REMIT

Reignite Multilateralism via Technology

Summary of the first REMIT Conference

New Perspectives for Technology and Multilateralism

Held on May 16-17, 2024 at KU Leuven

This event was been organized by the REMIT project, funded from the European Union's Horizon Europe research and innovation programme under grant agreement No 101094228.
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Overview of the first REMIT Conference, May 16-17, 2024

The 1st REMIT conference took place in Leuven, Belgium on May 16-17, 2024. The conference, mostly in-person, but containing a hybrid element for selected sessions, drew 97 attendees over the two days, 4 of whom were online listeners. As the inaugural conference had 114 registrations, the very high percentage of participants is a point of pride for the project, as well as showing the importance of the research done.

In addition to standard registration, the conference had a Call for Contributions, looking for those from young researchers for a panel-format plenary session, and PhD candidates for a more conversational PhD Special Session. The former ended up garnering so many strong applications, the planned plenary was instead split into parallel sessions based on the topics.

The conference consisted of 13 thematic sessions, and an additional PhD special session following the closing lunch. Of the 13, 8 were held in a parallel format.There were also 5 plenaries of which 4 either were or contained keynotes, and one had a roundtable format:

- **Plenary Opening Session**
    - Opening words by Prof. Roberta Haar (Maastricht University), and Prof. Joep Crompvoets (University of Leuven)
    - Keynote: Prof. Luc Soete (Maastricht University) on "Science, technology and innovation in a new geopolitical landscape"
    - Keynote: Christian-Marc Liflände r (Head of NATO Cyber & Hybrid Policy Section) on "Strategic Competition – Adjusting to an Era of Unpeace"
- **Plenary Keynote**: Prof. Mariarosaria Taddeo (University of Oxford) on "The Ethics of AI in Defence" (*introduction by prof. Paul Timmers, University of Leuven)*
- **REMIT Stakeholder Advisory Board Roundtable**

  Prof. Nicholas Thomas (City University of Hong Kong)

  Prof. Luca Belli (FGV Law School)

  Prof. Mariarosaria Taddeo (University of Oxford)

  Moderator: Prof. Roberta Haar (*Maastricht University)*
- **Plenary Keynote**: Prof. Bart Preneel (University of Leuven) on "Global supply chain risks in software and hardware"
- **Plenary Closing Session**
    - Keynote: Prof. Peggy Valcke (University of Leuven) on "Council of Europe and Artificial Intelligence"
    - Keynote: David Ringrose (Digital Transition & Global Gateway at European External Action Service EEAS)
    - Closing words by Prof. Roberta Haar (Maastricht University), Prof. Joep Crompvoets (University of Leuven), and Prof. Paul Timmers (University of Leuven)

The parallel sessions were organized by individual project partner organizations, and were as follows:

- **Session 1 The Dynamics of the Multilateral Approaches in the Context of the Two Wars in the EU's Geopolitical Neighbourhoods** (by Babeș-Bolyai University)

  Moderator: Prof. Valentin Naumescu, Babeș-Bolyai University, Romania

  Speakers: Mihnea Motoc, Principal Adviser, IDEA, European Commission; Prof. Valentin Naumescu, Babeș-Bolyai University, Romania;

Lt. Col. Curtis Cordon, Air, Space and Nuclear Policy Advisor to USA NATO Delegation;

Assoc. Prof. Raluca Moldovan, Babeș-Bolyai University, Romania;

Andrei Enghis, Policy Officer, European Commission;

Florina Caloianu, Babeș-Bolyai University, Romania

- **Session 2 Digital Governance between Multi-stakeholderism and Multilateralism** (by University of Bremen)

  Moderator: Dr. Dennis Redeker, University of Bremen, Germany;

  Speakers: Prof. Luca Belli, FGV Law School, Brazil;

  Dr. Jamal Shahin, Brussels School of Governance/University of Amsterdam/United Nations University-CRIS (Bruges);

  Dr. Julia Pohle, WZB Berlin Social Science Center;

  Elena Plexida, ICANN;

  Dr. Nicola Palladino, University of Salerno, Italy

- **Session 3 The Governance of Strategic Technologies: Geopolitics and Advocacy** (by Finnish Institute of International Affairs and LUISS Guido Carli University)

  Moderator: Dr. Katja Creutz, Finnish Institute of International Affairs, Finland

  Speakers: Prof. Thomas Christiansen, LUISS Guido Carli University, Italy;

  Dr. Ville Sinkkonen, Finnish Institute of International Affairs, Finland;

  Prof. Sophie Vanhoonacker, Maastricht University, Netherlands;

  Catherine Yuk-ping Lo, Maastricht University, Netherlands;

  Mahmoud Javadi, Erasmus University, Rotterdam, Netherlands;

  Siyan Amber Qiao, Maastricht University, Netherlands;

  Dr. Max Smeets, European Cyber Conflict Research Initiative

  Discussants: Prof. Mariarosaria Taddeo, University of Oxford, UK;

  Prof. Nicholas Thomas, City University of Hong Kong, China

- **Session 4 The Interconnections Between Cybersecurity and Critical Technologies** (by European Cyber Conflict Research Initiative)

  Moderator: Dr. James Shires, ECCRI, United Kingdom

  Speakers: Alžběta Bajerová, NATO, Belgium

  Jakob Bund, European Cyber Conflict Research Initiative (ECCRI), Germany

  Nikolas Ott, Microsoft, Belgium

  Dr. Alexandra Paulus, German Institute for International and Security Affairs (SWP), Germany

- **Session 5 Regulatory sandboxes with a focus on AI** (by University of Leuven)

  Moderator: Triantafyllos Kouloufakos, University of Leuven, Belgium

  Speakers: Filippo Bagni, PhD Candidate in Law &Technology, Scuola IMT Alti Studi Lucca, Italy;

  Nils Brinker, Senior Cybersecurity Expert at Intcube;

  Katerina Yordanova, IMEC KU Leuven, Belgium;

  Dr. Taina Junquilho, University of Brasília, Brazil;

Kai Zenner, European Parliament

- **Session 6 Related initiatives on technology & multilateralism** (by University of Leuven) *Moderator: Prof. Paul Timmers, University of Leuven, Belgium*

  Speakers: Prof. Roberta Haar, Maastricht University, The Netherlands;

  Prof. Hylke Dijkstra, Maastricht University, EU Support for Global Governance Transformation (ENSURED Horizon project);

  Prof. Maria Grahn-Farley, University of Gothenburg, Human Rights Justification (HRJust Horizon project);

  Prof. Daniel Mügge, University of Amsterdam (Regulaite Initiative), Netherlands

- **Young Researchers Panel 1: Quantum and Multilateralism** (by University of Leuven) *Moderator: Aysajan Abidin, University of Leuven*, *Belgium*

  Speakers: Raluca Csernatoni, Carnegie Europe,

  Andrea Rodriguez Garcia, ImpaQT;

  Kristiaan De Greve, KU Leuven, Belgium;

  Wouter Castryck, KU Leuven, Belgium;

- **Young Researchers Panel 2: AI and Multilateralism: Consensus under the Fragmented Governance?** (by Maastricht University)

  Moderator: Prof. Daniel Mügge, University of Amsterdam

  Speakers: Mahmoud Javadi, Erasmus University Rotterdam;

  Maya Müller-Perron, Maastricht University;

  Hengyi Yang, Maastricht University;

  Zhanwei Wang, Maastricht University;

  Siyuan Qiao, Maastricht University

Conference dissemination focused mainly on directing traffic to the project's website, with a conference subpage for all relevant information (as of June 17, 2024, having garnered around 2300 impressions) and news posts with more in-depth introductions into each session. This communication was further supported by posts about major updates on REMIT's social media channels in Twitter/X and LinkedIn.

Photos from the conference, taken by local photographer Luk Collet were published on REMIT website: https://www.remit-research.eu/events/conference/remit-conference-gallery-is-here/

Table of Contents

Summary of the Opening plenary

Prof. Joep Crompvoets: Introduction and welcome

Prof. Roberta Haar: Fabric of multilateralism is under strain. Rapid development of technology leaves us bewildered; we want to be a beacon of optimism. Int. Comm. Is grappling with profound uncertainties. Global south is growing uncertain about partners in the West. EU partners facing concerns about climate change. Will the US remain a steadfast security and defense ally?

We'll focus on digital governance, emerging technologies and AI at the conference. We hope to be collaborative with our audience. We hope to move toward a future where technology can be a catalyst for multilateralism.

Keynote presentation by Prof. Luc Soete on Science, technology and innovation in a new geopolitical landscape

In an insightful keynote address, Professor Luc Soete, an esteemed professor of international economics, explored the intricate relationship between trade, economics, and geopolitics. He began by reflecting on his role as an educator, teaching students about the "welfare gains" of trade and the ideal of returning to an economic paradise through open trade. However, he acknowledged that his discipline is currently facing a crisis.

Professor Soete highlighted the European Union's (EU) foundational principle of economic primacy in international relations, noting that this principle earned the EU the Nobel Peace Prize in 2012. The EU's commitment to open science, innovation, and transparency exemplifies its core values of democracy. For instance, the exchange of carbon credits underscores this intrinsic openness.

However, he pointed out that the primacy of economy in international relations is under strain. Economic sovereignty has always been central to the EU, with hopes that the EU's economic relationships could be insulated from geopolitical interference. Yet, it is increasingly evident that major global players like the US and China do not separate economics from geopolitics.

Addressing the feasibility of an open, EU-level industrial policy, Professor Soete discussed the impact of the shift from fossil fuels to renewable energy. He emphasized that this transition introduces geographical considerations, such as the availability of sunlight and wind, which will influence the location of energy-intensive industries. He lamented the lack of sufficient discussion on this topic at the European level.

Professor Soete critiqued the concept of "competitive sustainability" as being space-blind, advocating for security to be integrated as a new research and innovation (R&I) policy aim. He proposed that resilience, de-risking, and economic security should be new policy objectives, although he cautioned that economic security is a complex and potentially problematic concept, possibly even hindering risky yet necessary R&I efforts.

He offered three concrete proposals to address these challenges:

1. **From the ERA to a European Defense Research and Innovation Area (EDRIA):** This would not challenge individual member states' national security responsibilities but would allow for a parallel European competence, complementing the security provided by NATO.
2. **Enabling Dual Use in European R&I:** By linking the construction of the EDRIA more closely with the European Green Deal and the digital agenda, opportunities for dual-use innovations can be better exploited.
3. **From Cohesion to European Territorial Security Policy:** This involves transferring resources from wealthy central regions to the periphery, including in terms of defense production and military facilities, thus incorporating security elements into the EU's cohesion policy.

In conclusion, Professor Soete underscored the necessity of integrating security into the EU's economic and innovation policies to navigate the intertwined challenges of geopolitics and economic sovereignty.

His proposals aim to foster resilience and ensure that Europe can maintain its values of openness and democracy while addressing contemporary global challenges.

Keynote presentation by Christian-Marc Liflander on Strategic Competition – Adjusting to an Era of Unpeace

In a compelling keynote address, Christian-Marc Liflander highlighted the precarious geopolitical landscape in the Euroatlantic area, emphasizing that peace is far from assured. He pointed out that Russia has flagrantly violated international norms that previously maintained stability. Liflander stressed the interconnected and global nature of contemporary threats, often posed by authoritarian actors challenging our values and way of life.

He delved into the realm of cyberspace, describing it as a domain of malicious activities—referred to as "cybrid" or "hyber" threats—that undermine multilateral norms. Liflander underscored the challenge of long-term competition with adversaries who operate just below the threshold of open conflict, engaging in deniable hostile actions against democratic institutions and the global economy. These operations, he noted, are less about a catastrophic event like a digital Pearl Harbor and more about the cumulative effect of continuous, smaller-scale actions that can have significant impacts over time.

Liflander illustrated his point with the ongoing conflict in Ukraine, where cyber-attacks have been a critical component since 2014, long before the full-scale invasion in 2022. These attacks, including those deploying data-wiping malware, can paralyze nations and have spillover effects beyond Ukrainian borders. NATO has observed increased warnings of potential attacks on its national infrastructures, reinforcing the notion that cyber means can achieve substantial, albeit gradual, effects.

He advocated for a focus on long-term resilience, acknowledging that it is impossible to defend everything, everywhere, all at once. Liflander cited Lithuania as an example, facing hybrid attacks not only from Russia but also from China after significant geopolitical shifts.

Liflander also addressed the blurred lines between cyberspace and technology, noting that AI and quantum computing are dual-use technologies. He warned that strategic competitors, particularly China, are investing heavily in these areas with little regard for human rights or shared values. A fully operational quantum computer, he cautioned, could decrypt all current encryption technologies, posing a significant threat.

To counter these challenges, Liflander mentioned initiatives like DIANA and the Defence Innovation Fund, designed to drive innovations that protect against tech-infused attacks. He emphasized the importance of preparing for upcoming summits, such as the Washington summit, to protect national infrastructures and enhance diplomatic and defensive capabilities.

He concluded with a call for stronger public-private partnerships, highlighting the critical role the private sector played in Ukraine's cyber defense. Liflander asserted that maintaining a free and secure cyberspace requires systematic and long-term collaboration between governments and industry. He remained optimistic, stating that while the competition is fierce, outperformance is possible through better engagement and cooperation. Liflander emphasized that the protection of freedom and values must take precedence over free trade and profit.

Session 1. The Dynamics of the Multilateral Approaches in the Context of the Two Wars in the EU's Geopolitical Neighborhoods

Moderator: Valentin Naumescu (Babeș-Bolyai University)

Speakers: Valentin Naumescu (Babeș-Bolyai University), Curtis Cordon, (USA NATO Delegation), Raluca Moldovan (Babeș-Bolyai University), Andrei Enghis (European Commission), Florina Caloianu (Babeș-Bolyai University)

The session included five presentations on several perspectives linked to the issue of multilateralist dynamics in the EU's Eastern and Southern neighborhoods and whether it might help mitigate the consequences of the two wars currently affecting these regions: the Russia-Ukraine war and the war between Israel and Hamas in Gaza. The presentations focused on issues of military technology, international relations, geopolitics and the role of international organizations and institutions from a variety of perspectives, given the speakers' diverse backgrounds and expertise.

Valentin Naumescu's presentation tackled five components: conceptual clarifications, the ACF framework, the implication of Joe Biden's victory for multilateralism, geopolitical approaches, and the technological competition in the Black Sea region. The ACF framework due to its versatility can be employed in relation to the understanding of minilateralism and the increasing role of middle powers, as well as providing an explanation for the so called "double game" of powers such as Turkey, UAE, Saudi Arabia, Egypt. In the Black Sea region, as an example of versatility, Turkey's initiatives have been tackled to portray the effects of employing minilateralism while maintaining presence in multilateral frameworks. The case study portrayed the use of drones in the Ukraine war, including insights on Turkey's and Iran's role as producers and suppliers of drones. The conclusions drew upon the utility of sanctions in deterring aggressors, the reduced adaptability of large formats such as the UN, the impact of internal transformations within Western societies on multilateralism, the increased role of Global South and mid-level powers, and the renewed appreciation for minilateral frameworks.

Curtis D. Cordon's presentation started with an appreciation for the importance of the topic and the integrated air and missile defense (IAMD) – why does it matter, and what can be noted in relation to the changes concerning the conflict in Ukraine and its implications in relation to multilateralism. In the first segment, to define IAMD, its role in protection against missiles, drones and bombs needs to be noted.

The implication of multilateralism in relation to IAMD, is crucial. The war in Ukraine introduced the duo of cheap but highly developed technology, hinting at the cost advantages of using drones which provide an important role in surveillance as well as the prospective of employing them in attacks. The producers of IAMD are primarily private entities. The use of drones in Ukraine needs to be signaled because this conflict is the first one in which drones are used exponentially for big fights, and the demand for more grows as days go by.

The importance of IAMD for NATO tackles the prospect of victory, which would be achieved via securing victory in the air first and that every country can be regarded as a frontline in relation to IAMD.

In the introduction of **Raluca Moldovan's** presentation, the growing use of small cooperation had been stressed in contrast with large frameworks associated with multilateralism, as well as the role of narratives in the shift towards minilateralism. The axis of disruption (Russia, China, Iran and North Korea): driven by anti-liberal world order sentiments, gathered a strong hold on relativist narratives in which democracy can be interpreted to the point of stripping institutions and norms of their values. There persists a trend of downplaying the growing significance of the growing cooperation among these disruptive actors since it creates a false sense of security. Washington's hesitancy comes in handy for pro-active actors in the region such as Iran which thrive on chaos, as well as more demure states such as Saudi Arabia, UAE, and Qatar that prefer to balance multiple relations rather than increase tensions through various ruptures.

Andrei Enghis' presentation tackled four main topics: geostrategic importance, its importance for the Russian Federation, NATO and EU's responses towards the Black Sea region, and the expectations set and intended to be achieved in relation to the Black Sea.

A brief overview of the Black Sea's importance for empires across ages had been stressed, with a strong emphasis on Russia's interests in the region, geographical considerations, energy routes as well as the importance of maritime resources for neighboring states with access to the sea.

The presentation of UBB's PhD Candidate **Florina Caloianu** began with the definition and brief overview of the term and the application in relation to Russia's aggression in Ukraine, including further actions in the Eastern Neighbourhood. The following section focused on the tools used, among them information warfare, disinformation in conflict and peace time alike, economic coercion and cyber-attacks. The third section, concerning Russia's employment of sharp power in Ukraine as well as neighboring countries, tackled the disinformation campaigns, fake news, dependency on Russian gas, and the religious dimension introduced by Peter Mandaville. China's employment of sharp power had been mentioned but because the effects have been limited in the Eastern Neighbourhood, the topic represented a brief note on the topic. Finally, in the last section of the presentation, the multilateral responses in relation to disinformation, cybersecurity cooperation and economic resilience have been tackled showcasing the multiple actors involved in tackling mainly Russia's employment of sharp power tactics, among them EU, NATO, international, organizations, and civil society.

Session 2: Digital Governance between Multi-Stakeholderism and Multilateralism

Moderator: Dennis Redeker (University of Bremen)

Speakers: Luca Belli (FGV Law School), Julia Pohle (WZB Berlin Social Science Centre), Elena Plexida (ICANN), Nicola Palladino (University of Salerno), Jamal Shahin (Brussels School of Governance/University of Amsterdam/United Nations University-CRIS)

In the session's introduction, moderator Dennis Redeker pointed out that whilst the REMIT project focuses on "multilateralism" in global technology governance, it is a term normally applied in the context of defense and security (e.g., uni-/bi-/multi-lateralism). Across many fields of (global) digital governance, the roles of state actors are not clear, instead, there have been multiple stakeholders involved, and states also feel scared of the decreasing impacts of multilateralism in global digital governance, and they take actions. Therefore, digital governance nowadays works between multi-lateralism and multi-stakeholderism, this session focuses on the tensions between the two approaches.

Julia Pohle spoke about how the geopolitical landscape nowadays has experienced a major shift, which has led to a geo-politicized internet governance. Although multi-stakeholderism has become the mainstream narrative for Internet governance, the nature of the Internet should be reflected. States, even democracies, regulate the application layers and technologies, for example, the digital transformation and internet infrastructure, which is good for citizens. But meanwhile, these measures also strengthened digital sovereignty and then supported multilateralism, instead of multi-stakeholderism.

Elena Plexida explained that from the technical angle as ICANN holds, the actual policymaking process is multi-stakeholderism, but ICANN also needs to coordinate multilateral impacts from the states. The global Internet governance is fragmented, as stakeholders are also decision-makers in the field of the Internet, which is quite different from other fields.

Jamal Shahin presented from the IR angle, why multi-stakeholderism is important. Because separate ways of thinking about Internet governance based on pragmatic reflection are needed, for example, technical organisations are needed to develop expertise to govern the Internet outside the government. Different models are needed to make decisions, bring people onto the same page, and understand each other. The second point is the tensions of global digital governance are not only between the UN and the member states but also within the UN. Lastly, different definitions of the Internet and the governance models need to be clarified. In general, the main idea of multi-stakeholderism is to bring civil societies into the dialogue, however, multi-stakeholderism might mean different things or approaches for different groups.

Luca Belli clarified that multi-stakeholderism is not THE only approach, it contains diverse types and meanings; multi-stakeholderism does not only explain the decision-making process but also means solutions for policymaking, which indicates we can not only rely on state enforcement. Multi-stakeholderism is a good model and option, however, it is not universal, as it sometimes represents unilateral regulations. For example, ICANN is possible as a unique organization to regulate the Internet because it represents the US's intention, so global Internet governance here is a good model, but not replicable and hard to impose into systems like AI governance. In BRICS countries, Brazil's digital governance is implemented by private sectors but also improves its digital sovereignty, it is a good case to realize both. China applies state-led multi-stakeholderism, which means private sectors do not challenge the authority but still convey opinions. Besides the multi-stakeholderism, there are also many other effective models, it should not be the only "right" model.

Nicola Palladino added that AI has been the most digitalized system and is embedded into digital governance and Internet governance. Regulation aims to balance risk and safety for the better benefit of society. The best ecosystem is to include fundamental rights which give access to technology and development but also set the boundary. Conventionally, principles need to be embedded into the technology, however, digital technologies are different, they are created by a new layer of governance, which is the infrastructure of digital technologies. There are pros and cons to both models, but entirely the

governance is in fragmented way, combining regime complex and framework convention. For example, IOs are setting the principles like laws of human rights, while other actors are also involved: AI providers, EU standard organizations, EU legislation, ISO…

Session 3: The Governance of Strategic Technologies: Geopolitics and Advocacy

Moderator: Katja Creutz (Finnish Institute of International Affairs)

Speakers: Thomas Christiansen (LUISS Guido Carli University), Ville Sinkkonen (Finnish Institute of International Affairs), Sophie Vanhoonacker (Maastricht University), Catherine Yuk-ping Lo (Maastricht University), Mahmoud Javadi (Erasmus University Rotterdam), Siyan Qiao (Maastricht University), Max Smeets (European Cyber Conflict Research Initiative)

Discussants: Mariarosaria Taddeo (University of Oxford), Nicholas Thomas (City University of Hong Kong)

The aim of the session was to provide insights into two special issues being produced within Work Package 4 of the REMIT project, one focusing on the Geopolitics of Technology Governance for the journal Geopolitics and edited by Thomas Christiansen, Ville Sinkkonen and Sophie Vanhoonacker, the other exploring global governance of strategic technologies through the Advocacy Coalition Framework (ACF) for The Forum of the International Studies Review (ISR), convened by Catherine Yuk-ping Lo, Michal Onderco and Carolina Polito.

Thomas Christiansen introduced the aim of the special issues including the outline for the special issue for Geopolitics. He noted that in terms of geopolitics, the main emphasis is on the EU, the United States and China although the special issue also features contributions analyzing international organizations as well as India, Africa and Russia, to name a few.

Sophie Vanhoonacker addressed the European Union in her presentation, explaining that the EU is not a military power, but has a strong tradition as a normative and economic power, through which it enforces influence. In the study undertaken by Vanhoonacker, Christiansen and Flavia Lucenti, the authors argue that the EU's approach vis-à-vis regulation is very strong, and the Union has conducted very far-reaching regulatory activities in the realm of strategic technologies. The EU will not just have a domestic impact but also international. Strategic technology governance has been driven by domestic factors; foreign policy concerns play an important role. In the process, the EU also continues to support multilateralism.

Ville Sinkkonen, presenting a joint paper co-authored with Robert Haar, argued that the US fixation on competition with China has led to policies that are not oriented toward multilateralism. There are three competing coalitions with respect to strategic technology and China in the US – the multilateralists, the new-isolationists and the flexilateralists. Multilateralists deem decoupling impossible and especially remind that it is impossible to force the global South to decouple from China. They are also willing to maintain a dialogue with China on strategic technologies. New isolationists see Chinese Communist Party as the greatest threat, and they consider letting China into the WTO a big mistake. In the views of the isolationists, the US must use tariffs, secondary sanctions and bans on Chinese technology. Flexilateralists consider that engagement with China has failed, and that the Taiwanese threat is urgent. But favor international cooperation through strengthening US alliances in Indo-Pacific. Yet they have pushed for tariffs against China and domestic subsidies in critical technologies. The current administration has become largely flexilateralists lately.

The discussant **Mariarosaria Taddeo** discussed governance of AI and its general features. She noted AI governance must be both outward and inward looking – AI is produced in different places and sold in different markets. AI is increasingly a factor of growth in countries, also becoming an element of political discussion. Taddeo argued that its governance must be inclusive, multistakeholders are important. AI is going to be an enabler of services and infrastructure. Therefore, one should be careful in avoiding definitive polarization in AI governance.

The first panelists of the session were asked about the EU taking a more active role in bolstering its Brussels effect, and whether AI is a dangerous thing that should be regulated.

The second panel within the session was composed of authors to the ISR Forum on the global governance of strategic technologies and the ACF. Catherine Yuk-ping Lo from Maastricht University explained that

with the ACF they intend to explore policymaking process at the global level, as a product of the political dynamics occurring in international policy subsystems, which are shaped by the corresponding national and sub-national policy subsystems, and vice versa.

Mahmoud Javadi presented the merits of ACF over Alliance Theory and argued that studies of international security-based policy subsystems can enlarge the remit of ACF applications.

Siyuan Qiao spoke about cryptocurrency governance and different advocacy groups in the US. More specifically she addressed how internal events, such as the FTX collapse, could affect the policy subsystem heavily and drive regulatory changes.

Max Smeets presented his research on cyber warfare/conflict through the lens of the ACF, including how US Cybercom and State Department have shifted focus from deterrence to persistent engagement. Action needs to drive policy change in cyber. He also spoke about beliefs over values in coalitions, the legitimacy of Stuxnet and questions of privacy through the Edward Snowden case.

Nicholas Thomas featured as discussant to the second panel, commenting on how technological innovation always is a key driver of human development. States have always felt a need to regulate technologies, regardless of historical period or regime. He identified two emerging trends: 1) pace/rate and scope of technological innovation; and 2) globalization of domestic policies (i.e. domestic policies are connected to or affected by international actors). Challenges with the rate of innovation and policy coalition responses provide the possibility of analyzing the changing response times of policy makers. The longer a policy coalition is in existence, the more effective it is. According to Thomas, the original conception of ACF is national, but these papers confirm that transnational application is possible. Moreover, ACF in its original conception talks about singular coalitions. These papers show that you can have competitive coalitions wrangling over the same pool of policy resources, providing instability.

The second panel received a question on the utility of the ACF for the EU to play a greater role in the military use of AI.

Session 4: The Interconnections between Cybersecurity and Critical Technologies

Moderator: James Shires (European Cyber Conflict Research Initiative)

Speakers: Alžběta Bajerová (NATO), Jakob Bund (European Cyber Conflict Research Initiative), Nikolas Ott (Microsoft), Alexandra Paulus (German Institute for International and Security Affairs)

In Session 4, experts delved into the complex interplay between cybersecurity and critical technologies, particularly focusing on the integration of artificial intelligence (AI) into these domains. The discussion underscored the essential role of trustworthiness in leveraging AI, especially in the context of EU and US technological collaborations. Speakers emphasized that trust and solidarity are fundamental for fostering international partnerships and ensuring responsible behavior in cyberspace. They called for credible commitments to support and capacity building, which are crucial for meaningful protections of critical infrastructure and the effective functioning of incident response teams.

The panel explored the dual aspects of AI's interface with cybersecurity:

AI for Security: AI's potential in enhancing cybersecurity was discussed, highlighting its applications in intrusion detection and incident response assistance. The speakers noted that AI could significantly improve cyber espionage capabilities by automating tasks and lowering entry barriers for new actors.

Security of AI: The importance of frontloading security considerations in AI systems was stressed. Fixing issues post-deployment is not viable, as flawed outputs or vulnerabilities can lead to severe consequences. Establishing a baseline for assessing AI models' trustworthiness is crucial to prevent user manipulation.

The session also covered AI-enabled cyberattacks, such as advanced intrusion techniques and enhanced phishing messages, emphasizing the need for robust defenses. Additionally, the role of AI in influence operations and disinformation was examined. The speed and volume at which AI can generate disinformation pose significant challenges, necessitating scalable solutions. AI's ability to produce content comparable to mainstream media in quality but at a much faster pace could increase exposure to disinformation. The discussion considered whether a self-policing model for social media news content, based on user ratings, is feasible, especially given the challenges of user authentication.

Digital solidarity emerged as a key theme, with positive experiences, like Costa Rica's response to ransomware attacks in 2022, showcasing the benefits of international cooperation. Costa Rica's subsequent involvement in UN processes and its development of a substantial position on international law in cyberspace highlighted the reinforcing effects of solidarity. Commitments to solidarity in managing cyber risks set expectations for support in other technological areas, demonstrating the interconnectedness of international governance and technology language.

The session concluded by addressing the critical issue of **software supply chain security** for armed forces. The far-reaching effects of software supply chain compromises were discussed, emphasizing the strategic vulnerabilities they create. Challenges in military software security persist due to reliance on external components, insufficient security prioritization, and difficulty in security assessment. The potential risks include espionage, data manipulation, and disruption of weapons systems. Speakers suggested that developers could enhance software safety through proofs for every link in the supply chain, though scaling this approach is challenging. The idea of central vetting for open-source software was debated, with comparisons drawn to the AppStore model. GitHub's community review and upload system was proposed as a potential model. Despite high regulatory interest in software liability solutions, practical implementations remain elusive.

Overall, the session highlighted the need for international cooperation, robust cybersecurity measures, and proactive security strategies to navigate the evolving landscape of cybersecurity and critical technologies.

Summary of the keynote presentation by Prof Mariarosaria Taddeo on The Ethics of AI in Defence

Mariarosaria Taddeo, professor at the University of Oxford, Oxford Internet Institute is a philosopher who has researched ethics and information technology. Her keynote, or rather lecture at the REMIT conference focused on ethics of AI in defence. She took us on a systematic journey, that went from defining what AI is, what the usages of AI in defence are with particular attention to AI for adversarial yet non-kinetic (i.e., cyber) uses, that is, digital warfare. This then led into a deep dive in ethical challenges – and these are plentiful. She anchored the journey to familiar territory for scholars of war, namely Just War Theory as well as ethics being about a *conceptual* analysis to identify a strategy for *risks* and *opportunities*.

She turned the question 'why' would AI be used for warfare into 'whether' it would be used, showing that AI-based strategies make it easier to launch non-kinetic attacks which leads into persistence of an offensive environment in cyberspace which in turn enables the weaponization of cyberspace – risking escalation into interstate cyber warfare.

The shape of ethics in this context (i.e. that conceptualisation) is a matter of great attention for military agencies such as UK and US DoD and NATO. Over the past years, a huge amount of work has been done on AI ethical frameworks. The conceptual analysis of ethical risks of AI includes security ethical risks, namely the ethics of the risk of lack of control and ethics of the risk of escalation.

Principles established by various military agencies for AI ethics in defence remarkably do not address AI to deliver coercive behaviour – that is, they do not combine AI and defence, and more specifically they avoid the use of justice, that is, 'just war'. Prof Taddeo argued that ethics of AI in defence must address the consistency with Just War Theory of AI for coercion (i.e. as in defence), both ontologically and for risk assessment.

A second criticism, more general, on AI ethics principles is that these are too high level to be of any real guidance. They 'provide a compass but not a map'. To get to the map, that is, mapping principles to ethics tools, is a process that risks derailing into ethics devolution and lobbying. What is rather needed is to deliver moral impartiality by means of an independent, multistakeholder, expertise-led body, to have reproducibility, transparency, and accountability. This then brings it to the theme of this conference, technology, and multilateralism. With this Prof Taddeo's gave a powerful concluding message: ethics of AI in defence is about designing democratic, pluralistic, and just (post)digital societies. Doesn't the same hold for the REMIT project?

Summary of the Stakeholder Advisory Board (SAB) Roundtable

At the recent Stakeholder Advisory Board (SAB) roundtable, Mariarosario Taddeo from the Oxford Alan Turing Institute shared profound insights into the growing role of AI as an interactive, autonomous, and self-learning agent capable of performing tasks that traditionally require human intelligence. She emphasized the necessity of viewing AI not just as a tool but as an agent capable of interacting with its environment. While much of the debate around AI has been dominated by its use in autonomous weapons, Taddeo argued for a broader perspective, encompassing the diverse applications of AI across defense operations.

AI in Defense Operations

Taddeo highlighted various possible uses of AI in defense:

1. **Sustainment and Support Uses:** AI can optimize back-office operations, logistics, operational planning, and intelligence.
2. **Adversarial and Non-Kinetic Uses:** AI can enhance system responses, offensive cyber operations, and malware design.
3. **Adversarial and Kinetic Uses:** AI can assist in lethal autonomous weapons systems (LAWS), tactical decisions, and combat personnel support.

Blending Physical and Digital Warfare

The traditional separation between physical and cyberspace in warfare is increasingly blurred. Digital warfare now involves both physical and digital agents and targets, employing low to high levels of force. This integration raises numerous ethical challenges, such as trust, accountability, robustness, transparency, and human rights in support operations, risks of escalation and control in non-kinetic uses, and moral responsibility in kinetic uses.

Ethical Considerations and Strategies

The roundtable participants debated the ethical implications of AI in warfare, acknowledging the critical need for ethics to navigate risks and opportunities effectively. Taddeo asserted that ethics should provide a strategic framework rather than merely setting boundaries. This approach is essential for developing strategies to mitigate risks in the evolving landscape of cybersecurity and AI.

The Nature of Cyber Attacks

Cyber attacks redefine traditional concepts of defense and security. In cyberspace, offensive actions often overshadow defensive measures, with technology being vulnerable to data poisoning, backdoors, and prompt injection attacks. The weaponization of cyberspace and interstate cyber warfare pose significant threats, exemplified by the offensive cyber capabilities of the UK, US, and NATO. Taddeo noted that the rapid evolution of this technology has outpaced regulatory frameworks, highlighting missed opportunities for effective regulation.

Ethical Risks of AI

AI introduces several ethical risks, including escalation, lack of control, enabling human wrongdoing, eroding human self-determination, reducing human control, removing human responsibility, and devaluing human skills. Taddeo stressed that general AI principles are insufficient for military applications and called for specific principles that include justice and fairness to maintain an ethical advantage.

AI Ethics in Practice

The roundtable emphasized the need for practical implementation of ethical principles in AI. This requires involving all stakeholders to prevent ethics devolution and lobbying, and developing methodologies that translate high-level principles into actionable guidelines.

Insights from Luca Belli and Nick Thomas

Luca Belli discussed AI governance within BRICS countries, highlighting the trend of emulating developed nations like the US. He noted that while research is crucial for defense, as seen with ARPA and DARPA in the US, the impact of European values is waning in the Global South, which prefers the pragmatic approach of trading with China for cheaper technologies.

Nick Thomas, an Associate Professor at the City University of Hong Kong, focused on the intersection of health and security, particularly in East Asia. His research during the Covid-19 pandemic underscores the strategic importance of biotechnology in addressing global challenges. Thomas advocated for increased transparency and communication from governments to build trust, especially in regions where cultural norms and historical contexts shape perceptions of authority and Western influence.

Future Directions

Looking ahead, Thomas emphasized the need for proactive policies to address emerging health-security challenges. He underscored the importance of collaboration and preparedness in navigating the complexities of biotechnology and global health-security issues, with a particular focus on advancements like CRISPR gene editing.

In conclusion, the SAB roundtable provided a comprehensive exploration of the interconnections between AI, cybersecurity, and critical technologies, emphasizing the need for ethical frameworks, international cooperation, and proactive strategies to address the evolving challenges in these fields.

Summary of Keynote by Bart Preneel on Global supply chain risks in software and hardware

In his keynote address, Bart Preneel highlighted the challenges and complexities of cybersecurity in an era dominated by cloud computing. He began by noting that the major cloud service providers are based outside of the European Union, which raises significant trust and security concerns for EU stakeholders. Preneel emphasized a critical point: "The cloud is someone else's computer," implying inherent risks in relying on external entities for data storage and processing.

Growing Vulnerabilities and Data Breaches

Preneel drew attention to the increasing number of reported critical vulnerabilities in computer systems and the escalating scale of data breaches. He likened the proliferation of Big Data to pollution, suggesting that its unchecked growth could have detrimental effects. He humorously remarked that the only truly secure computer is one kept in a windowless basement, disconnected from any network, and powered off.

Historical Context and Recent Incidents

Referencing historical and recent cybersecurity incidents, Preneel discussed the NSA revelations by Edward Snowden and the SolarWinds attack. These examples underscored the pervasive and persistent nature of cyber threats. Preneel also shared insights from a study he participated in, commissioned by Intel, where he was the only non-US participant. This study examined the axiomatic basis of trust in cybersecurity.

Bases of Trust

Preneel detailed different bases of trust:

1. **Axiomatic Basis of Trust:**
    - **Acceptance Without Evidence:** Trusting the supplier without needing proof.
    - **Accountability:** Holding individuals or companies accountable when necessary.
    - **Supply Chain Source Selection:** Employing secret or random selection methods to ensure trustworthiness.
2. **Analytic Basis of Trust:**
    - **Observation (Inductive):** Continuous testing, acknowledging that proving security is more challenging than identifying weaknesses.
    - **Deductive:** Using verification and model checking to establish trust.
3. **Synthesized Basis of Trust:** Combining trusted components in secure ways, such as:
    - **Smaller Trusted Computing Base:** Utilizing a hypervisor.
    - **Split Device Fabrication:** Manufacturing parts of a chip in different countries.
    - **Replication:** Employing blockchains and Secure Multi-Party Computation (MPC) to enhance security.
    - **Multi-Party Computation (MPC)**

Preneel elaborated on MPC, a method where sensitive data is divided among multiple service providers, with each receiving a meaningless part of the data. This approach enhances security by preventing any single provider from accessing the complete dataset.

Trust Mechanisms and Their Challenges

He discussed various mechanisms to establish analytical trust, such as testing, isolation, attestation, and distribution through blockchains and secure MPC. However, he acknowledged that testing is never exhaustive, and isolation of systems can be challenging.

Corporate and Nation-State Trust

On the axiomatic side, Preneel stressed the importance of corporate governance and adherence to standards like GAAP, ISO 27000, and NIST. Effective trust mechanisms require well-designed operations integrated with business practices, auditable processes, and commitment from senior management.

Preneel also touched on the role of nation-state policies and laws in establishing trust, which require transparency, the right to contest decisions, equal enforcement, and independent decision-makers. He highlighted the delicate balance between informal influence (ranging from coercion to voluntary compliance) and formal laws, particularly in national security contexts.

Key Questions and Open Solutions

Preneel posed several key questions for consideration:

- How can a vendor build a trustworthy artifact?
- How can a consumer assess the trustworthiness of an artifact?
- How should a consumer decide to treat an artifact as trustworthy?

He warned against relying on single points of trust, which can become single points of failure, advocating instead for open-source solutions. These solutions, he argued, offer effective governance and transparency for service providers.

Audience Q&A

In the Q&A session, an audience member asked if a "zero-trust" approach could solve these trust issues. Preneel responded that while zero-trust is a good starting point and currently a popular concept, it alone cannot fully address the complexities of trust in cybersecurity.

Overall, Preneel's keynote underscored the multifaceted nature of trust in the digital age and the need for comprehensive, multi-layered approaches to secure computing and data management.

Session 5: Regulatory Sandboxes with a Focus on AI

Moderator: Triantafyllos Kouloufakos, University of Leuven, Belgium

Speakers: Filippo Bagni, PhD Candidate in Law &Technology, Scuola IMT Alti Studi Lucca, Italy;

Nils Brinker, Senior Cybersecurity Expert at Intcube;

Katerina Yordanova, IMEC KU Leuven, Belgium;

Dr. Taina Junquilho, University of Brasília, Brazil;

Kai Zenner, European Parliament

In Session 5, Filippo Bagni began by explaining the foundational elements of regulatory sandboxes, drawing a parallel to the concept of a sandbox in which children safely play. Similarly, a regulatory sandbox is an artificially created environment where new technologies can be tested in a controlled and safe manner. This concept has been applied in sectors like fintech and privacy, with about 70% of sandboxes being utilized in these areas.

Purpose and Key Elements

The primary purpose of regulatory sandboxes is to foster innovation while ensuring regulatory learning and consumer protection. Constant communication with regulatory authorities, such as the Bank of Italy, is essential. Bagni outlined six key elements that a product must have to be eligible for a sandbox:

4. Innovative nature.
5. Societal value.
6. Advanced development (near market-ready).
7. Immediate experimentation readiness.
8. Economic sustainability.
9. Identification of applicable legislation and regulatory authority.

The Role of AI Act and Cyber Resilience Act

Before the AI Act and the Interoperability Act, there was no clear definition of regulatory sandboxes. Now, the AI Act includes provisions for these sandboxes, marking a significant step in European legislation. Each Member State (MS) is mandated to establish at least one regulatory sandbox within 24 months of the Act's adoption. This initiative aims to provide legal certainty, promote best practices, foster innovation, facilitate regulatory learning, and enhance market access for SMEs.

The Cyber Resilience Act (CRA) aims to create a cyber-safe digital market by addressing low levels of cybersecurity awareness among consumers and implementing specific obligations for economic operators throughout the production chain. Though not originally part of the CRA proposal, regulatory sandboxes have been introduced as an optional tool for Member States to establish.

Interaction Between CRA and AIA

Both the CRA and AIA share the goal of ensuring a safe EU market for new technologies. Regulatory sandboxes in the AI sector help SMEs bring products to market that comply with both the AIA and CRA. This dual compliance ensures a holistic approach to cybersecurity and AI regulation.

Key Points by Kai Zenner

Kai Zenner highlighted the complexities and differing views within the European Parliament regarding regulatory sandboxes. He noted that policymaking in the AIA is principle-based, which requires secondary legislation like templates and guidelines to fill in the details. This is the first-time stakeholders are closely involved in the policymaking process, which has been a long-standing need for industry actors.

Contentious Points and Challenges

Regulatory sandboxes initially faced resistance, particularly from those concerned about creating a "lawless place." However, a balance has been reached, allowing Member States some discretionary power in defining the objectives of these sandboxes. Article 58 of the AIA ensures fair criteria for accepting companies, addressing concerns about national biases, such as France's attempt to restrict its sandbox to French companies.

Zenner also pointed out challenges related to liability, privacy, funding, coordination, and the participation of smaller players like SMEs. He questioned whether SMEs would be able to participate for free, especially compared to larger tech companies.

Insights from Nils Brinker

Nils Brinker discussed the subjectivity in risk management, particularly in the context of the AIA's risk-based approach, which originated from the finance sector. He emphasized that risk management in AI involves more theoretical considerations and less tangible metrics than financial risks. The assignment of risk management obligations significantly influences the types of risks considered and the outcomes of these assessments.

Brinker stressed the importance of including third parties in risk management discussions to ensure a broader perspective and reduce biases. He also highlighted the potential of regulatory toolboxes to better articulate and address concrete risks arising from AI usage.

Conclusion

Overall, Session 5 provided a comprehensive overview of the regulatory sandboxes' role in AI and cybersecurity, underscoring their importance in fostering innovation while ensuring safety and compliance. The speakers emphasized the need for collaboration, detailed guidelines, and the inclusion of diverse perspectives to navigate the complexities of AI regulation effectively.

Session 6 Related initiatives on technology & multilateralism

Moderator: Paul Timmers (University of Leuven; REMIT project)

Speakers: Hylke Dijkstra (Maastricht University; ENSURED Horizon project), Maria Grahn-Farley (University of Gothenburg; HRJust Horizon project), Daniel Mügge (University of Amsterdam; REGULAITE project), Roberta Haar (Maastricht University; REMIT project)

The presentations delivered complementary perspectives on technology and multilateralism: the global challenges and crisis of multilateralism in which Europe tries to find its way, the profoundly different perspectives on law and governance between notably the West and China as barriers to international dialogue on human rights, the framing of regulation of AI in Europe and internationally, and the multiple perspectives emerging from actor engagement in technology and geopolitics.

In the debate, panelists addressed amongst others the state of multilateralism and clearly refuted the 'multilateralism is dead' thesis. However, the way multilateralism is instrumentalized profoundly differs between for instance the EU – also given its mandate - and others in the world.

Finally, the discussion and the audience addressed the question how research projects such as the ones in the session can influence policymakers and politicians who often have little time to engage with research. Experiences were shared, overall concluding that with creativity more interaction between the worlds of research and policy is possible and influence can be increased.

This session illustrated that there is a need to bring together a multitude of perspectives on multilateralism and technology, even if it is a very hard task to contrast, combine, and perhaps reconcile them – this is the challenge to researchers. It also suggested that while doing so, such research can be made relevant to current ongoing policy-making and must be made more relevant by interaction with policy-makers.

Young Research Session 1: Quantum and Multilateralism

Moderator: Aysajan Abidin (University of Leuven)

Speakers: Kristiaan De Greve (University of Leuven), Wouter Castryck (University of Leuven), Raluca Csernatoni (Carnegie Europe), Andrea Rodriguez Garcia (ImpaQT)

Andrea Garcia presented a snapshot of the current context of global quantum investments from a European perspective and outlined the role envisioned for her non-profit ImpaQT in this context. The EU and its member states are fragmented in what they want to achieve, even if there are also some points of connection. Competition is significant and contributes to secrecy around the development of quantum technology. There is talk about following the EU, which is hardly implemented at the industry level. Therefore, something like ImpaQT is needed. ImpaQT seeks to create a new way of competing called 'smart competition.' ImpaQT functions as a system integrator that creates standardized interfaces. To join ImpaQT, companies have to be interoperable by design. The competitive advantage of European firms will be created through a puzzle that pieces them together with the rest of the puzzle, thereby making them more competitive abroad.

Kristiaan De Greve provided an update on the current state of quantum computing and quantum systems. He used the analogy of a moonshot operation to show that the state of development is currently in the geometric mean between nothing and working quantum systems – like Tintin's moonship ready for launch but not quite sure if launch or what comes after will be successful. Professor De Greve highlights that the current state of building quantum computers is scientifically at a toy problem juncture, where the system is visibly complex but not yet sufficiently scaled to be realistic. And the number of qubits (and thus the speed of calculations) is still limited. A quantum computer that can pose a real threat to current digital security requires several millions of physical qubits. How can this gap to more qubits be bridged? This is not clear. Quantum error correction and the very high level of overhead during calculation means it is difficult to get into the millions when it comes to qubits. Silicon scaling took 50+ years to get to where we are now; this illustrates the complexity. Considering recent developments, there is an increasing realization that the laboratories where quantum computers are being made right now are not exactly what is needed. But it is not clear what the next steps are. We are in pre-competitive research, and depending on how much the research efforts can be pulled in the right direction, there can be acceleration or deceleration. Getting from a geometric mean to a realistic working system still requires a lot of resources as well as intelligence and cooperation.

Raluca Csernatoni brought an international relations and governance studies perspective on the digital security threat posed by quantum technologies. She shared the key questions related to quantum tech in international relations that she and her students came up with. The first question is, what exactly are the risks, challenges, and opportunities coming from quantum technologies when it comes to national security? Current and recent developments regarding AI policy can be telling here. Secondly, how should expectations of quantum technologies be managed? Maybe quantum advantage is a better term than quantum supremacy, which fits in better with digital sovereignty and technological sovereignty discourses. Thirdly, which actors in the quantum tech sector can be trusted? Are state-driven investments more ethical and, therefore, trustworthy than corporate-driven initiatives? Fourthly, there is the question of where we are geopolitically when it comes to quantum technologies. There is the perception of an arms race. Finally, which global governance initiatives are there and should be promoted? There seems to be room for initiative and opportunity because we are at an early stage in developing these technologies. Overarching these questions is the issue of who gets to lead and set the agenda regarding all of these actions. The students thought the EU was well-positioned because of its normative regulatory empire. For Dr. Csernatoni, this question is not technological but political. Politics draws the red lines for technologies, such as whether they can be weaponized, used for offensive purposes, etc. Who gets to shape the socio-technical imaginary surrounding such technologies? The World Economic Forum Quantum Computing Network has been asking questions like these.

Wouter Castryck talked about Post-Quantum Cryptography (PQC), in particular, the quantum threats to digital security and the current efforts to transition to PQC, as well as the open nature of the

standardization process for (post-quantum) cryptographic algorithms. The ongoing transition to PQC concerns public-key cryptography, used to authenticate and set up secure connections. It is a lifeline of today's society that these technologies work. The issue that quantum computing poses is that it can solve the hard-computational mathematical problems that underly a lot of public key cryptography. For cryptographers, Shor's algorithm is a big elephant in the room because it shows that a quantum computer can crack RSA encryption (which is used to secure website traffic, among other things). Therefore, action and research are being undertaken to develop cryptographic methods that can secure digital data against quantum algorithms. Two concrete motivators underpin this research. Firstly, there is the threat of 'harvest now, decrypt later', which entails that the encrypted data that contains secrets that are useful for, e.g. 30 years can be harvested now to decrypt in 20 years. Secondly, moving from an academic proposal to worldwide deployment of standards usually takes decades. Due to these motivators, even if there is not a realistic quantum computer, PQC will happen. The main driving force for this right now is the NIST competition. NIST is a US organization that has already announced four PQC standards. They are relatively trusted despite being in the US because they are open. However, vigilance is warranted because of alleged NSA interference in the past. For these kinds of efforts, worldwide cooperation is important. There must be an open research culture because small-scale, isolated efforts are a recipe for disaster. People working by themselves run into trouble. But accessibility is an issue – for example, conference costs. In principle, NIST competitions are open to everyone but can be pricey in practice. Moreover, the security of mathematical algorithms depends on continual trusted efforts to try to crack them.

Afterwards, the panelists engaged in discussions centered around curated questions by the moderator about the playing field regarding quantum technologies and whether multilateralism is achievable. Ms. Rodriguez Garcia argued that competition is important and that ImpaQT seeks to be compatible with it by allowing for more scaling. Moreover, in terms of standardizing technologies, it was highlighted that the approach should be multistakeholder if it is not multilateral, that is always better than unilateral approaches. Finally, the point was made that in military competition, military organizations are both actors and audiences of discussions surrounding quantum technologies. They often signal when they participate. The inter-panel discussion also considered other PQC standardization initiatives than NIST and their scope. However, NIST has the upper hand compared to them because the EU endorses it.

Finally, following two questions from the audience, the panel ended with insightful closing remarks by the panelists.

Young Research Session 2: AI and Multilateralism

Moderator: Daniel Mügge (University of Amsterdam)

Speakers: Mahmoud Javadi (Erasmus University Rotterdam), Maya Müller-Perron (Maastricht University), Hengyi Yang (Maastricht University), Siyuan Qiao (Maastricht University), Zhanwei Wang (Maastricht University)

Mahmoud Javadi employed the ACF to analyze Council of Europe's Framework Convention on AI. There are two coalitions: United States-led coalition and EU-led coalition. Regulation of AI life cycle applicable to both public and private sectors is the deep core belief. Despite the dominant position held by the EU-led coalition, the substantial US technological power compelled the European Commission to act as a policy broker between the two coalitions.

This presentation reveals that the significance of AI governance lies in regulating the private sector, but the Council of Europe's convention has shown weak outcomes, indicating that future multilateral efforts may face similar challenges.

Maya Müller-Perron focused on the US AI governance under the Biden administration. Ethical Regulationists hold the belief that AI is discriminatory and biased, and the US government should regulate tech companies. In contrast, Innovation Regulationists are rather skeptical of government regulations. They aim to maintain the US's status as the global tech leader and fear China's growing influence, advocating for less AI regulation and greater innovation.

In summary, AI policies is heavily shaped by tech industry leaders which reflected in "cyber libertarian" approach of US AI governance. In addition, "Innovation Regulationists" are better at utilizing their resources to shape policies.

Hengyi Yang utilized Policy Network Analysis (PNA) and Qualitative Content Analysis (QCA) to identify how China perceives AI as a strategic technology. 15 national policy papers are selected to conduct the network analysis. In 2016, China launched the "Internet Plus" Three-Year AI Action Plan, and only one year later, in 2017, introduced the Development Plan for New-Generation AI (AI 2). This initiative highlights the central role AI 2 occupies within China's key policy frameworks. The Ministry of Science and Technology emerges as the most influential institute in this field, underscored by significant contributions from the Ministry of Industry and Information Technology, the Ministry of Education, the National Development and Reform Commission, and the Cyberspace Administration of China, all important in governing AI in China. Moreover, the governance structure is analyzed through three dimensions: perceptions, goals, and the MoFA, which show the advocate and oppose coalitions.

In the field of AI governance, the involvement of multiple stakeholders extends beyond the state-driven approach. Before the national AI governance plan, major technology companies played vital roles. After 2019, local governments also began to participate actively in AI governance, marking a shift towards more diversified involvement.

Siyuan Qiao concluded and explained the state pattern of AI governance: EU explifies right-driven pattern, US adopts market-driven pattern and China is dominated by the state-driven pattern. Russian and Saudi Arabia tends to adopt a state-led model; Japan and South Korea resembles the market driven model; A hybrid model combining market-driven and government regulation is exhibited in South Africa and India; Singapore and Brazil combines a state and right driven governance pattern; Canada, UK and Australia emphasize ethical principles and privacy protection, but also incorporate the market-driven methods.

There are two potential paths regarding the development of AI governance in multilateral international organizations. One is to strengthen coordination and capabilities among existing institutions, the other is establishing new institutions.

Zhanwei Wang emphasized the role of international organizations (IOs) in the global AI governance. The United Nations published the White Paper on AI Governance on October 2023 and explained models, functions, and existing international normative frameworks applicable to global AI governance. In addition, a Global Digital Compact that 'outline shared principles for an open, free and secure digital future for all' is expected to launch on September 2024. There are five principles of the OECD advocated in 2019: inclusive growth, human right, and democratic values, transparency, robustness and accountability.

To sum up, global AI governance necessitates collaboration among a vast array of stakeholders, such as academia, civil society, citizens, and the private sector. However, the Global South have been largely absent from these discussions and risk being marginalized.

Daniel Mügge gave some comments on the presentation and delved into the future imaginaries surrounding AI governance. He suggested that political institutions may systematically advantage certain actors while disadvantaging others, shaping the outcome of governance coalitions. Socioeconomic structures, like contemporary digital capitalism, can also advantage specific actors, influencing policy decisions. Additionally, divergent views on existential risks associated with AI shape discussions on global governance, with differing opinions on the role and scope of international organizations. What's more, a nuanced approach to AI governance is needed, focusing on specific subsets of issues rather than a singular, overarching framework. This includes considerations for technology diffusion, trade standards, and safety regulations.

Summary of the Closing session

Keynote Prof Peggy Valcke, University of Leuven: The First-ever AI Treaty

Prof Peggy Valcke is both a renowned scholar in AI and law as well as a key contributor to the work of the Council of Europe on AI. In particular, she has been instrumental to develop and negotiate the AI Convention of the Council of Europe. Coincidentally the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law was adopted on 17 May 2024, the same day of Prof Valcke's keynote at the REMIT Conference. It will be opened for signature on the occasion of the Conference of Ministers of Justice in Vilnius (Lithuania) on 5 September 2024.

Prof Valcke gave her keynote as a great example of a policy narrative, perfectly fitting in the narrative policy framework approach, well-known in political sciences. In particular she highlighted the struggles to keep all parties on-board in this multi-country (46!) exercise with serious differences of opinion, holdouts and holdups, even drama yet ultimately, reconciliation and successful delivery of the Convention, a landmark document in global governance of AI.

The path towards the AI Convention gave us most illustrative and personable insights into technology and multilateralism in action!

Keynote David Ringrose, European External Action Service EEAS: EU Digital Diplomacy

David Ringrose heads the unit for Digital Transition & Global Gateway. He gave an enlightening overview of the many ways EEAS and the European Commission now connect what are called internal policies in the digital domain (such as for cyber-resilience) with the external policies on digital affairs (such as digital diplomacy, or international cooperation on digital development). A wide set of actions is being undertaken, from dialogues to investment. In parallel, digital and cyber capacity is being built in the foreign affairs ministries of the EU Member States and in the EU institutions. The opportunities and interest are with considerable to connect to the research of REMIT and related projects.

The two days were wrapped up by closing words by Profs Haar, Timmers and Crompvoets, who addressed the inspiration, insights and teambuilding to which this conference has contributed, which has all been highly satisfactory. Much effort has gone into organizing this first REMIT conference. Gratitude was expressed to all organizers, speakers, public communications and supporting staff and the host, KU Leuven.

The background of REMIT project

The REMIT project aims to Reignite Multilateralism via Technology. A reigniting that not only reacts to China's rise as a systemic technology rival or Russia's resurgence as a technology abuser or the dominance of large U.S.-based digital platforms, but that sets a clear vision for the future — one in which Europe plays a leading role.

Coordinated by Maastricht University, the REMIT project brings together leading European researchers from nine partners from Belgium, Estonia, Finland, Germany, Italy, the Netherlands, Romania and the United Kingdom. The goal is to develop recommendations, clear understanding of the status quo and innovative methodologies that support effective policies to revitalize global democratic structures.

REMIT aims to re-mobilize a transnational collective spirit that addresses global problems through technology, because

1. Technology has strong effect on economic competitiveness
2. Technology is important to national security including threats to democratic principles
3. Technology is crucial to the solutions for global challenges

By focusing on technology and the policy areas that emerge from the REMIT researchers' expertise, the project provides the needed analysis and the theory building to support the EU. The four technology areas are also instrumental in finding solutions to all important challenges, including climate, digital transitions, the rise of inequalities, ageing and disabilities, migrations, health pandemics, and information disorder. Ultimately, REMIT intends to design policy recommendations that will give a remit to reignite multilateralism via technology.

The detailed objectives of the REMIT project are:

» Objective 1: To define the EU's role in leading the renewal and defence of multilateralism starting with the global governance of technologies in four crucial policy areas (digital, health bio, security and defence, and financial technologies). The lack of comprehensive, multilateral tech regulations represents material national security threats to the EU and its allies by allowing others (especially China) to set the rules for the digital future.

» Objective 2: To provide evidence-based advice to reinforce European institutions in the field of technology that work and propose innovative, multilateral-governance constructs for those that do not.

» Objective 3: To develop policy recommendations and scenario testing workshops offered to relevant EU administrators, important regional groups, and national officials.

» Objective 4: To share knowledge among stakeholders and to communicate policy recommendations. REMIT will recommend policy action for the European Union that further re-conceptualizes multilateralism in the four technology areas.

The REMIT project is carried out from March 2023 till February 2027 and has a total budget of almost €3 million, of which €2.6 million is funded by the EU's Horizon Europe research and innovation program and €370k is provided by the UK government through the UK Research and Innovation fund (UKRI). The project is being carried out by internationally recognized researchers from University of Maastricht, Universitatea Babes Bolyai, Universitaet Bremen, Katholieke Universiteit Leuven, Luiss Libera Universita Internazionale Degli Studi Sociali Guido Carli, Erasmus University Rotterdam, the Finnish Institute for International Affairs and the University of Tartu. In addition, the European Cyber Conflict Research Initiative (ECCRI) joins the consortium as an associate partner, receiving funding from UKRI.