technologies.

Dr. Berna Akçali Gur is a Lecturer in Space Law at the Centre for Commercial Law Studies, Queen Mary University of London, and an Associate Research Fellow at UNU-CRIS. Her expertise spans space law, international governance frameworks, and the legal implications of cybersecurity and space technologies.

Kulesza and Akçali Gur have been collaborating on the **Global Governance of LEO Satellite Broadband** project, funded by the Internet Society Foundation as part of its **Decolonizing the Internet** program. Currently the project focuses on "Trust and Data Governance," exploring legal frameworks around LEO satellite broadband.

This workshop builds upon the work of the Sino-European Expert Working Group on the Application of International Law in Cyberspace, coordinated by the Geneva Center for Security Policy, the EU Institute for Security Studies, China Institutes of Contemporary International Relations, and Xiamen University Law School. However, the content of the workshop and individual contributions to this report are independent of these institutions, with speakers presenting their views autonomously.