Global Digital Foundation
The Digital Policy Network

Digital Trust – Strategies for Europe

Outcome Report of the Digital Trust Workshop, Brussels, 11th December 2023

Produced by

Rob Wortham, Global Digital Foundation

Contents

Introduction

This short report follows from a half-day digital trust workshop held in Brussels on 11th December 2023. Firstly the report seeks to define digital trust and explore the meaning of trust in an increasingly polarised and distrusting world. The report goes on to explore digital trust specifically in the EU, and then offers a more global perspective, specifically concentrating on EU-China digital trust relations. The workshop included opportunities for round table discussion, and these are summarised in the final two sections, covering practical suggestions and next steps.

Digital Trust Defined

In an era dominated by unprecedented technological advancements, the concept of digital trust has emerged as a critical determinant of success and security in the online realm. As individuals, organisations, and societies increasingly rely on digital platforms for communication, commerce, and collaboration, the importance of fostering trust in these digital interactions cannot be overstated.

Digital trust, at its core, refers to the confidence and assurance that users place in the reliability, security, and integrity of digital systems, services, and transactions. It encompasses the belief that the digital entities involved will perform as expected, without compromising privacy, confidentiality, or data integrity. Various definitions exist, reflecting the multidimensional nature of digital trust. One commonly accepted definition is the reliance on information systems and technologies that consistently operate as intended, securely handling sensitive data and maintaining user privacy.

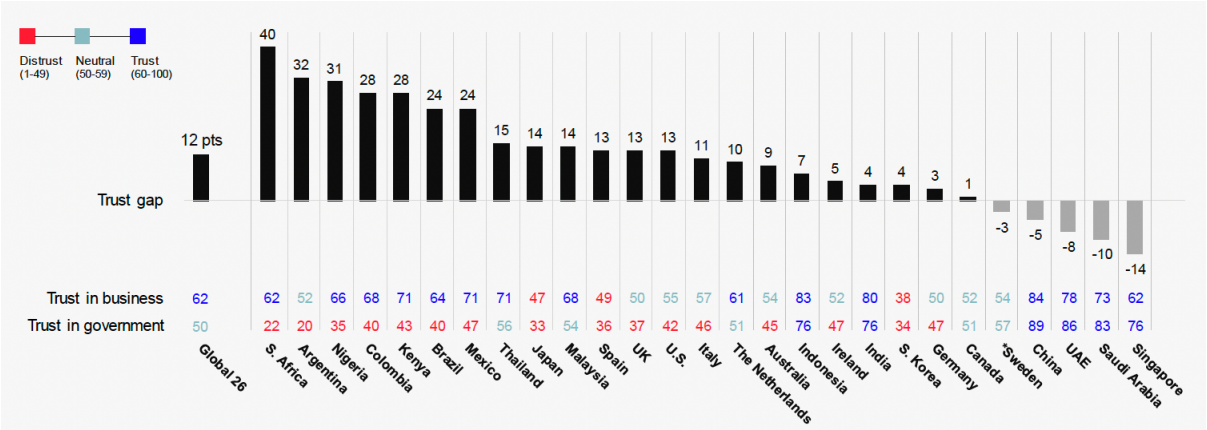
Trust, in a broader context, is a fundamental element of human interaction, influencing relationships, decision-making, and societal structures. While digital trust focuses on the online dimension, the foundations of trust are deeply rooted in human psychology and social dynamics. Trust involves the willingness to be vulnerable based on the expectation that others will act in a reliable and responsible manner.

In the global landscape, the significance of trust has been acknowledged in international standards, where trust is often defined as a verifiable expectation. This emphasises the importance of establishing not only subjective confidence but also the capability to verify and validate the factors contributing to that confidence. In the digital domain, this translates to the ability to assess the reliability and security of systems through tangible evidence and transparent practices.

As we explore digital trust, examining the factors influencing trust in the digital realm, we must recognise the geopolitical realities of establishing trust in an increasingly polarised world.

Trust in a Polarised World

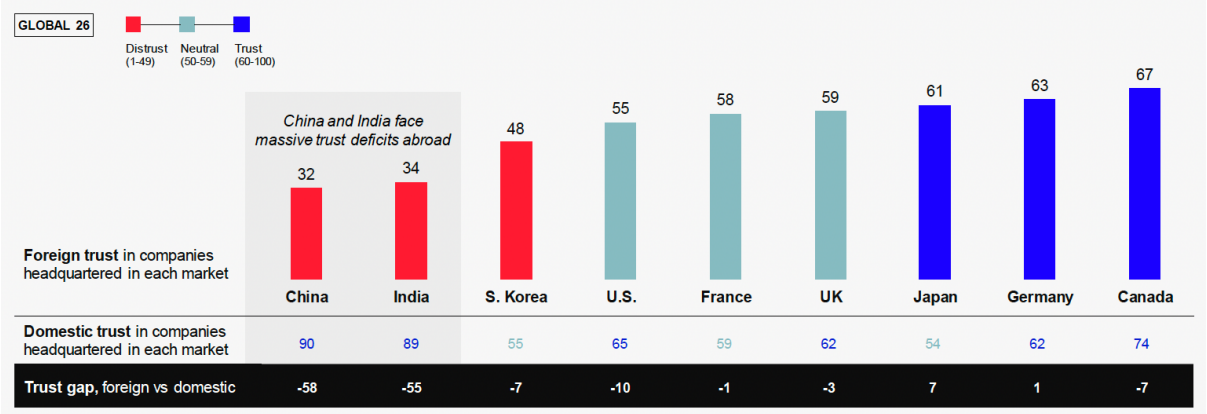
In the ever-evolving landscape of digital trust, geopolitical factors play a pivotal role in shaping perceptions and influencing global interactions. For more than 20 years, Edelman have studied the influence of trust across society — government, media, business, and NGOs. They produce an annual 'trust barometer'[1] that attempts to assess global trust across its many facets. The 2023 report notes the effect of increasing polarisation and offers some notable insights in graphic form as below.



Government Less Trusted than Business - Percent trust, and the percentage-point difference between trust in business vs government. Reproduced from Edelman Trust Barometer Report, 2023

Interestingly, while Business is almost universally more trusted than Government in democratic states, the trend is reversed in those with alternative political systems, notably China.

[1] https://www.edelman.com/trust/trust-barometer



Trust at Home Does Not Guarantee Trust Abroad - Percent trust in companies headquartered in each country. Reproduced from Edelman Trust Barometer Report, 2023

China and India have a wide disparity between the high domestic trust in their businesses and the much lower international trust. Writing in the FT in December 2023, Robin Harding[2] explores the increasingly difficult plight of Huawei as an international employee owned engineering and technology company selling its products and services in the West. His analysis casts Huawei as victim rather than villain, however he notes that from a western perspective: *"Just as a bank cannot have a credit rating higher than the sovereign that implicitly stands behind it in a crisis, a company cannot be more trustworthy than the government it must answer to."* It is therefore imperative to acknowledge the specific challenges associated with trust in digital systems originating from China and companies under Chinese control.

One focal point of concern revolves around the deployment of 5G technology, especially in regions like Europe and the United States. The involvement of Chinese companies in providing 5G infrastructure has raised questions about the security and integrity of these systems. While technological advancements promise unprecedented connectivity and efficiency, the geopolitical implications surrounding the adoption of Chinese-developed 5G equipment have led to heightened scrutiny and cautious evaluations.

Another dimension of the digital trust landscape involves export restrictions on critical technologies. Several countries, particularly the United States, have imposed limitations on exporting certain technologies, including microprocessors and GPUs, to China. This has contributed to a complex environment, fostering discussions about technology flow, security implications, and the broader implications of such measures on international collaboration.

[2] https://www.ft.com/content/3d40fa50-ca60-43b3-89cd-1587a184981f

Digital Trust in Europe

From a European perspective, we can consider digital trust within four relevant cornerstones of the EU: The Precautionary Principle, the Internal Market, the Resilience and Recovery Fund, and finally the principle of National Autonomy and Sovereignty.

Precautionary Principle

The precautionary principle is a fundamental concept in European governance, guiding decision-making in the face of uncertainty and potential risks. In the context of digital trust, this principle emphasises the need to anticipate and address potential harms to individuals, society, and the environment associated with the adoption of new technologies. European regulators employ a cautious approach, ensuring that measures are in place to mitigate risks before widespread implementation. This principle underscores the importance of comprehensive risk assessments and proactive measures to safeguard digital ecosystems.

Internal Market

The European Union's commitment to the internal market promotes the free movement of goods, services, capital, and people across its member states. In the realm of digital trust, the internal market facilitates the harmonisation of regulations and standards. A unified approach ensures a level playing field for businesses and fosters interoperability, enabling the seamless functioning of digital services across borders. This cornerstone supports the creation of a cohesive and collaborative digital environment, where trust is nurtured through consistent standards and practices.

Resilience and Recovery Fund

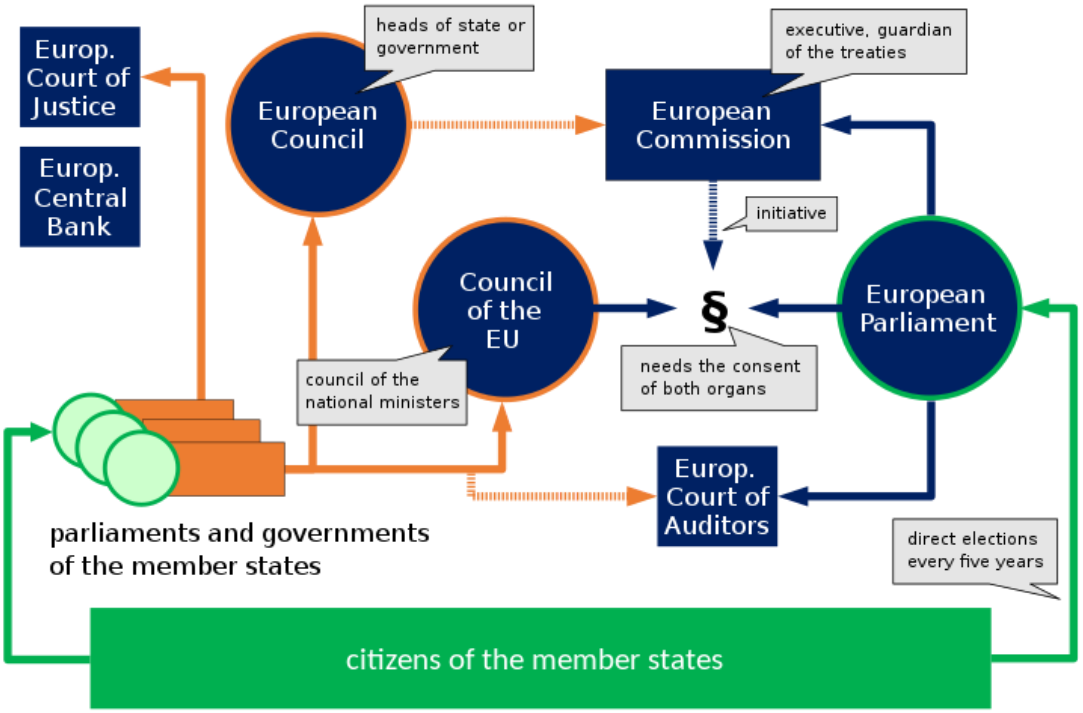
The Resilience and Recovery Fund (RRF) is a financial instrument designed to address the economic and social impacts of crises, such as the COVID-19 pandemic. In the context of digital trust, the RRF serves as a mechanism to invest in the resilience and recovery of digital infrastructures. Funding initiatives focused on cybersecurity, digital innovation, and the development of secure technologies contribute to building a robust digital foundation. This cornerstone reflects the EU's commitment to ensuring the resilience of digital systems in the face of evolving challenges.

Autonomy and Sovereignty

Autonomy and sovereignty are key principles guiding the EU's approach to digital trust. European countries emphasise the importance of maintaining control over their digital destinies, avoiding dependence on external entities that may pose risks to security and privacy. This principle is particularly relevant in the context of critical digital infrastructure, where European nations strive to achieve technological autonomy. Sovereignty in digital matters supports the development and implementation of policies that align with European values and priorities.

Integration and Synergy

These four cornerstones are interlinked and work together within the European governance model. The precautionary principle guides the crafting of regulations that align with the internal market, fostering trust and collaboration. The Internal Market facilitates the free flow of digital services while ensuring compliance with precautionary measures. The RRF provides financial support to initiatives that reinforce the precautionary principle and contribute to the overall autonomy and sovereignty of the EU in the digital realm.



The EU Governance Model

The European approach to digital trust creates a comprehensive framework that not only addresses current challenges but also lays the foundation for a resilient, secure, and sovereign digital future for the European Union and its member states.

Advancing Global Digital Trust

This section focuses on digital trust from a China-EU perspective.

A Historical Perspective

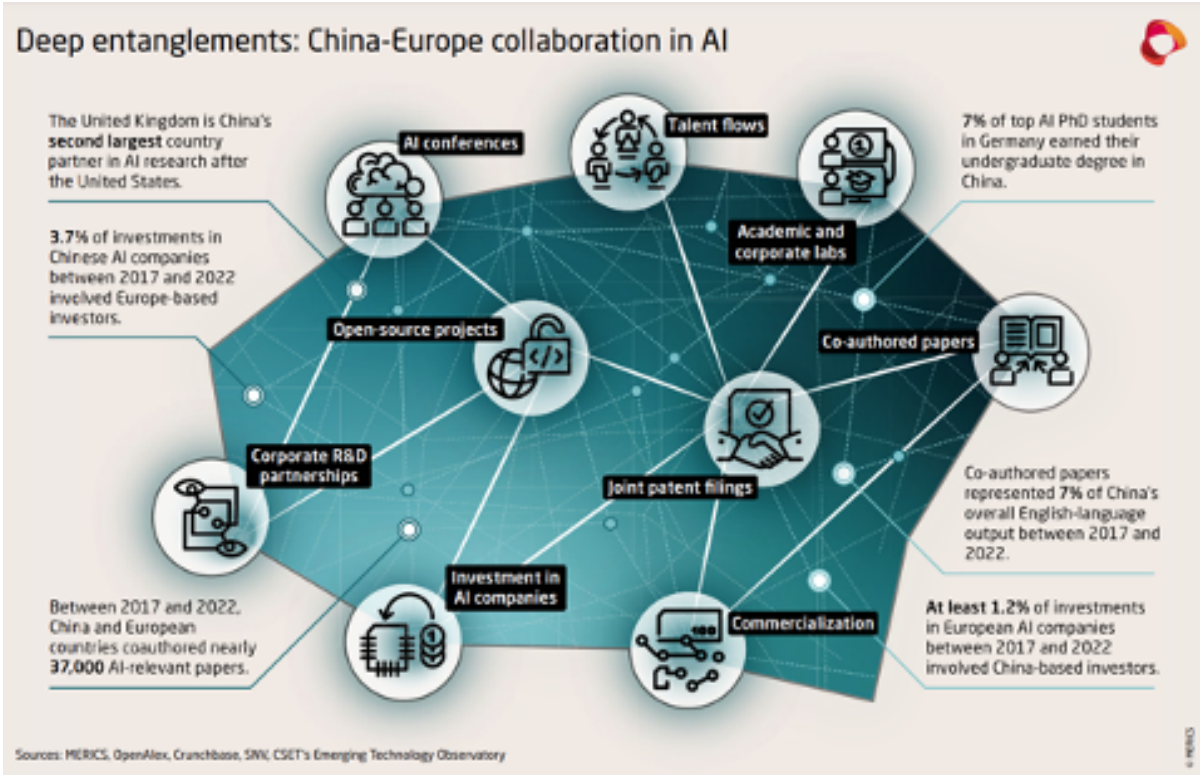
The historical collaboration between China and the European Union (EU) in technological domains such as 5G standards, cybersecurity, and the Internet of Things (IoT) has laid the groundwork for a multifaceted partnership. These collaborative efforts, marked by joint initiatives and shared standards, underscore the potential for mutual benefit in the evolving digital landscape.

The China-EU Green and Digital Dialogue agreements of September 2020 served as a pivotal platform for reinforcing bilateral cooperation, recognizing the need for a more cooperative approach to environmental sustainability and digital security. This demonstrates the potential for synergies in areas of shared interest.

Trust and Engagement: A Clear Correlation

A recent survey investigating China-EU cooperation unveiled insights into the technical, economic, and political factors influencing collaboration. European respondents highlighted concerns, particularly in foreign policy. The survey showed a significant correlation between their views on trust, human rights and Chinese foreign policy with their willingness to engage with Chinese companies in the 5G field, emphasising the intertwined nature of geopolitics and technological collaboration.

In the realm of artificial intelligence (AI), academic research cooperation between China and the EU exhibits resilience and growth opportunities.



While Europe has expressed some support for international cooperation in quantum technology, caution arises due to its dual-use nature. Concerns, particularly regarding post-facto decryption of sensitive data, underscore the need for careful consideration. From a Chinese perspective there are several reasons for EU hesitation in cooperation. Economic concerns about competitiveness, political fears of technology dependence, security apprehensions related to espionage, and philosophical uncertainties about values and privacy protection represent significant barriers.

In-group/Out-group theory predicts that once we define the out-group we strongly stereotype their intentions and behaviours. This thinking can result in strong misconceptions regarding intention. In addition, digital technology security is ubiquitous and virtual, giving rise to "security anxiety" that complicates rational decision-making. Bridging this gap in understanding requires effective communication channels. The three-year disruption caused by COVID-19 underscores the urgency of designing an efficient dialogue framework to foster better understanding and collaboration.

Promoting Rational Decision-Making through Intellectual Support

Leveraging "intellectual support" from think tanks and research institutions becomes crucial in navigating the complexities of China-EU cooperation. Their insights can assist decision-makers in approaching challenges with rationality, informed by a deep understanding of technical, economic, and political dimensions.

Enhancing Information Communication and Sharing

Establishing more channels for information communication is vital for eliminating misperceptions. While summit forums and round tables have been traditional models, the complexity of new technologies necessitates additional avenues. A recommended cooperation catalogue guiding working-level exchanges and an effective information exchange system can contribute to a deeper understanding of emerging technologies.

In the face of cybersecurity challenges, instant investigation and information sharing are imperative. The establishment of a China-EU information sharing mechanism in cybersecurity, involving public security and cyber information departments from China and police and data protection authorities from the EU, could foster a collaborative approach to address cyber threats.

China-EU Summary

Advancing digital trust between China and the EU demands a strategic and comprehensive approach. By understanding historical cooperation, addressing hesitations, promoting rational decision-making, and enhancing information communication and sharing, both entities can pave the way for a resilient and mutually beneficial technological partnership. This requires overcoming geopolitical challenges, fostering open dialogue, and embracing the transformative potential of digital collaboration in the years to come.

Some Practical Steps to Increase Digital Trust

Firstly, we must not fail to acknowledge the global realities of geopolitics covered in this report and their significant influence on trust. We must also assume that we cannot effectively change minds solely through rational argument and information sharing. The trust positions that are held by individuals, civil society groups and governments have much to do with group alliances and alignment ('us versus them'). However as a first step towards increasing digital trust, we can help people reduce perceived risks. We can do this by working with trusted third parties – especially scientists, academics and think tanks. Indeed, though trust may be about choice and allegiance, ***trustworthiness*** (verifiable expectation) is verifiable at three levels: Policy, Conformity to regulations, and Standards Compliance. It is worth noting that the processes of standards authentication require a lot of interactions that can build reputation.

Partnership, particularly with mutually trusted third parties such as standards bodies, university institutes and think tanks can, over time, change the public narrative about who can be trusted.

It is important to recognise that consumer uptake is important, even for unrelated business to business commercial transactions. The perception that the 'layman' trusts a technology supplier is important. After all, we are all consumers. Public opinion is also influenced by the alignment or disagreement between businesses and governments on specific issues. Trust tends to decline when conflicts arise, but it increases significantly when the two entities share the same perspective. It is therefore worthwhile to seek to build consensus with government around the appropriate extent and application of trustworthy digital technologies.

Finally, rather than attempting to alter perceptions of the Chinese state, we can help European organisations and individuals more clearly recognise that all business interactions involve some element of risk. The benefits of any digital technology deployment must always be weighed against the potential risks. In many cases solid commercial benefits outweigh risks and engagement with Chinese or other international suppliers brings solid business benefits and may be readily justified.

Conclusions and Next Steps

A strategic and comprehensive approach is required to advance digital trust between China and the EU. Broad objectives include improving understanding of historical cooperation, addressing hesitations through frank dialog to promote rational decision-making, and enhancing information communication and sharing to improve trust through increased transparency.

Resilient and mutually beneficial technological partnerships can be actively fostered through open dialogue, engagement through trusted third parties and frameworks that assess true business and commercial value, taking risks into account in a realistic manner.

Alignment between business and government in terms of international technology policy will dramatically reduce perceived risk. Continued engagement with target market policy, regulation and standards is therefore critically important.