

**British-Irish  
Parliamentary  
Assembly**



**Tionól Parlaiminteach  
na Breataine agus  
na hÉireann**

---

Committee B (European Affairs)

---

Interim Report on

UK-EU Defence and Security Co-operation Post-Brexit

May 2023



# Contents

<b>1. Introduction</b>	<b>1</b>
<b>2. Response to the war in Ukraine and threat from Russia</b>	<b>5</b>
<b>3. Cybersecurity</b>	<b>10</b>
<b>4. Intelligence and Policing</b>	<b>11</b>
<b>5. Summary of conclusions and recommendations</b>	<b>13</b>



## 1. Introduction

---

1. Post-Brexit, and particularly since Russia’s invasion of Ukraine in February 2022, there has been a significant shift in the European defence and security landscape. Governments from across the UK, Ireland and Europe have worked together to respond to the situation in Ukraine – including, most notably, on military support and sanctions – and the UK and EU are continuing to develop new defence and security arrangements since the former left the European Union in 2020. The war in Ukraine has led to a significant shift in German defence policy, resulted in applications by Sweden and Finland to join NATO and, just last month, the Irish Government announced the upcoming Consultative Forum on International Security Policy, which will “allow for a discussion on Ireland’s policy of military neutrality.”<sup>1</sup> Many of these developments would have been unthinkable just 18 months ago.
2. Most recently, we note reports that Russia has a programme to sabotage wind farms and communication cables in the North Sea<sup>2</sup> and UK Ministers have warned of Russia-aligned hackers that are seeking to “disrupt or destroy” Britain’s critical infrastructure.<sup>3</sup> Also, it is well known that Ireland plays a significant role in the world of data, both regulatory and subsea physical infrastructure, with 1,000s of kilometres of cables presenting complex security concerns.
3. It is with all this in mind that we launched a new-three part inquiry into UK-EU Defence and Security Cooperation Post-Brexit to review the current landscape and to make recommendations based on the evidence we received. Our inquiry is examining the response to the war in Ukraine, cyber security and intelligence and policing.
4. On 13 October 2022, we announced the following terms of reference which would provide the basis for our work. The aim of the inquiry is:

---

<sup>1</sup> Irish Department of Foreign Affairs, [Tánaiste announces plans for a Consultative Forum on International Security Policy](#), 5 April 2023

<sup>2</sup> BBC News, [Ukraine war: The Russian ships accused of North Sea Sabotage](#), 19 April 2023

<sup>3</sup> BBC News, [Russia-linked hackers a threat to UK infrastructure, warns minister](#), 19 April 2023

## Ukraine

- To consider the approaches of the UK Government, Irish Government, Crown Dependencies, devolved UK legislatures and EU in response to the crisis in Ukraine.
- To consider the cooperation between the UK, the EU and its individual member states and how effective this cooperation has been.
- To consider the impact of Brexit on the UK's cooperation with European partners in the context of Ukraine.
- To consider whether there are any lessons to be learned thus far from UK-EU cooperation on Ukraine or whether there are future opportunities to do things differently.
- To consider the outlook for longer term UK/EU cooperation on defence and security.
- To consider to what extent the recent change in German defence policy, the prospect of Finnish and Swedish accession to NATO and the AUKUS agreement has had on the UK-EU defence and security relationship.

## Cyber security

- To consider the biggest challenges facing the UK, Ireland and EU in cybersecurity, including whether they have identified the same priorities and whether are they broadly aligned in what they need to do to address these challenges.
- To consider how the UK, Ireland, Crown Dependencies and EU can cooperate effectively to tackle these challenges now the UK is no longer part of EU bodies including its Agency for Cyber Security (ENISA).
- To consider implementation of the UK-EU Trade and Cooperation Agreement in this area, including the current status and outcomes of the 'regular dialogue'.
- To consider whether there are lessons to be learnt from how the UK and EU Member States pursue such cooperation in other settings, such as NATO.
- To consider the extent to which the UK and EU's separate legislative agendas are compatible or divergent.

- To consider how the UK and EU can cooperate effectively to influence cybersecurity standards for existing and emerging technologies.
- To consider any risks for effective cooperation between the private sector in the UK and Ireland/ the EU if there is regulatory divergence and the impact on private and academic sectors ability to cooperate on cyber.
- To consider the importance of UK researchers being able to participate fully in EU-funded research into new cybersecurity measures under the 'Horizon Europe' programme.

#### Intelligence and policing

- To consider the practical impact of the arrangements for law enforcement and criminal justice cooperation under the UK-EU Trade and Cooperation Agreement (TCA).
- To consider the impact of Brexit on practical law enforcement cooperation on the island of Ireland and between Irish and relevant UK authorities.
- To consider the legal structures and/or mechanisms that now apply to the exchange of operational information between law enforcement authorities in Ireland, the Crown Dependencies and in the UK.
- To consider whether the UK and Ireland have concluded any bilateral cooperation agreements since the UK left the EU to facilitate cross-border cooperation, over and above the long-standing Common Travel Area.
- To consider the effectiveness of TCA provisions on surrender/ extradition and whether the transition from the (pre-Brexit) European Arrest Warrant (EAW) procedures to the new TCA procedures has been straightforward.
- To consider whether post-Brexit developments in EU or UK law could jeopardise cooperation under Part Three of the TCA (e.g.: UK Bill of Rights, Data Protection and Digital Information Bill as well as proposed changes to the EU's Prüm rules governing the transfer of DNA and fingerprint data during criminal investigations).

- To consider whether there are specific areas of law enforcement and criminal justice cooperation in which differing EU and UK approaches to the use of technology, or the development of standards, could jeopardise cooperation under Part Three of the TCA.
  - To consider whether the UK's exit from the EU affected the Irish Government's approach to its EU justice and home affairs opt-ins and whether divergence in substantive criminal laws and procedures in Ireland and the UK make cooperation more difficult over time.
5. This report predominantly covers the first part, the response to Ukraine, although we also touch on issues relating to the second and third parts of the inquiry that came up during our evidence gathering, given their wider relevance to Russia and the conflict in Ukraine. We intend to take further evidence on cyber security and intelligence and policing from other witnesses, including industry, and will publish a second report in due course.
  6. We held our first evidence session in London on 13 October 2022 where we took evidence from Ian Bond, Director, Foreign Policy, Centre for European Reform; Dr Nicholas Wright, Visiting Researcher, Centre for Britain in Europe, University of Surrey; and Irish Vice Admiral Mark Mellett DSM (retired). We visited Brussels on the 30 and 31 March 2023 to be briefed by or take evidence from: Lindsay Croisdale-Appleby CMG, Ambassador and Head of the UK Mission to the European Union; Brigadier John Oldroyd, Deputy MILREP (EU) and UK Defence Advisor, UK Mission to the European Union; Angelina Eichhorst, Managing Director, Europe Division, EU European External Action Service; Joanneke Balfort, Director of Security and Defence Policy at the EU European External Action Service; and Nick Pickard, Deputy Permanent Representative, UK Joint Delegation to NATO. We received written evidence submissions from a number of stakeholders, including Cisco Systems UK and Ireland; Dr Amanda Kramer, University of Belfast; Gemma Davies, Durham University; and Rights and Security International. We are extremely grateful to all those who have engaged with our inquiry by providing evidence or briefing on this subject.

## 2. Response to the war in Ukraine and threat from Russia

---

### Overview

7. The ongoing conflict between Russia and Ukraine has highlighted the vulnerability of countries across the continent of Europe to geopolitical threats. Against this backdrop, relations between the UK and EU (including Ireland) have often been strained, following Brexit. However, each of the stakeholders we heard from have been clear that both sides continue to hold similar values and perspectives, not least in their shared view that the Russian invasion is a gross violation of international law. UK-EU relations have warmed significantly since the announcement of the Windsor Framework on the implementation of the Northern Ireland Protocol in February 2023. It was pleasing to hear that the UK is now gradually advancing the nature of its relationship with the EU on a range of foreign and defence issues, outside of the UK-EU Trade and Cooperation Agreement structures. The UK signalling its willingness to join to the EU Permanent Structured Cooperation (PESCO) military mobility project to contribute to driving defence cooperation is a key example. There is clearly a desire on both sides to deepen the UK-EU security and defence relationship and now that mutual trust is increasing, this can now be achieved more easily. We note the EU External Action Service comment that working with the UK represents more than just working with a normal third partner, which reinforces the importance of our inquiry.

### UK-EU cooperation on Ukraine

8. On Ukraine specifically, stakeholders suggested that there has been very strong cooperation in many areas and military to military relationships have been good throughout. The UK Government, we heard, is acting in a pragmatic, cooperative way and there was a concerted effort to ensure that both UK and EU responses to Ukraine were complementary. There has been tangible cooperation on sanctions against Russia and Belarus, as well as military support (including weapons and tanks) and training for Ukrainian service personnel. Both sides have schemes in place for hosting Ukrainian refugees (with Crown Dependencies such as the Isle of Man taking them in for the first time), and there is dialogue relating to financial support and reconstruction, and on accountability for international crimes. As a neutral non-NATO member, Ireland has



been contributing by way of non-lethal support, such as food, fuel and medical supplies. Where the European Peace Facility is used to reimburse EU countries for the delivery of military support to Ukraine, Ireland exercises its right to ‘constructive abstention’ in relation to lethal weapons and therefore does not contribute financially to such aid for Ukraine.

9. Prior to Brexit, we were told, the UK as a Member State was clued into what other EU Member States were thinking in relation to potential threats and the decisions in response to such threats. Stakeholders highlighted the importance of being “in the room” at EU level. In the early stages of our inquiry, we heard that it is no longer clear how well the UK can exercise its influence as it did before as a result of the UK’s withdrawal. However, the feeling from the UK Mission in Brussels more recently was that the impact of Brexit is minimal in terms of the UK and EU response to Russia’s invasion of Ukraine. We heard that the UK now has the benefit of acting independently of the EU and thus had the ability to respond faster following the Russian invasion. Nonetheless, it was noted across our evidence that the EU also responded very quickly given the number of countries within it.
10. We heard how, before Brexit, the EU was often reliant on intelligence supplied by the UK to underpin foreign policy sanctions and how this relationship is now weaker. While our evidence set out that informal channels have reopened in relation to sanctions, the UK has diminished influence in this area with very limited capacity to have a direct impact on EU sanctions. We note comments made about the problem of circumvention of sanctions imposed on Russia and Belarus and that this is a natural area for potential further cooperation post-Brexit. This is because the UK has greater access to information than many EU member states and there is potential for this to be made available across the EU once again. We also acknowledge the specific need for greater cooperation between the UK and Crown Dependencies on sanctions.
11. During our evidence gathering with stakeholders, we touched on the establishment of the European Political Community (EPC), an initiative bringing 44 countries together with the aim of strengthening relations between EU and non-EU countries who share the same European values and increasing political cooperation between EU and non-EU countries. The first summit of the EPC took place on 6 October 2022 with the second

due to take place on 1 June 2023 (where the UK and Poland are due to jointly host an event on security issues). Former UK Prime Minister Liz Truss' decision to attend the first EPC was commended by those we heard from, with the feeling that it is not possible to have a genuine discussion on European defence and security without the UK in the room. The UK is due to host the EPC in spring 2024.

12. We discussed whether the UK requires a formal relationship with the EU on defence and security beyond what currently exists. Given that, over the past year, intelligence has been shared, the cooperation on supplying weapons and training to Ukraine has been effective, there was not the feeling on the UK side that much would have been done differently with a formal relationship. The UK is agile in its current position outside the EU, although it could be when it was a Member State, we were told. There could be potential for a framework participation agreement with the EU which give third countries, such as the UK, the option to contribute to EU military operations. On a more general point concerning the UK side, we were told that there should be more consideration given to the turnover of staff responsible for developing and maintaining key relationships – the regular movement of people between roles risks losing trust and weakening UK-EU relations.

13. It should also be noted that the Tánaiste and Minister for Foreign Affairs and Defence, Micheál Martin T.D. has announced plans for a Consultative Forum on International Security Policy to take place in June 2023. The Forum will build a deeper understanding of the threats faced by Ireland, and the links to, and between, foreign security and defence policy. It will focus on a wide range of issues, including Ireland's efforts to protect the rules-based international order, through peacekeeping and crisis management, disarmament and non-proliferation, international humanitarian law, and conflict prevention & peacebuilding as well as allowing for a discussion on Ireland's policy of military neutrality. The Forum will also provide an opportunity to examine the experiences and policy choices of other partners in responding to the new security environment in Europe following the Russian invasion of Ukraine.<sup>4</sup>

---

<sup>4</sup> Irish Department of Foreign Affairs, [Tánaiste announces plans for a Consultative Forum on International Security Policy](#), 5 April 2023

## *Role of NATO*

14. As part of our inquiry, we heard about the role played by NATO and the role of the UK within NATO in the post-Brexit European security and defence environment. Throughout the Ukraine war, NATO has been used as a platform to meet allies and share and engage on information but has played a limited role in the war itself due to the risk of escalation. We were told the UK is doing more at NATO now that it no longer has representation within the EU. NATO is focussing on longer-term support for Ukraine; interoperability of military operations is important to ensure countries' support for Ukraine. We note the view that the recent applications of Sweden and Finland to join NATO have been widely seen as a positive step, as they are very like-minded allies for the UK in particular and bring capable forces. We recognise the sentiment that NATO unity is fundamental, especially with Russia moving to make attacks in the cyber sphere to gain strategic advantage.

## *Links between defence and security*

15. With reference to the Russia-Ukraine conflict, evidence conveyed to the Committee highlighted the inextricable link between economic security and state security with the war linking these further to energy security. We heard about the need for governments to provide resourcing for defence forces to enable the delivery of defence security and service across all five domains; that is land, air, maritime, cyber and space.

16. Since the war in Ukraine, the linkage between energy and security has been brought into sharp focus with the climate crisis further establishing the threat to security faced across the globe. Evidence referred to the lengthy period of peace and security enjoyed by Europe up to this point, a peace that can be attributed to the multilateral approach to EU values and principles.

## *Threat to critical infrastructure*

17. We discussed the significant vulnerabilities exposed by the attacks on Nord Stream which, at the time of writing, had been ongoing with attempts to interfere with communications cables as well as supply cables. It was also noted that Ireland is a major centre for the IT industry and banking sector. Ireland has sovereign rights over a jurisdiction that is almost one million square kilometres in size throughout which there are significant interconnectors of fibreoptic cables between Ireland and North America.

We noted the significant challenge for Ireland and all European states to protect this critical infrastructure in part due to its geographical location and its sheer size. It was made clear that any offshore infrastructure, be it floating wind farms or cabling infrastructure, carries a potential security risk that will require a collaborative approach in order to best protect it. This has been made clear from several instances of Russian vessels operating off the west coast undertaking perceived maritime surveillance activity.<sup>5</sup> Given this vulnerability, we note the view that the defence and resilience of this critical infrastructure is down to an EU-NATO taskforce, with NATO increasingly concerned by the threat to this critical infrastructure. We heard, from the EU side, that this is one area that could be on the agenda for security and defence dialogue with the UK, with Ireland playing an active role on the security side.

18. Our inquiry heard that, post-Brexit and in the context of Ukraine, there is an even greater need for a common vision and approach to security across the UK and Ireland, as well as Europe as a whole. There is a memorandum of understanding between Ireland and the UK which we heard is a good starting point in terms of greater collaboration to provide the security to protect UK-Irish infrastructure but also European infrastructure upon which all countries will be mutually dependent. We have shared jurisdictions and common interests and critically, the memorandum of understanding predates Brexit. As such, we were told it would be prudent to review the memorandum and look at how it can be enhanced to provide for current circumstances. Bilateral arrangements must of course take account of Ireland's membership of, and relationship with, the EU.

19. We note a collaboration between England, Wales, Scotland and Ireland with regard to renewable energy infrastructure in the Celtic Sea, North Sea and off the West Coast of Ireland. Such infrastructure will be largely autonomous and unmanned but will require an increased collaborative effort to ensure there is common infrastructure in terms of ports and also adequate security architecture.

20. With regard to renewable energy, the greater connectivity there is in terms of shared infrastructure, the greater the benefit for Europe. But, we heard, there are challenges in that the greatest ambition lies in floating offshore wind which will require significant

---

<sup>5</sup> The Irish Times, [Nato warns Ireland over Russian maritime surveillance activity](#), 4 May 2023

port infrastructure to assemble and facilitate the wind turbines. Currently, we do not have one port in any BIPA jurisdiction and as such, neither the UK nor Ireland is currently fit for purpose for floating offshore wind. Governments on both sides need to support the ambitions around floating offshore wind before moving on to collaborative initiatives such as the Celtic Sea lines to ensure best outcomes for energy security.

21. In terms of UK-Irish security architecture, stakeholders said there is a mutual interest with regard to offshore infrastructure that will need to be created together with developers before any infrastructure is put in place, perhaps as part of the licensing. To avoid significant retrofit costs to the State, security architecture should be looked at as a part of the offshore structures. Evidence set out to the Committee highlighted that such security architecture will require smart technology to support it as well as the response capability.

### 3. Cybersecurity

---

22. Given future plans for further offshore wind infrastructure off the UK and Ireland, we considered the vulnerability of such networks to the threat of cyber-attacks and whether more can be done for prevention and rapid response in such cases. Evidence pointed to the NATO Cooperative Cyber Defence Centre of Excellence in Tallin and the European Centre of Excellence for Countering Hybrid Threats in Helsinki as models for greater collaboration and understanding of hybrid and cyber.

23. We note comments that, from a government perspective, the issue of cyber security has never been more relevant as it is today where IT systems, data systems and communication networks support the effective running of the economy. It is important to recognise that while cyber-attacks may take place in London, Dublin or other European locations, these locations may not be the point of attack. This highlights the key challenge of addressing cyber security.

24. Due to the cross-border nature of cyber and hybrid attacks, we heard the need to strengthen mutuality in this area. Approaching cyber from a unilateral perspective simply will not work, we were told – there needs to be collaboration to remove vulnerabilities. The war in Ukraine and the increasing prevalence of cyber-attacks has proved to demonstrate the need for this greater level of international cooperation and as such, it is essential that the UK, Irish and other EU Governments develop policies and strategies in this regard.

25. While Ireland, the UK and the EU are broadly aligned in their approach to cyber space, stakeholders stated that Brexit has impacted EU-UK cooperation levels in this area. Given the shared threats faced by EU-UK and BIPA jurisdictions, greater cooperation and collaboration would be welcome. The regulatory divergence on cybersecurity following Brexit poses a threat to the security of both the EU and the UK. As such cooperation and better alignment of policy would cater to the needs of industry, Government and society. We note comments we heard in Brussels that more pragmatic cyber and counter terrorism cooperation between the UK and EU can now be expected, following the announcement of the Windsor Framework. On cyber, efforts are now underway to prepare the first meeting of the formal UK/EU cyber-security dialogue, as foreseen by the UK-EU Trade and Cooperation Agreement (TCA).
26. It is clear from our evidence gathering that both the EU and UK have shown leadership in the area of cyber security, with the EU legislating and creating common EU standards and the UK committing to advancing the UK's global leadership and influence in its recent Cyber Security Strategy. Both the UK and Ireland are moving ahead with enhanced legislation regarding cybersecurity and cybercrime with the EU working towards building upon its current legislative framework through its draft "Cyber Resilience Act".
27. While there is potential for greater cooperation between the EU and UK with regard to legislative alignment, this would be a political decision. On a collaborative level, the EU-UK TCA commits to establishing regular communication to enable the exchange of information regarding cyber security, defence and cybercrime. While these are positive steps, stakeholders emphasised that there is a need for far greater collaboration in this area.
28. We were told of the potential risk that EU leadership on cyber security legislation may lead to further divergence in policy between the EU and the UK. Again, better engagement and policy alignment is necessary to ensure this does not occur.

## 4. Intelligence and Policing

---

29. In relation to Ukraine, the UK and US shared considerable amounts of intelligence with the EU because, we were told, they needed to work closely with allies. More generally, while the UK-EU Trade and Co-operation Agreement (TCA) has ensured that the impacts of Brexit has been minimal, evidence suggested that there are areas where further bilateral arrangements would be beneficial where Brexit has impacted practical law enforcement co-operation, including on the island of Ireland. We heard the desire

for a closer extradition and intelligence arrangement than the one in the TCA, although that has been made to work. There is a large network of intelligence agencies and more can be done over time to improve cooperation, although it is not clear what appetite there is for that at the moment.

30. We note the need to review how to strengthen our military intelligence services as potential indications may have been missed regarding the Russian invasion of Ukraine. Russia had been controlling LNG supplies which should have raised a red flag in Europe. This reiterates the need for better collaboration, better co-operation, and better sharing of information across jurisdictions between the UK and Ireland and the UK and the EU.
31. We heard that close co-operation between the UK and Irish law enforcement is required in relation to cross-border crime due to the open border between Northern Ireland and Ireland. Under the TCA, a new security partnership was agreed in relation to cross-border criminal activity. While some cross-border issues of law enforcement are dealt with cooperatively between the PSNI and An Garda Síochána, stakeholders expressed concern that, following Brexit, UK legislation – having no constitutional safeguards – will undermine human rights protections as provided for under the Treaty of Lisbon and the Charter of Fundamental Rights in the EU.
32. We were told that there are a number of cross-border areas which also require further examination and enhanced cooperation measures following Brexit. These include mechanisms regarding the exchange of operational information between law enforcement authorities in Ireland, the UK, and Crown Dependencies, such as financial information, DNA and fingerprint exchange, vehicle registration data, passenger name records and criminal records.
33. In addition, stakeholders highlighted that the sharing of evidence was provided for under a previous EU framework for which there is not yet a replacement mechanism. The Committee agreed that a bilateral arrangement would facilitate freer movement throughout the Common Travel Area (CTA). It should be noted, however, that the existence of the CTA has long required bilateral cooperation between police authorities across BIPA jurisdictions and has survived the UK's exit from the EU.

34. On an EU-UK level, the TCA provides for new arrangements between the UK and Europol. While this is welcome, we note, from the evidence heard, a number of practical issues; one being that the UK no longer has access to the Europol Information System (EIS) and two being that the UK no longer can participate in institutional decision-making on the operational and strategic development of Europol. As a result, crime threats of interest to or affecting the UK will not be the focus of Europol.
35. A significant loss resulting from Brexit is the UK's access to SIS II which allows the efficient sharing of information with EU Member States. The TCA does allow for new bilateral mechanisms to be developed once they are in line with EU law and future information sharing will be dependent on when these new mechanisms are developed and the maintenance of strong inter-State relationships. Stakeholders expressed concern that proposed legislative changes within the UK has the potential to jeopardise maintaining the trust and relationships with Member States.

## 5. Summary of conclusions and recommendations

---

**36. The evidence provided to the Committee has shown that while there is significant cooperation across BIPA jurisdictions and indeed on an EU-UK level, greater efforts could be made to ensure a more collaborative approach to security and defence, including cyber and hybrid risks while also being cognisant of Ireland's longstanding tradition of military neutrality. In light of this, we make the following recommendations:**

- **We recommend a joined-up approach and vision to defence and security across the EU-UK and UK-Ireland-Crown Dependencies. Focus should be given to cooperating more effectively on sanctions and particularly critical infrastructure, where there appears to be most scope for improvement. Consideration may wish to be given to a framework partnering agreement that would allow the third countries, such as the UK, to participate in EU operations.**
- **Due to the UK's Crown Dependencies not being part of the UK and each having separate legislative provisions in many of the areas covered by our report, we recommend improved information sharing between the UK Government and**



**Crown Dependencies on sanctions, cyber security and financial intelligence to ensure that future cooperation is more effective.**

- **We recommend that adequate resourcing for defence and security is provided by the relevant governments to ensure security levels are maintained effectively in BIPA jurisdictions. We recommend that staff churn, particularly in the UK Government, is addressed to avoid a detrimental impact on security and defence relationships with Ireland and the EU.**
- **We recommend a full review of the Memorandum of Understanding regarding defence cooperation between Ireland and the UK to ensure it is up to date with current arrangements following Brexit and to enhance future defence cooperation.**
- **We recommend an examination of the NATO Cooperative Cyber Defence Centre of Excellence in Tallin and the European Centre of Excellence for Countering Hybrid Threats in Helsinki as models for greater collaboration and understanding of hybrid and cyber.**
- **We recommend greater consideration be given to the area of energy security and how it impacts on the economic security of countries within the continent of Europe.**
- **We recommend that governments support the ambitions around floating offshore wind without delay and encourage the development of port infrastructure to facilitate this in BIPA jurisdictions. We also recommend that priority is given to developing security for offshore wind infrastructure in advance or in tandem with such ambitions as part of the licensing process.**
- **We recommend that unilateral approaches to cyber security should be avoided and encourage stronger engagement and collaborative policy development on an EU-UK and UK-Ireland level to ensure best outcomes for industry, Government and society.**

- **Due to its cross-border nature, we recommend that regulatory divergence in the area of cyber security be avoided in as far as is practicable between UK and EU Member States in order to best protect the security of all jurisdictions.**
- **We recommend a review of the bilateral arrangements and mechanisms between Ireland and the UK following Brexit to ensure efficient sharing of evidence and information in the area of intelligence and policing. We also recommend a closer UK-EU relationship on extradition and intelligence sharing.**