RISCS

EU cyber policy workshop report

Future directions in EU cyber security: implications for UK policy and strategy

RISCS held an online policy workshop on 13th January 2022 with 30 participants from Government and academia as part of the RISCS International Dimensions theme led by Fellow Dr Tim Stevens.

Context

The UK's departure from the EU has sharpened the need for timely and insightful research into EU cyber security policy and strategy and how this affects the UK. This workshop brought together policymakers with researchers to explore future directions in EU cyber security and implications for UK cyber security policy, strategy, decision-making and research. During the session, working groups investigated three priority questions which were identified in collaboration with our project partners, NCSC, around law and regulation, technological sovereignty, and EU partnerships.

The aim of the session was to achieve a collective understanding of the latest thinking and look to identify possible future research questions which have value for the policy community.

Key Points

- The EU is looking to achieve 'digital and technological sovereignty', but there is a lot of ambiguity about what this would look like in practice. EU member-states have different values, levels of trust and attitudes to risk.
- While the UK may have gained some independence post-Brexit, it could end up being constrained by international standards if it is not involved in the appropriate development processes.
- It is an ideal time for the UK to consider the direction of travel as a middle power exerting its view of cyber security in an international landscape in the context of a new cyber strategy and revised international position.

The three priority questions were:

- What EU legal and regulatory developments in cyber security are likely to require UK responses and/or alignment?
- What does EU 'technological sovereignty' mean for UK cyber security?
- What renewed or additional cyber security partnerships should the UK seek with EU agencies and organisations?

The report summarises the discussions from the workshop, set out as themes which emerged across the separate groups. We invite the RISCS community to consider taking the potential questions for further investigation forward and explore how we can support research and collaboration.

1. Understanding the EU's aspirations and values:

Digital and technological sovereignty

The EU's stated ambition to achieve 'digital and technological sovereignty' was articulated during the European Commission President Ursula von der Leyen's inaugural speech in November 2019. A working definition was proposed by a European Parliamentary Research Service report as "the ability [of the EU] to develop, provide, protect and retain the critical technologies required for the welfare of European citizens and prosperity of European businesses, and the ability to act and decide independently in a globalised environment". As a minimum, this would require the EU to increase investment in research and development (R&D) and translate this into marketable goods and services to reduce its dependence on non-EU countries. This would require regulatory support, including the development of policies and standards reflective of European values. This is already happening: for example through the 'EU Chips Act' which looks to scale-up manufacturing and innovation in semiconductor technologies and make Europe an 'industrial leader' in semiconductors.

This overarching concept is widely regarded as ambiguous and in need of clearer definition in both its detail and its strategy. The scope of 'technology' is unsurprisingly wide, but the concept of 'sovereignty' is more problematic for the EU, its partners and even competitors. The EU seems to be looking for technological sovereignty as a defence against 'digital colonisation' by the US and China, and to prioritise its capacity to compete with its economic and strategic rivals. These aspirations also suggest that power and authority over 'technological' issues will be shifted away from member-states to the EU.

Implications of the digital and technological sovereignty ambition

For EU member states

The EU by no means speaks with one voice on cyber security matters, rather its member states have different values, levels of trust and attitudes to risk. The extent to which this will play into the EU's ambition and potentially complicate cyber security regulation and governance remains to be seen. The values relevant here include differing security and economic goals and commitments to human rights, privacy and data access. For example, the Visegrád Group countries (Czech Republic, Hungary, Poland, Slovakia) have been considered to have aligning views, but have differing approaches to tackling online harms and cybercrime.

Attitudes to risk depend on a country's geopolitical context and domestic political calculations. Any EU-wide risk assessments required by 'technological sovereignty' may need to be diluted to accommodate member-states' priorities. There may be tradeoffs between these the value placed on each of these elements, requiring democratic debate. Participants discussed the idea of a 'digital social contract' to govern digital technologies as a solution. It could allow the EU to be driven by an agreed set of principles rather than private sector needs (as in US tech companies) or demands of authoritarian regimes (as in China and Russia). It would necessarily consider whether the private sector should be a trusted partner in a regulatory network, a digital service, or an informal governance mechanism.

For the UK

This agenda could exclude the UK from opportunities with the EU, or force it to align with new standards in order to access markets or to be a part of security initiatives. Participants discussed whether alternative business models for UK-based digital service companies could be more aligned with UK values but allow them to join the market. It's still unclear what this ambition could mean for other international groupings (such as the NATO and Five Eyes alliances).

Questions to explore

- What does the EU mean by 'technological sovereignty' and how does it want to achieve it?
- What do EU member states think about working towards technological sovereignty?
- What values are attached to an agenda for technological sovereignty (regarding security, economy, privacy and human rights)?
- What would a 'digital social contract' look like and does this align with the UK's aspirations?
- What is the private sector's role: can it be a trusted partner in a regulatory network?
- To what extent will the EU be affected by the approaches to technology of its allies and competitors, such as Russia and China?

2. UK aspirations and alignment with the EU

The UK as a 'science and technology superpower'

Participants considered the UK's aspirations set out in recent policy announcements and to what extent they align with those of the EU and of member states. The UK hopes to be a 'science and technology superpower' – supported by announcements to increase R&D spend to £20bn a year by 2024/5 and a new Office for Science and Technology Strategy. The UK National Cyber Strategy 2022 includes an aspiration to "shape global governance to promote a free, open, peaceful and secure cyberspace" and to promote multi-stakeholder processes for governance of the internet (such as ICANN and the IGF). The UK has indicated its desire to take a more active international leadership role, including through continuing to develop digital technology standards as demonstrated with the ETSI standards for consumer Internet of Things (IoT) security.

Brexit impacts

The lack of national borders in cyberspace makes alliances and partnerships essential to maintaining UK cyber security. As an EU member-state, the UK was integral to developing EU cyber security policy over many years and benefited from it. The UK's decision to leave the EU in 2016 has affected the political climate on every topic in a multitude of ways. There has been a mutual appetite for collaboration on cyber security, including positive indications towards further cooperation with ENISA (such as on capacity building, knowledge sharing and education) when the COVID-19 crisis subsides. However, this is impacted by tensions in other areas, such as the implementation of the Northern Ireland Protocol and other elements of the Trade Cooperation Agreement (TCA). This adjustment has impacted how UK and EU civil

servants work together in terms of information-sharing and day-to-day cooperation, with participants suggesting that these collaborations do not always directly reflect formal agreements.

The immediate impact of Brexit was a reduction in the operational effectiveness of security and policing (for example, being outside of ENISA and Europol), as well as excluding the UK from EU cyber security decision-making. Despite it being low on the political agenda during the Brexit referendum and EU withdrawal negotiations, law enforcement practitioners and others voiced concerns about reduced policy and operational co-operation on cyber security post Brexit. The TCA includes voluntary arrangements for the UK to work with ENISA and other bodies including the EU's Computer Emergency Response Team (CERT-EU).

UK-EU alignment

The EU's direction of travel on cyber policy continues to be important to the UK and the future alignment of UK and EU policies is a topic of interest. One challenge is that EU member states which align most closely with the UK's aspirations (such as the Netherlands) are smaller and 'quieter' on the EU stage, which may prevent less direct future UK-EU alignment. Another concern is that the UK-EU relationship could be strongly politically influenced by the country holding the EU Council presidency, resulting in an absence of long-term stability. It is unclear how the UK's unwavering strategic commitment to the US may help or hinder UK-EU alignment on cyber security issues, including the law and ethics of offensive cyber operations and military cyberwarfare. Neither the National Cyber Strategy or the 2021 Integrated Review include particular commitments to work with the EU over other partners which may be a missed opportunity for strengthened collaboration.

Questions to explore

- How will the UK's 'science and technology superpower' agenda be affected by EU technological sovereignty?
- What are the implications of EU technological sovereignty for the UK's strategic ambitions in technology leadership and economic influence?
- What cyber security cooperation and alignment should the UK seek in further political settlements and adjustments to treaty law?
- How can the UK leverage its EU relationships to contribute to cyber diplomacy, or should it seek its own path? Can it do both?
- What scope is there for furthering collaboration between the UK National Cyber Force and the EU Joint Cyber Unit?

3. UK partnerships and influence

International partnerships

The UK was a leading cyber security nation in the EU and has had a disproportionately powerful position in international cyber discussions, such as most recently in the International Telecommunication Union (ITU) negotiations on emerging technology rules and standards. The new UK National Cyber Strategy reaffirms and deepens the government's emphasis on international engagement, whereby it will seek to work with EU partners on equal terms with other multilateral organisations and partnerships, including the UN, Five Eyes, NATO and the G7.

Mutual legal assistance (MLA) is a method of cooperation between states for obtaining assistance in the investigation or prosecution of criminal offences. Requests can be made formally into mutual legal assistance treaties (MLATs) as an opportunity to enable productive international collaborations. A growing number of MLA mechanisms are appearing in relevant cyber policy areas. Participants suggested that it would be useful to understand how well these are working and whether there are opportunities for the UK to build new collaborations in this way.

Cyber policy and diplomacy issues

The UK was recently brought into an argument between the US and China over Huawei, resulting in the UK removing Huawei from its current and future 5G networks. This was not simply a technology issue: it highlighted the UK being forced to pick sides between the US and China. Similarly, standards setting processes are not just a technicality. They come with questions around which standards should be adopted and whose interests they reflect. While the UK may have gained some independence post-Brexit, it could end up being constrained by international standards if it is not involved in the development processes of those standards. The ongoing refinement of the EU cyber security certification framework for ICT products is a real example of this, as it affects UK businesses wishing to sell into an emerging European Digital Single Market.

Questions to explore

- To what extent does the UK's cybersecurity depend on partnerships with the EU, versus other partnerships such as the US, NATO and Five Eyes?
- How can the UK's influential position in NATO contribute to closer EU-NATO cooperation?
- How well are current cyber-related MLATs working and what opportunities are there for the UK to pursue our own?
- How can the UK contribute to the direction of global cyber policy as a 'middle power' outside of the EU?
- Could a mapping exercise be used to identify initiatives around the world (e.g. forthcoming policies, regulation and standards) across the cyber policy landscape?
- What is the UK's approach to standards setting and what does the right process for setting standards look like internationally?

4. Looking to the future

The UK as a 'middle power'

Divergent national approaches to technological innovation by the UK's allies and competitors will shape the trajectories of its uptake and deployment of new technologies. This, alongside the contrasting approaches and geopolitical context of the American and Chinese digital superpowers, could be an opportunity for the UK to explore the idea of acting as a flexible middle power in this field. Specifically, the UK could be a bridge between the US and the EU, exploring the traditional 'special' relationship with the US, as well as building selective strategic partnerships with the EU and/or like-minded EU member-states. The UK could act as an essential partner that understands both and become a core component of a western 'cyber alliance'.

An opportunity?

The lack of cohesion and cooperation among EU member states in the fields of AI, quantum computing and other emerging technologies, combined with the UK having comparatively less bureaucracy (for example in terms of launching new policies and allocating funds) could provide a window of opportunity for the UK to 'keep up' in the technological race of the 21st century.

This is a multi-disciplinary, sociotechnical policy question of national interest. EU cyber security developments offer practical, normative, political and strategic challenges to the UK, as well as opportunities for leverage and partnership. It is in the UK's interest to leverage its position and develop these strategic partnerships to maximize the opportunities presented in this report.

Contributors

This workshop and report were produced in partnership with Florence Greatrix in UCL Engineering's Policy Impact Unit (PIU) as part of the Research Institute for Sociotechnical Cybersecurity (RISCS) Fellowship on the International Dimensions of Cybersecurity, led by Dr Tim Stevens, KCL.

This workshop series on the RISCS Fellowship themes is funded by the UCL EPSRC Impact Acceleration Account and by RISCS.

The team is particularly grateful for contributions and engagement from NCSC who worked with us to identify the topics for this session, and from the Academic Chairs for each group: Professor Lorna Woods (University of Essex), Dr Andrew Liaropoulos (University of Piraeus, Greece) and Dr Helena Farrand-Carrapico (Northumbria University).

Participants list by organisation

- University of Aberdeen
- University of Bath
- University of Bristol
- Cardiff University
- City, University of London
- Department for Digital, Culture, Media and Sport
- University of Essex
- Foreign, Commonwealth and Development Office
- King's College London
- National Cyber Security Centre
- Newcastle University
- Northumbria University
- University of Piraeus, Greece
- Royal Holloway, University of London
- University of Sheffield
- University of Southampton
- University College London

Contact us

Dr Tim Stevens, Senior Lecturer in Global Security and head of the KCL Cyber Security Research Group, King's College London
RISCS International Dimensions Fellow
tim.stevens@kcl.ac.uk

For more information on the PIU, please visit our web pages.