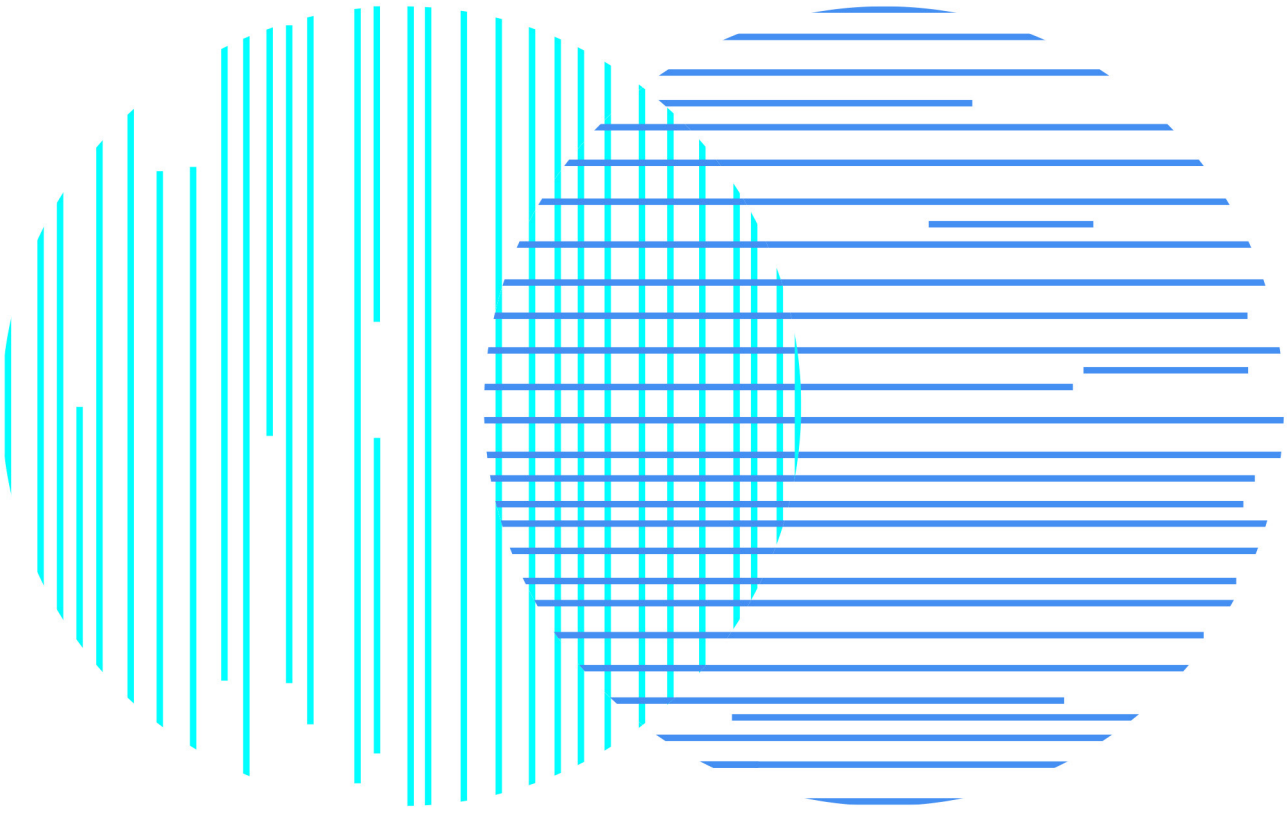
IIEA Europe's Digital Future

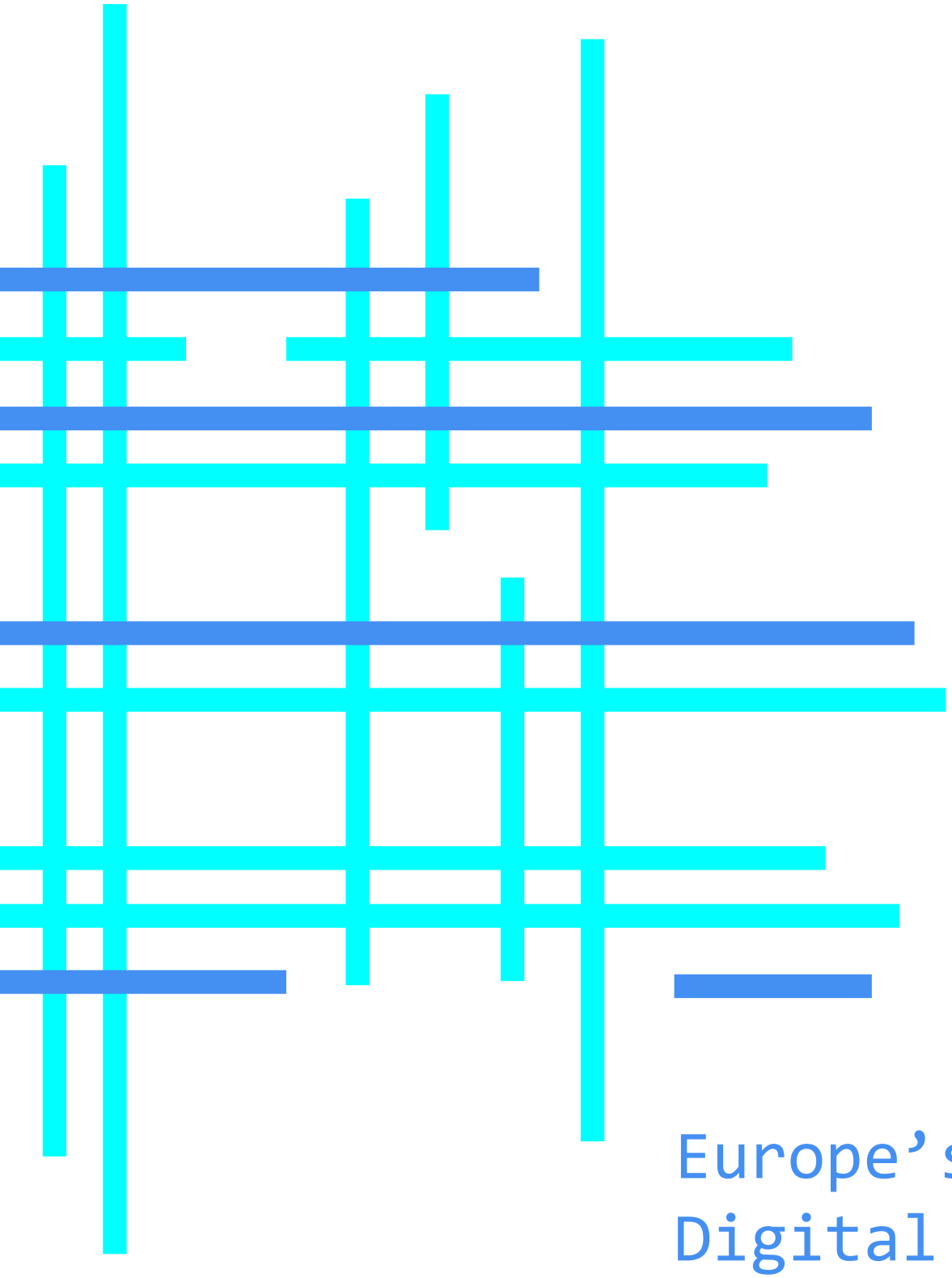
CYBER SECURITY AND EUROPEAN STRATEGIC AUTONOMY:

COHERENCE AND CAPABILITY CHALLENGES



Professor Ciaran Martin

May 2022



Europe's Digital Future

An IIEA project supported by Google

About the author

Ciaran Martin is a Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government. Prior to joining the School, Ciaran was the founding Chief Executive of the UK's National Cyber Security Centre, part of GCHQ. Prof. Martin led a fundamental shift in the UK's approach to cyber security. He successfully advocated for a wholesale change of approach towards a more interventionist posture and this was adopted by the Government in the 2015 National Security Strategy, leading to the creation of the NCSC in 2016 under his leadership. In his 23-year career in the UK civil service, Prof. Martin held senior roles within the Cabinet Office, including Constitution Director (2011-2014), which included negotiating the basis of the Scottish Referendum with the Scottish Government; and director of Security and Intelligence at the Cabinet Office (2008-2011). Between 2002 and 2008 he was Principal Private Secretary to the Cabinet Secretary and Head of the Civil Service and Private Secretary to the Permanent Secretary to HM Treasury.

Introduction

In the autumn of 2017, Estonia, Europe's digital star performer, used its extended presidency of the EU (taking an extra slot from the departing British) to showcase the nation's technological prowess. A two day 'Digital Summit' was tacked on to a routine Council of Ministers meeting, and several weeks later, technocrats flocked back to Tallinn, this time without their heads of government, to a follow up conference on cyber security. Here, the European Commission planned to promote its latest cyber security strategy under the now ubiquitous umbrella narrative of European "strategic digital autonomy".

Arne Schönbohm, the ebullient and impressively no-nonsense President of the Bundesamt für Sicherheit in der Informationstechnik, or German Federal Office for Information Security (BSI), plainly did not get the memo. On stage with his French opposite number, Guillaume Poupard, Germany's cyber security chief launched into a devastating public critique of EU posture on cyber security. First, he said, the Commission was interfering in matters that were properly the function of Member States, and the cyber security organisations wtihin them, such as his own. Second, he said, whilst that was bad enough, it wouldn't matter so much if the Commission and EU institutions more generally understood cyber security properly and had the right capabilties themselves, strongly implying that they did not. Schönbohm doubled down on both these points in a TV interview in April 2018, saying that EU institutions needed to "walk the walk" in terms of their own cyber security, likening the EU Commission's proposals for EU wide certification to "thunder coming out of the sky" and warning the Commission that it was not "a spaceship that can come down and do what it likes".

This was a rare show of public dissent about how Europe responds to the challenges of cyber security. But it illustrates one of the two serious challenges to the European Union and its Member States about strategic autonomy in cyber security - an essential part of any meaningful attempt to forge digital strategic autonomy more widely. No European country can, in practice, be strategically autonomous alone in cyber security; European strategic autonomy can only be achieved at an EU wide level. But, to a significant extent, national governments remain operationally autonomous in cyber security, and guard that autonomy jealously as essential to national security. The EU has yet to find the right balance between a collective and individual nation-state (and multilateral voluntary cooperation) approach for addressing cyber threats.

Cyber security: A fragmented division of responsibilities

This matters, acutely. That's because the nature of the cyber threats faced by the EU and its Member States (which are broadly the same as those faced by other parts of the Western alliance) straddle both national security areas which are typically Member State competencies, and common areas of European economic regulation. Malign cyber activity threatens these societies at two levels. First, hackers pose a threat to the national security of the state. Concerns about such attacks have, understandably, gained a higher profile in the context of Russia's invasion of Ukraine. Such activity is mainly carried out by other nation states for geopolitical and strategic reasons and (sometimes) exhibits a high degree of technical sophistication. Second, more mundane cyber threats threaten economic and social disruption on a daily basis. These are usually the work of transnational cyber criminals, many of whom, though not all, are based outside the west's network of friendly, cooperative legal jurisdictions. Tackling the first problem engages the national security equities of the nation state. Tackling the second is primarily about economic policy, business and trade regulation. So, the former will be jealously guarded by national capitals; the latter will be determined to no small degree at EU level, particularly in single market regulations as well as EU wide cyber strategies.

So, for example, the ever-present threat of espionage against the elected legislatures or diplomatic missions of European countries from the likes of Russia, Iran and China is something that few if any Member States will see as something requiring a common approach at an EU wide level, imposed by the EU's institutions. More serious attacks on infrastructure, such as the apparent Russian state disruption of broadcasts of France's TV5 Monde in 2015 – one of the most sophisticated cyber attacks ever carried out – was a matter for Paris. Even when criminal activity spills over into national level harm – such as the ransomware attack on Ireland's healthcare system in 2021 – the response is one for the national government.

However, hacking does not exist in a vacuum: the digital environment is one driven primarily by economics and commerce, which will fall within the purview of the European Single Market. So, for example, the prevalence of Internet of Things devices has changed the cyber security threat picture because of the ways in which they can be hijacked at scale, which in turn has increased the magnitude of potential (and real) attacks. Moreover, the first generation of IoT devices were riddled with common security flaws, for which the fix was product regulation. This then takes us to EU level intervention, because of the way in which the Single Market works. So, the EU took new powers in the Cyber Security Act of 2019 to regulate products in pursuit of cyber security, and followed this up with a directive on IoT security, applied EU wide, in 2021. Going further up the national security food chain, the Network Information Systems (NIS) Directive of 2016 was a mandate from the Commission to Member States requiring critical sectors, such as health, water, energy, telecoms and finance, to adhere to certain cyber security standards. And, the Digital Operational Resilience Act, or DORA, of 2020-21 introduced highly specific requirements to apply throughout the EU in financial institutions.

So, responding to cyber threats within the European Union is a mostly unplanned mix of rules, procedures and capabilities divided between Member States and the EU. This gives rise to several problems.

First, given how important the Member State governments are for determining national cyber security, it matters that capabilities across EU Member States are very patchy. There are many attempts to rank national capabilities in cyber security globally, and whilst they show conflicting pictures, all illustrate a pattern in which many EU Member States fall short. In the UN's International Telecommunications Union's latest Global Cybersecurity Index (2020), three EU countries make the top ten (Estonia, Spain and Lithuania). A further four – France, Luxembourg, Germany and Portugal – are in the top 20. However, some nine EU Member States rank outside the top 40, and six outside the top 50, with, in general, a pattern that the further south and east one goes, the weaker the capabilities (the exceptions are the Baltic states, with strong rankings, and Ireland, a north-west outlier ranked 54th). Second, the division of responsibilities between Member States and the EU's institutions makes a coherent strategy on strategic autonomy very difficult to conceive, and nearly impossible to deliver. This is augmented by a third problem, which is a lack of capability within the EU itself. This is both operational, where its two main operational bodies – CERT-EU, which deals with emergency response, and the External Action Service's IntCen (Intelligence Analysis and Reporting Centre) – depend on the more capable Member States for capabilities and threat information, and technical support. ENISA – the EU's cyber security agency – is significantly smaller than many national authorities for cyber security and it is based in Greece, far from the normal centres of EU power and far from the main geographical regions in which technical expertise is concentrated.

And cumulatively, this takes us back to the crux of Arne Schönbohm's concern. As Aleksandra Samonek of the Catholic University of Louvain put it "in the case of Germany, the Commission tried to replace a more advanced security strategy with a less advanced one". Till such matters are resolved, serious impediments to a coherent plan for EU cyber security autonomy will remain.

The lack of indigenous European technological capability

Striking a more optimistic tone, such problems are technocratic and fixable, and the EU has shown an ability, at least over time, to evolve in similar areas in the past. However, assuming the EU and its Member States can cohere better, a second, more fundamental obstacle awaits in the path to meaningful strategic autonomy in cyberspace. And that is the lack of indigenous European industrial capability in technology.

Europe is way behind both the United States and China in terms of indigenous technological industrial capabilities and therefore dependent on one or both of those technological superpowers. For as long as that remains the case, discussions of 'strategic autonomy' will to some degree be irrelevant.

Scale matters in technology. And in the top 20 technology companies by market capitalisation at the beginning of 2022, ten were American, five were Chinese, and the remainder were from Japan, Korea and Taiwan. Outside of the faltering telecommunications infrastructure market, where Nokia of Finland and Ericsson of Sweden provide crucial European (and wider western) capability in a contracting market, Europe has to buy virtually all of its large scale, strategically important technology from elsewhere, mainly from the United States. (Interestingly, given the profound shock to the world order represented by Russia's war in Ukraine, the country does not feature in this debate. Russian actors are very good at hacking other countries' technology; it has little serious technological capability of its own).

This has policy implications and national security ones too. For example, over the course of recent years both the UK and France have tried to reach an accommodation with the American authorities over implications arising from the predominance of US platforms and cloud service providers. The UK, after years of exhaustive negotiations, reached a legally binding agreement with the US in 2019 to allow the transfer of US held data to the UK, with strict controls, in the interests of national security and for the purpose of the prevention and detection of serious crime. Separately, late last year, Guillaume Poupard, head of France's cyber security agency ANSSI, called for EU wide regulations to prevent the dominant US cloud providers in Europe giving access to data held within the EU to the US authorities.

The precise details of this are largely irrelevant for our consideration of strategic cyber security autonomy in Europe. What matter is that the European continent's two major security powers – the UK and France – have been required to grapple with first order policy consequences of the dominance of US technology. The difference between the two is not so much that the UK achieved its policy goal and France has not, to date, done so. It is that the UK, for better or worse, is not in any meaningful way trying to reduce its dependence on US technology. France, and the wider EU, is.

And this dependency is starting to matter even more. At the start of the communications revolution, technology was unipolar. The vast majority of the technology that the world was coming to depend on was conceived, patented, standardised and built by the American private sector (drawing, of course, on some technological breakthroughs by the US military and agencies such as DARPA).

The dominance of US tech was painful for Europe, for sure, particularly in the aftermath of Edward Snowden's revelations of large-scale espionage by the US, including, allegedly, against European allies. The pain was compounded by a sense of impotence that there was precious little that could be done; ideas of easily breaking free of dependence on US tech were fanciful. Then German Chancellor Angela Merkel's calls for increased digital autonomy for Germany and Europe were met with repeated references to the underlying reality, and writing six years later, Julia Pohle

of the Konrad Adenauer Institute, wrote that "a common or at least consistent understanding of what is meant by this or what its associated requirements are, has yet to emerge".

However, over time, in this unipolar world of technology, the EU managed to begin to use its considerable regulatory power, utilising its position as home to half a billion wealthy Internet users, to chart a path into some form of global influence in the development of technology. Regulations, notably the General Data Protection Regulation, or GDPR, which came into force in 2018, is the most obvious example of that. And it was not just data protection regulators, but competition ones too, which began to flex their muscles. The size of the European 'policy' offices of American Big Tech companies in Brussels ballooned as a result. Despite its dependence on the US for its technologies, the sheer size of the EU market had given the Union a way in.

The Bifurcation of the Internet: Choices for Europe

But this model works best when there is a unipolar environment where, for all its faults, the 'American' Internet was broadly consistent with European values. The increasing and accelerating bifurcation of the Internet into two 'technospheres' – led respectively by the United States and China - is not only exposing the underlying weakness in Europe's technological capabilities but is also increasingly blunting the effectiveness of regulation – Europe's one major lever.

Unlike Russia, which poses a cyber security threat to the West solely by cheating on the American-built Internet, China (which does this as well, at high volume) has built, and continues to build, an entirely separate model of technology. It is extraordinarily large in scale, relatively cheap to buy, high performing, and, importantly, much easier for states to control. This more authoritarian version of technology is backed by a state strategy, the so-called "Made in China 2025" paper published in 2015 and sets out Chinese intentions to dominate key technologies by the middle of the next decade. Furthermore, by dint of the digital subset of its Belt and Road Initiative (BRI), it aims to export this to other countries. Hence the rise of the 'two technospheres'.

Despite the size of the EU digital market, and the Union's regulatory reach, no serious analyst of technology thinks that Europe is a third 'technosphere' at the moment, or will be one any time soon. European technology thought leaders know this themselves. A survey of more than two and a half thousand public, private and civil sector leaders conducted by Kaan Sahin and Tyson Barker for the German Council on Foreign Relations revealed that three quarters of them thought the EU was too dependent on external suppliers for cloud services, and nearly seven in ten thought the same for artificial intelligence. In both of these areas of critical technology, the US is the source of dependence. The figure fell to just over half when it came to 5G suppliers, where Europe does have considerable indigenous capability but the US does not, and here, the dependency was reckoned to be on China.

Both the Trump and Biden administrations have treated the rise of Chinese technologies as one of the most important aspects of their most significant foreign policy priority. Put simply, Washington now demands that the rest of the world chooses between its technosphere and Beijing's.

Despite the many, often well-founded concerns of European policymakers about American tech, it is demonstrably closer in its economic model and its ethics to the commercial model of the EU and the values of most European societies. So, the choice Europe faces in the long term is not really between the US and China, but between depending on the US or making a serious effort to depend more on itself. Fascinatingly, Sahin and Barker's study revealed a near split on the issue, with 54 per cent of those surveyed favouring strategic autonomy within Europe, and 46 per cent wanting to move closer to the United States.

But whichever path is chosen, Europe has to change. If the EU accepts the industrial weakness of its own position in the long term and allies more closely with the US, then a regulatory strategy based on reining in

American tech becomes impossible. But those who want to build Europe as a third 'technosphere' must realise that focussing the efforts of the Union on regulating American tech does nothing to achieve that. Nor do declaratory strategies. Repeated documents from the Commission and declarations from the Councils of Ministers that Europe must move towards strategic autonomy in technology does not create a European Microsoft. As Sahin and Barker have noted, "the push for digital or technological sovereignty or a "European third way" are buzzwords often heard thrown around. The prevalence of these buzzwords signals a deep desire and strategic need for technological autonomy. But the question of how the EU can achieve that goal remains unanswered".

They also note the rise in China, and the return in the US, of what they call 'tech-industrial policy': strategic planning to ensure competitive, innovative and reliable technological capabilities. If the EU is serious, over the long-term, about challenging the two leviathans of the modern digital age, it will need to get serious about tech-industrial policy. This will be a huge challenge: the Single Market is not designed to accommodate a continent-wide strategy of fostering giants. Indeed, it can (and has been) argued that the EU's focus on low consumer prices forced a once thriving telecoms industry into disastrous consolidation and its customers into dangerous levels of dependence on Chinese suppliers. But if the EU is to develop the sort of technological capability it needs within its borders, these are the challenges that must be confronted.

For now, these issues will be parked in the slow-moving but vital talks under the auspices of the EU-US Trade and Technology Council, initiated by the EU last year. This was the result of a realisation in Europe of both the scale of the challenge of digital authoritarianism from China, and that the concern over the matter was not going to leave the White House with Donald Trump. Whether Europe achieves strategic autonomy or not, it is still going to be closer to the US on technology than it is to China. But to achieve strategic autonomy, another realisation will have to be accepted: autonomy in cyber security cannot be fully achieved if you're mainly securing someone else's tech. And changing this goes to the heart of how the EU is run. Arne Schönbohm's dissent might just be the start of a challenging but crucial era in European cyber policy and posture.

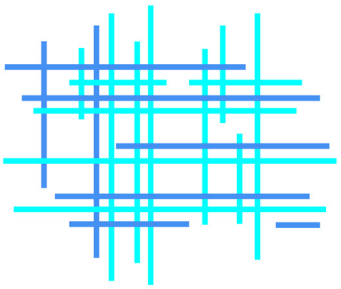
The Institute of International and European Affairs (IIEA) is Ireland's leading international affairs think tank. Founded in 1991, its mission is to foster and shape political, policy and public discourse in order to broaden awareness of international and European issues in Ireland and contribute to more informed strategic decisions by political, business and civil society leaders.

The IIEA is independent of government and all political parties and is a not-for profit organisation with charitable status. In January 2021 the Global Go To Think Tank Index ranked the IIEA as Ireland's top think tank.

The IIEA acknowledges the support of the Europe for Citizens Programme of the European Union.

IIEA

Sharing Ideas
Shaping Policy



Europe's Digital Future

IIEA
Sharing Ideas
Shaping Policy

An IIEA project supported by Google