

## KEEPING EUROPE SAFE AFTER BREXIT

Findings of a reflection group led by Marta Dassù,  
Wolfgang Ischinger, Pierre Vimont, and Robert  
Cooper. Edited by Susi Dennison



20 March 2018

### SUMMARY

- There is a strong rationale for close EU-UK cooperation on security and defence after Brexit. Each side should preserve the principle of cooperation in different arrangements for different areas, from policing to foreign policy.
- The EU should embrace the UK's proposal for a treaty on intra-EU security. Because no such treaty will be ready by March 2019, each side should aim for an interim agreement extending existing arrangements until one is in place.
- On foreign policy and defence, the UK should not expect a seat at the table in European bodies, including in discussions around possible CSDP operations. Instead, both sides should establish new arrangements that keep them in touch with the other's thinking. Regular working-level

exchanges rather than a treaty are the aim here, such as monthly bilaterals between the British embassy in Brussels and the PSC chair, and UKREP and the EDA chief executive.

- All this is achievable but needs clear principles if it is to succeed. These include: a broad understanding of the components of European security; agreement that unique arrangements are required for a unique situation; and a commitment not to treat security like just another element within the Brexit negotiations.

Now is not the moment for either the European Union or the United Kingdom to risk allowing the political tensions around Brexit to harm their own interests or weaken protection of their citizens. On the contrary, this is a moment that demands cooperation, investment in research and capabilities, and renewed commitment in order to deepen European security, regardless of Brexit.<sup>[1]</sup>

While the UK's departure from the EU is a major challenge to Europe's continued cooperation on security matters, in particular given the political and institutional obstacles that it entails, this event could also serve as a valuable opportunity to look critically at the array of threats that Europe is currently facing as well as the ways in which it should respond to them. From that perspective, the issue of EU-UK post-Brexit cooperation on security should not get bogged down in procedural matters around EU treaties and the process side of exit. Instead it should be an inherently political and a strategic matter. The question that we should be asking is about how to develop a new EU-UK security partnership that enhances Europe's comprehensive security and its power in the world.

This paper sets out the principles which should serve as the basis for constructive EU-UK security cooperation after Brexit. It focuses on the political economy of making this happen by placing emphasis on the major obstacles that the EU and the UK alike need to tackle. It then assesses key questions that both parties will have to reflect on before engaging in the negotiations on this complex and difficult matter. Finally, it

proposes some concrete ways of doing this.

### ***Security challenges***

Europeans live in an increasingly complex security context. This includes:

- old and new external threats and challenges including: Russian subversion and intimidation from the east; instability and asymmetric threats in the Mediterranean; economic and strategic competition from China and other emerging powers; immigration and integration pressures, linked to climate change, conflict, and resource scarcity; and the challenge of cyber threats.
- the growth in the scale, impact, and complexity of terrorism, cyber crime, and organised crime. These threats have become more transnational and globalised in nature. Organised crime in particular now sees a more dominant role played by technology and cross-border movements of suspects, trafficked victims, firearms, and illicit money. There is a blurring of the distinction between state and non-state actors, and of who controls the technology and weapons that they use.
- growing interlinkages between external and internal security issues, as well as between military and non-military ones, in the form of hybrid threats.
- redistribution of power across the world, in the context of deep changes in the global order. This includes rising doubts concerning the US security guarantee for Europe, which did not begin only under Donald Trump. This has prompted European countries to strengthen their security and defence cooperation.

These challenges threaten European security as a whole and are cross-border in nature, pointing towards a collective European security approach as the most effective response. Security is an interest shared by all European citizens, not only by EU citizens. Any dialogue between the EU and the UK on their future relationship on security should start from this point, taking as their guiding principle what is best for achieving this end, and not treating it as part of the wider Brexit negotiations.

### ***The will to overcome obstacles***

EU and UK leaders have indicated willingness to cooperate on security after Brexit. There is no doubt about the importance of the UK's current – and potential ongoing – contribution to European security, as a permanent member of the United Nations Security Council and of the G7, and as player with significant intelligence, diplomatic, and military resource.

In September 2017, the UK published two future partnership papers covering [internal](#) and [external](#) aspects of security.<sup>[2]</sup> Both urged the closest possible continuing partnership between the UK and the EU after Brexit. Theresa May's speech to the 2018 Munich Security Conference set out a vision on this basis.<sup>[3]</sup>

In January 2018, the European Commission published background documents on Brexit, which together comprise its starting point for negotiations on security, defence, and foreign policy, and on police and judicial cooperation.<sup>[4]</sup> The negotiating guidelines released in March 2018 expressed its aim of finding ways to work closely together in these areas. <sup>[5]</sup>

However, there are some political and institutional obstacles. On the UK side there are the domestic political divisions caused by Brexit. On the side of the EU27, the 'rules are rules' approach exemplified by Michel Barnier's November 2017 [Berlin speech](#), and reiterated in the European Commission's March guidelines, risks poisoning future relations with the UK, which sees the Brexit process as a negotiation.<sup>[6]</sup> Meanwhile, there is also a certain risk of complacency among the EU27 following the launch of Permanent Structured Cooperation (PESCO), that this represents a sufficient level of progress, and because NATO membership provides a certain safety net. Any temptation – on either side – to use bilateral and minilateral cooperation in addition to serious EU-UK engagement must be assessed in the context of the impact on overall European security arrangements. Perhaps most importantly, the Brexit negotiations have seriously eroded mutual confidence, and the situation may yet deteriorate. Many EU members resent the UK's obstructive, or at least reluctant, approach to Common Security and Defence Policy (CSDP) of recent years. This is especially given the UK's sense that its role in international security is so indisputable

that it does not need to convince its EU partners that the security and defence relationship it wants is not just about broader economic access to markets and resources, but also about contributing to the EU's activities and actions. On the other hand, support from other EU member states following the Russian nerve agent attack in Salisbury, UK, will be critical in shaping the UK's confidence that its EU partners continue to take its security concerns seriously. In the meantime, while the outcome of the deal on the future EU-UK economic relationship remains unclear, there are major unknowns about the nature of future cooperation which impact on the security relationship.

The stark fact is that the UK cannot participate in the EU's security decision-making processes if it is no longer an EU member state: its presence would mean that the body concerned was no longer an EU body. There would also be limits on its ability to shape decisions since the political dialogue that previously existed with EU states would no longer be there. There will inevitably be less ongoing contact between the EU27 and UK diplomats and officials once the UK stops attending European Council meetings. Long-standing British reluctance and new EU legal issues could further complicate this. For example, while the UK's reputation for cooperation on internal security is generally positive, its restrictive approach towards data-sharing on counter-terrorism through EU mechanisms has attracted criticism from other member states in recent years. In fact, the UK has earned a reputation as a 'free-rider' for using common databases extensively but contributing to them relatively little. As this sort of accusation has gained currency over the last year, it is noticeable that the UK has made determined efforts to improve its data-sharing record.

Despite the UK's half-hearted engagement in the recent past, on the political aspects of European external security, including coordination of diplomatic initiatives and sanctions, spaces for cooperation are not hard to envisage. They could be found on specific dossiers or even be based on more a structured and regular basis.

Strong economic interests are at stake in the European security and defence industry, and the future EU-UK economic relationship may have strong implications for the

launch of common projects. The leading role played by the UK industrial base is not in doubt, but British support to pan-European research and development projects has been inconsistent, especially within the European Defence Agency (EDA). A handful of third countries (including Norway and Switzerland) have administrative arrangements with the EDA which enable them to participate in its projects. But they can only do so if the member states initiating a given project wish to invite them. Third parties have no access to the discussions in which new projects are conceived, prioritised, and shaped. With the establishment of the European Defence Fund (EDF) and the activation of PESCO, these issues will only grow in importance, with the risk of distancing the UK from what is happening in this domain.

The will may well currently exist on either side to conclude a new agreement. However, much depends on the dynamics around the Brexit discussions as they progress.

### ***The logic of cooperation***

The way the EU tackles its security issues is changing. The EU Global Strategy offered a common vision, and member states have already taken some steps forward on this, especially in defence (PESCO, the EDF, the Coordinated Annual Review on Defence – CARD). Much remains to be seen, while EU cooperation on foreign policy, counterterrorism, and intelligence-sharing could be far closer. In this context the UK may be able to provide external added value to the EU's effectiveness on security, and equally the EU to the UK too. Compromises will, of course, be necessary. But the essential logic that both parties should follow should be to agree common actions in pursuit of common goals.

Some caveats exist. The UK's involvement should not undermine EU consensus-building. This means that UK participation in EU security and defence activities ought to be based on a special arrangement or an 'enhanced third country status' that facilitates UK-EU cooperation, but does not include involvement in decision-making. The unique status of the UK as a former member should be the justification for this special partnership, to avoid setting any precedent for other third countries. This

should be considered as a mutual guarantee of independence, because, although the convergence of UK-EU interests in security matters is clear, there could be cases in which a common EU response may contrast with the UK's interests, and vice versa. However, the UK cannot be seriously involved in any cooperation without assigning to it some rights of participation in the EU bodies. The UK will need to earn this right of participation, through active contribution to collective European initiatives, to dispel any fears about the possibility of it free-riding within this cooperation.

Even if both the EU and the UK accept that they need each other in the security area and find creative ways of pursuing that cooperation, there is still a substantial risk that this may fail to materialise because of political considerations. There could be a mixture of unintended consequences, spillovers, and path dependencies – as well as external pressures, including from the US – which could push the EU and UK further away from the logic of cooperation and towards that of divorce.

Whether the former or the latter prevails depends on both sides. The EU has to decide which institutional path it wants to follow to strengthen its security cooperation. Differentiated integration justified by a security-driven approach might be the best way to involve the UK. Such an approach would also enable the EU to show that it is stepping up its game, through budgetary means as well as political will. Alternatively, an integration approach that favours the widening of the security policies within the EU framework at the expense of the deepening offered by more differentiation, may lead to some results, but would probably lose the UK along the way. On the UK side, the British government has to make up its mind about what exactly it expects from its post-Brexit relationship with the EU. It will need to decide if it can resist the temptation to, say, subordinate the wider negotiations with the EU to its domestic political dynamics, or to pursue other political preferences which might include bilateral alliances, and NATO and transatlantic alignment.

## **Principles**

### *A security-driven approach*

The EU should embrace a security-driven approach right from the start. This should encourage the UK to follow the logic of cooperation, rather than that of divorce. Though enhancing European security is the guiding aim, this should not be to the cost of EU integrity. The cooperation arrangements that emerge should be primarily based on UK engagement with EU structures, rather than building new ones.

The security-driven approach should focus on four issues that would define the nature of the relationship:

- the UK and EU legal constraints in launching the cooperation arrangements;
- the UK presence and role in EU bodies;
- the economic conditions and benefits originating from the cooperation arrangements;
- the establishment channels and instruments to back a constant and fruitful political dialogue at all levels.

Each side should take account of these issues when discussing future security cooperation, although ultimately the forms of cooperation and their level of intimacy will vary depending on the legal and political constraints in each domain.

### ***A special partnership***

Both parties should accept from the very start that there will have to be a special relationship, with no ready precedent at hand for a European security actor comparable to the UK. The EU has other agreements with significant security partners – for example, the EU-Canada Strategic Partnership Agreement concluded in 2016. But, as it becomes the first former member of the EU, but retains its status as a P5 and G7 country, the UK's relationship with the EU in this area is unique.

The UK brings significant weight to diplomatic initiatives in the interests of European security: one notable example is its role with France and Germany in spearheading the Iran nuclear deal. Its military capability is also important in guaranteeing European efforts in regions of strategic interest – for example, its contribution of a

reserve for EUFOR Althea in Bosnia and Herzegovina, a mission of which the UK is a long-standing supporter. The UK is, today, an integral part of the European defence technological and industrial base (EDTIB) which the EU is now seeking to further strengthen. An EU negotiating stance that led to amputation of the UK from these arrangements would be perverse. Apart from that, uncomfortable though this is, full strategic autonomy will never be attained as long as Europe relies on others for the ultimate defence backstop of nuclear deterrence. The Brexit defence settlement needs, at the least, to keep open the possibility that the UK's nuclear weapons could one day, with those of France, underpin Europe's strategic autonomy. And finally, there is the unique nature and scale of the UK's cooperation with EU partners on internal security.

These factors make the UK a unique 'third party', to which the EU could sensibly make a unique offer, although upgraded access in these arrangements will depend on continued demonstration of good faith on the UK side, and would be open only to European countries. One can imagine a partnership in the field of foreign and security policy (both internal and external) in which the UK and the EU collaborate as closely as possible, with the EU inviting the UK to participate in work in this area as it deems useful.

At the same time, bilateral relationships between the UK and some EU member states can complement and reinforce this structure, as long as they do not undermine cooperation and consensus-building at the EU level. Such relationships could even be an alternative way to pursue cooperation with the UK if and when the EU political and legal framework becomes an obstacle to such close cooperation with third countries.

### ***Institutionalised cooperation***

The EU must choose between having a 'plug and play' approach of tactical cooperation between the EU and the UK, and agreeing an institutionalised way for the UK to take part in EU discussions. The latter would be more fit for purpose. This is first and foremost because a clear and formal space for these discussions taking place would disincentivise side channels and ad hoc bilateral cooperation. If too large a

proportion of these discussions with an important security partner like the UK takes place outside the formal EU structures, it would run the risk over time of diminishing the apparent value of discussion in EU structures, and instil a habit of crucial discussions happening elsewhere. This risk of the UK's departure exacerbating a tendency towards operating through informal groups – for example, the Quint (the United States, France, Germany, Italy, and the UK)– is something that concerns medium-sized EU states in particular. They see this as a reason for finding ways to include the UK through formal structures. Secondly, major EU policy initiatives such as the Iran nuclear deal and the sanctions on Russia after its invasion of Ukraine emerged out of sustained dialogue between EU partners, which should take place within these informal structures.

## **Key security dimensions**

Because the EU's external security mainly relies on the intergovernmental area of CSDP and the Common Foreign and Security Policy (CFSP), it will be easier to realise external participation of UK as a non-EU member. However, each side should consider special arrangements in conceiving a stronger special strategic partnership between London and Brussels.

### ***Foreign policy***

Diplomacy is one of the EU's key security tools. With the establishment of the European External Action Service (EEAS) under the direction of the high representative, the EU has given more substance and coherence to the CFSP. In the coming years, UK representatives and staff will leave the European Council and its dedicated foreign affairs bodies (the Foreign Affairs Council, the Political and Security Committee, the working group, and so on). But nothing prevents the EU Council from inviting the UK to find new working methods with its bodies where it deems it useful. On specific tools such as sanctions, or files such as nuclear non-proliferation and

disarmament, the search for a common effort with the UK is essential. Policy coordination on these and other dossiers could take place through regular meetings between UK, EU, and member state representatives to prepare positions in EU delegations in international organisations or in third countries, making use of existing formats. Although the UK has been reluctant in the past to share its diplomatic reports within the EU, new forms of collaboration may open up, as may the opportunity of having British officials temporarily seconded to the EEAS. The highly intergovernmental nature of the CFSP should be conducive to this cooperation.

### *Sanctions*

The EU increasingly uses sanctions to address a number of different challenges – from human rights violations to proliferation crises – as well as to influence a broad array of actors – from states, including major powers such as Russia and China, to informal entities and individuals like migrant traffickers.

Even if the impact of sanctions remains hotly debated, they have clearly contributed to some of the EU's most significant recent successes, such as in Iran. And they add to the EU's toolbox, harnessing its economic and technological leverage to send political signals, obstruct threatening actions, and bring about behaviour change. As such, they have become a security policy of choice for the EU, which currently enforces over 30 sanctions regimes.

Although some European states have developed national sanctions regimes, not all have done so, and in any case the clout and impact of the EU's autonomous sanctions is without comparison. While preparing for its own national sanctions policy post-Brexit, the UK has been working based on this analysis, and intends to “import” EU sanctions in its political and legal order as a first step. But this will only be a beginning.

The fact is that the UK has played a key role in EU sanctions policy. It has not only demonstrated diplomatic leadership on adopting sanctions, it has provided the technical expertise to review and adjust these restrictive measures, and shared intelligence to refine targeting and give them a sound legal basis. The UK often claims

to be responsible for at least 50 percent of current EU restrictive measures.<sup>[7]</sup> Whatever the exact proportion, it is a fact that it has currently no peer in terms of capacity.

This is a result of both the resources that the British government dedicates to this (as illustrated by the size of the staff working on sanctions in Whitehall) and the political involvement (from the number of British sanctions experts within the EU institutions to the political leadership it gives in Brussels on those issues). <sup>[8]</sup> This political clout is important; the political balance on sanctions within the EU may change after Brexit, given some other member states' more reluctant views on sanctions. Irrespective of the need for EU institutions to continue growing their expertise on these issues, and in a context where member states still play a key role (taking the initiative, gathering and sharing intelligence, implementation), there will be a need for some key member states to 'own' the issue as the UK has in the recent period.

The fact that the UK currently seems intent on maintaining its sanctions posture close to and consistent with that of the EU is important. Such close cooperation will require arrangements to cover: diplomatic coordination (especially at the PSC and Relex committee, but also in multilateral bodies such as the United Nations Security Council or the G7), sanctions design, intelligence-sharing, implementation and enforcement cooperation, as well as consistent postures against third parties (whether Russia's counter-measures or US sanctions' extra-territorial impact). It should be noted that British interlocutors interviewed in Paris particularly insist on their need for legally robust sanctions policy to be able to continue to coordinate closely with EU decisions.

To make the most of this cooperation, both EU institutions and member states need to start at home and step up their own game. Both the EU and the most interested capitals – which at this stage would be Paris, but also Berlin, The Hague, as well as Stockholm and Brussels – will need to increase resources and expertise to take over the current British leadership. Interviews in Paris indicate that the UK is currently considering seconding significant numbers of sanctions experts and is keen to

nurture close consultations and exchange of information with some bilateral partners. But in any case, the EU and its 27 remaining member states should seek their own autonomous expertise on these strategic issues. This will not make close and intense cooperation with the UK less useful, but the EU will still need such expertise in order to be able to deploy sanctions in a strategic and effective way.

### ***Defence***

All EU partners recognise the quality of both the civilian and, even more importantly, military capabilities that the UK can deploy in crisis management operations and welcome the UK's focus on stabilisation. Nevertheless, the UK's obstructive behaviour on CSDP over a number of years still rankles. Though the British may have good capacities and focus they have also usually been absent in the most recent CSDP missions and operations. In the early days of the Bosnian conflict in the 1990s, the UK was on the ground, but for the last decade its contributions to CSDP operations have been no more than marginal, except for providing the operational headquarters for the Atalanta anti-piracy mission. So in their September 2017 future partnership paper, the British account of their long-standing commitment to CSDP prompted general incredulity in Europe.

Cooperation in minilateral European initiatives – like Emmanuel Macron's European Intervention Initiative – and also within the framework of NATO, as well as increasing use of joint deployments in ad hoc coalitions, may also be helpful to keeping the UK close. They could create an indirect channel of cooperation with the EU through its member states. But bilateral relations, minilateral cooperation, and ad hoc coalitions would not exhaust all the opportunities under which the UK and EU member states could cooperate on crisis management, both under civilian or even military missions. The UK-EU relationship will also depend on Britain walking the walk on its willingness to contribute to CSDP.

### ***Development***

A third area where the UK has invested considerably in a broader definition of

European security is in development and humanitarian aid. Although with its departure from the EU, one aspect of formal coordination in this area – through the EU budget – will fall away, both sides are interested in continuing to cooperate on aid, given the strong alignment of EU and UK interests in many theatres, including their shared volatile neighbourhood, and the expectation that the UK will sustain its significant financial contributions to European aid levels. In addition, the UK may have quicker decision-making processes at a national level for aid expenditure than the EU budget mechanisms, meaning its potential to be a ‘first mover’ in crisis situations would be an added advantage for the EU in cooperating with it. To some extent this need for coordination might be met by UK diplomats being invited to participate in some aid coordination discussions at the EU, UN, World Bank, and other relevant multilateral forums. The EU should develop specific mechanisms for both strategic longer-term coordination and actual cooperation in specific countries and regions, especially in crisis situations.

### ***Justice and home affairs***

The scale and complexity of security threats within Europe, notably terrorism and cyber security, has increased substantially in recent years, and they have become more transnational and globalised in nature.

A more effective response to such threats depends on greater levels of information-sharing and integration of security efforts among all member states. Over the last five years this principle as applied to the area of internal security has driven increasingly closer levels of cooperation in the EU. Major developments in this arena include: a common EU policy cycle to combat organised crime; a new European Agenda for Security launched by the European Commission; ongoing efforts to align the interoperability of EU security databases; and various new initiatives at Europol, including the establishment of the European Cybercrime Centre and European Counter Terrorism Centre.

In the wake of recent terrorist attacks in EU states, government leaders have repeatedly called for greater levels of security integration and coordination to make

Europe safer in the face of more dangerous threats, but this ambition has yet to yield a step-change in levels of cooperation

The UK has made a significant and leading contribution to the effort to achieve this, in terms of strategic and thought leadership and the practical implementation of new initiatives. It is currently, for example, the top provider, among all member states, of intelligence contributions to many discrete projects on cybercrime and organised crime.

This strategic context is an important part of the framing of the debate concerning future EU-UK security cooperation after Brexit. A sudden, unplanned, or underprepared dislocation of the UK from these current integrated efforts by the EU in this field will bring significant risks to the security of the UK and the EU as a whole.

More specifically, the UK's Munich speech proposal for 'business as usual' on internal security – continued close cooperation on issues ranging from counter-terrorism to immigration police to fight against organised crime – faces legal and political obstacles. Continued UK access to key databases such as the Schengen Information System II and the European Criminal Records Information System will likely require an EU determination of the 'adequacy' of the UK's arrangements for data protection and privacy. The UK's recent assumption of new state powers such as bulk data retention under the Investigatory Powers Act (the "Snoopers' Charter") could make this difficult. And the EU will expect the European Court of Justice (ECJ) to have continuing oversight, a point that May acknowledged in her Munich Security Conference speech.

There are precedents of third party access to some EU databases. But precedents may not help, because the EU's approval has frequently required third parties to sign the Schengen agreement, which is not a requirement that the UK would be willing to meet. For example, Norway and Iceland have a suspect surrender agreement with the EU – but this falls short of the European Arrest Warrant (EAW) by including exceptions for "political" offences and surrender of their own citizens. Some member states had to change their constitutions to allow own-citizen surrender to fellow EU

members under the EAW. And though both the US and Denmark have operational agreements with Europol, neither permits the direct database access the UK will want.

All in all, the main challenges and obstacles on internal security include an absence of legal precedents for EAW (and other similar cooperation schemes), as well as a recognition that notable differences apply between the access rights of member states and those of other partners. Of course, the scale of the UK's current contribution to common EU efforts means that the EU can hardly afford to lose most of the benefits that this creates. In the end, therefore, the general principle of securing a collective security interest is a very powerful one.

The non-EU Schengen states already call for direct access to Europol databases for third parties at the political level. The resource burden on Europol of acting as an information gateway is also increasing and may stretch beyond reasonable levels once the UK becomes a third party. So this may be one of the areas where a practical compromise is required.

On these issues the UK has recently offered some clarification of its position, including formally proposing a treaty between the UK and the EU. In her Munich speech, May stressed the importance of UK-EU cooperation to ensuring security within Europe, citing the EAW, collaboration through Europol, and the Schengen Information System II as common achievements to which the UK has contributed. At the same time, she said, such an agreement should fulfil three requirements:

- “it must be respectful of the sovereignty of both the UK and the EU’s legal orders”. The UK seems ready to accept the jurisdiction of the ECJ when participating in EU agencies, but has asked for a “strong and appropriate form of independent dispute resolution”;
- it should be based on a specific EU-UK arrangement on data protection;
- and it has to be flexible in order to adapt the future relationship to changing threats.

The UK has made the first move by asking for a comprehensive treaty. Now it is the

turn of the EU. On these issues, cooperation is clearly desirable and probably achievable, but each side must tackle several operational and legal aspects that could affect or delay the conclusion of such an agreement.

## *Cyber*

Cyber security is one of the key areas where European security depends on the best possible cooperation arrangements between EU and non-EU partners, given its global nature and the dominant role the US currently plays. This is also the case in terms of the closest alignment of internal and external security, given the increasing convergence of state and non-state actors in certain high-profile cybersecurity incidents. The EU and UK will need to find ways of working together on the following cyber matters in the coming years.

The Networks and Information Systems (NIS) directive entered into force on 8 August 2016.<sup>[9]</sup> As the first comprehensive piece of EU legislation on cybersecurity, the directive is designed to improve cyber security capabilities at the national level, increase EU cooperation, and establish risk management and incident-reporting obligations for operators of essential services and digital service providers.<sup>[10]</sup> According to the European Commission, all member states, including the UK, “will have 21 months to transpose the Directive into their national laws and six months more to identify operators of essential services.”<sup>[11]</sup> This effectively pushes the application deadline back to the end of 2018. The UK and the EU can both only benefit from each side applying the NIS directive, as it aims to build a common European cybersecurity standard. This standard introduces mandatory incident reporting requirements, guarantees an appropriate level of cyber security capabilities, and establishes a network of competent authorities to exchange information for incident response and early warning purposes. Not transposing the directive in the context of Brexit would set a negative precedent which could spill over into other areas of security cooperation in the cyber domain.

Following the British exit the UK government will also need to sign an EU-UK Privacy Shield agreement, similar to the recently negotiated EU-US Privacy Shield, to ensure

“an adequate level of protection [...] surrounding a data transfer operation or set of data transfer operations” from the EU to the UK. The UK’s Information Commissioner’s Office shared this assessment in a statement, noting that “if the UK wants to trade with the Single Market on equal terms we would have to prove ‘adequacy’—in other words UK data protection standards would have to be equivalent to the EU’s General Data Protection Regulation framework starting in 2018.”<sup>[12]</sup>

The UK’s quest for adequacy will not come easily. There are at least three factors that will complicate matters for it. First, the pending ECJ case brought by Labour Party deputy leader Tom Watson and Conservative member of parliament David Davis (who withdrew his name from the case after being appointed secretary of state for exiting the EU) against the UK government’s Data Retention and Investigatory Powers Act 2014 (DRIPA). Second, the UK’s Investigatory Powers Act (IPA) which May introduced as home secretary following the English High Court’s disapplication of DRIPA in 2016. And third, a possible wave of legal challenges to any post-Brexit UK adequacy assessment, given the public’s knowledge of multiple GCHQ programmes that have spied or are still spying on EU data transfers, as revealed by former National Security Agency contractor Edward Snowden.

The ECJ fired a shot across the British government’s bow in July 2016 when the advocate general published his non-binding legal opinion.<sup>[13]</sup> While he noted that DRIPA “may be regarded as consistent with EU law”, the advocate general also stipulated that multiple requirements need to be satisfied in order to justify any interference with the EU Charter of Fundamental Human Rights or the EU’s directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58). In particular the advocate general was not convinced that “retaining data in combating ‘ordinary’ (as opposed to ‘serious’) offences” could be justified as an objective of general interest to the EU. Additionally, he noted that in his opinion all safeguards, as laid out in the Digital Rights Ireland case, are indeed mandatory (including an independent authority to oversee compliance with the requirements of privacy protection and security).

With the ECJ following the advocate general's opinion and handing down its judgement in December 2016, the Home Office began a government consultation which closed in January 2018.<sup>[14]</sup> Time will tell whether the impact on IPA and the UK's adequacy assessment will force the UK government to take a stand. Either the British government decides to push through IPA regardless of the ECJ's ruling, or it reforms IPA in a bid for a smooth adequacy assessment. Max Schrems, who infamously brought down the Safe Harbour agreement, which allowed the transfer of EU citizens' data to the US, has already voiced his interest in the UK after Brexit, arguing that one would simply have to search for a case in which EU data could possibly fall under some UK surveillance law and then say: "you're not allowed to transfer my data to the UK any more because I can't be sure that my data is not spied on."<sup>[15]</sup>

Indeed, the UK government would be well advised to avoid such a scenario at all costs. If a watered-down IPA is the price to pay for maintaining trade, then so be it. Even the US chose to accommodate European concerns regarding NSA surveillance programmes and practices by implementing: Presidential Policy Directive 28 (PPD-28), which sets out a number of principles and limitations for the collection of signal intelligence; the Judicial Redress Act (HR1428), which "allow[s] foreign citizens in European countries to sue the United States for unlawful disclosure of personal information obtained in connection with international law enforcement efforts"; and the USA Freedom Act (HR 2048), which "limits bulk collection of data and allows companies to issue transparency reports on the approximate number of government access requests."<sup>[16]</sup>

Brexit might create future confrontation in the area of coordinated vulnerability disclosure, especially when the UK or EU embark on developing vulnerability equities processes. Finding a healthy balance between national security needs and the public interest is not an easy task for governments anywhere. One aspect of this dilemma is vulnerability disclosure, which forces government agencies to choose between searching for vulnerabilities and developing zero-day exploits in an effort to

penetrate target systems, and leaving private sector companies open to security flaws that hostile actors might exploit. In this respect, governments have two choices: to either retain the knowledge of the vulnerability, or disclose it to the vendor so that it can be patched. While in the US, discussion of vulnerability disclosure has been in the spotlight for more than a decade, in Europe, this conversation has not gained much traction.

If the British government, EU member states, or both, decide to embark on developing vulnerability equities processes during or after Brexit, this might create incentives to not disclose vulnerabilities in systems that are overwhelmingly used on the other side. It would be wise to find a cooperative approach that will prevent any such ‘adversarial’ view taking hold.

If measured by the number of Certified Information Systems Security Professional (CISSP) certificates, a must-have document for information security professionals, the UK has the best cybersecurity workforce in Europe. The UK is the tearaway leader among EU member states, boasting 5,559 CISSPs compared to the EU27 combined total of 8,664. If, in the context of Brexit, the principle of free movement of workers is undone, the British exit might end up being more detrimental to the EU rather than the other way around (unless hundreds of UK security professionals apply for EU citizenship).

Finally, coordinated attribution is an area where there is a strong interest for both the EU and the UK in continuing to work closely together after Brexit. In reaction to the NotPetya malware campaign of June 2017, the Five Eyes countries coordinated their public attribution assessments for the first time in the cyber domain. As a result, the following year the UK issued a statement on 15 February warning Russia of “international consequences”, followed by the US and Canada a few hours later.<sup>[17]</sup> Australia and New Zealand joined on 16 February.<sup>[18]</sup> Meanwhile, several European nations cautiously joined the chorus (the Estonian foreign ministry, the Lithuanian foreign ministry, and the Danish ministry of defence all issued statements). Other EU member states, most notably Germany and France, were absent from the NotPetya

attribution discussion – this, despite current talks about the EU cyber diplomacy toolbox which is specifically designed as a framework for a joint EU diplomatic response to malicious cyber activities. With the UK spearheading coordinated attribution in the NotPetya case within the Five Eyes, and the EU absent from any coordinated attribution efforts, it is currently questionable whether the UK’s policies on attribution can be harmonised with the EU cyber diplomacy toolbox. With the UK out of the EU, it is critical to build a cooperative linkage between the Five Eyes and the EU when it comes to coordinated attribution assessments.

### ***European security and defence industry***

The importance of the European security and defence industry goes beyond the research and development of military technologies at the service of European security needs. It involves many economic interests, spillover into civilian industries (ie. dual-use technology), and the attempt to win strategic and technological autonomy from other countries, namely the US (see the framework agreement between France, Germany, and Italy to develop a European drone).[19] For instance, under a wider understanding of the ‘security industry’, it also refers to the instrumental role played by private parties in combating terrorism, cybercrime, and organised crime. Examples include cooperation with social media platforms to remove online terrorist content, the role that internet security partners play in fighting cyber crime, and the close role that banks currently play in improving efforts to combat money-laundering. From a European perspective major banks with a headquarters in London, such as HSBC, are very important.

With regard to the defence industry, EU member states and their private companies have shown an ambivalent attitude towards transnational cooperation and the establishment of a single European defence market. National, private, political, and economic interests have frequently merged, slowing EU integration in this sector. Recent decades have seen some results, but much more could be done.

The UK and its national champions have shared this ambivalence with other big EU countries and companies, but they feature among the major and most advanced

players.

As with other high-tech manufacturing industries, Brexit risks introducing damaging new frictions into supply chains, research cooperation, market integration, and the movement of both human and financial capital in the defence industries.

And significant interdependencies exist between the UK and continental partners. For example, it would not be cheap or easy for continental partners to replicate BAE Systems' expertise in carbon fibre aerospace wing work (a major issue for Airbus, of course, on the civilian side). Similarly, the technology developed from the UK's Storm Shadow deep-strike missile remains one of the crown jewels of MBDA, the pan-European missile house. (At their Sandhurst summit in early 2018, May and Macron singled out missiles for even deeper cooperation under the 2010 Lancaster House treaties.) But things may be about to change. Over the past couple of years a raft of new initiatives has begun, designed to revitalise the European defence 'project' on the industrial side. Given the history of false dawns in this area, a degree of scepticism is justified; and British membership or otherwise of PESCO may be unimportant, given that PESCO is turning out to be the EDA minus Malta. But two factors are significant.

First is the new mood of confidence among the 27, which feel rather pleased with the progress they have made precisely since the UK voted for Brexit. Member states that used to feel that 'there can be no European defence without the Brits' may now no longer see it as axiomatic that the UK must be cut a special deal. (And even though replacing British know-how in particular technologies would, as noted above, not be cheap or easy, there are some who would love to try.)

The second factor is the prospect of significant sums of money now becoming available for new collaborative projects from the EU budget, in the shape of the European Commission's new European Defence Fund, which launched on the back of the European Global Strategy whose focus was 'strategic autonomy'. This concept is variously interpreted by analysts as hedging against the evaporation of US defence guarantees, and/or the need for the EDTIB to be as comprehensive and free of external dependencies as possible. The weakening transatlantic security guarantee

does not fall to the European Commission to deal with; the latter is the basis upon which the European Commission justifies this new departure into defence funding.

And so, the EDF money – which will also support PESCO projects – comes with a pronounced new flavour of ‘European preference’. Thus, while under Horizon 2020 countries like Israel and Switzerland could buy their way into this pan-European research programme as effectively full members, the defence research programme that the European Commission hopes to subsidise at half a billion euros a year will be specifically for the benefit of entities on EU territory. Similarly, the even larger sums – a billion a year – proposed for new military capability development projects are framed as a “European Defence Industrial Development Programme, aimed at supporting the competitiveness and innovation capacity of the Union’s defence industry”.[\[20\]](#)

But what is the EU’s defence industry? Does it, for example, include European subsidiaries of US companies? What about MBDA, in which BAE Systems holds a major stake? The EU will codify the rules in the regulation under negotiation this year for the pilot scheme due to start next year. In December, the European Council agreed its version; the European Parliament will come up with its own in the spring; the final version, negotiated between the institutions, should emerge this summer.

The European Council version looks pretty restrictive. The beneficiaries of the EDF are to be “undertakings established in the Union”. Infrastructure, facilities, assets, and resources employed are to be located on EU territory; their “executive management structures” are to be established inside the EU. They must not be “subject to control by third countries or third country entities”. But it provides for derogations and exceptions – for example, eligible beneficiaries may cooperate with outsiders “if this would not contravene the security and defence interests of the Union and its Member States”, though the share of the action taken by those outsiders will be ineligible for funding.[\[21\]](#)

There are a lot of imponderables here. How will this language evolve in the months ahead? US industry is putting in a major lobbying effort with the European Parliament

against European preference in the new EDF, and US ambassador to NATO, Kay Bailey Hutchison, issued a strong attack on it in her speech to the Munich Security Conference this year. Will the EDF really be funded at the ambitious levels proposed? And will it be fully taken up? There is much grumbling in industry about the various constraints involved, such as ensuring SMEs can compete for contracts, and the subsidy is, in any case, capped at 20 percent for any one project. Can the British count on being allowed into EDF projects – assuming they bring their own money and/or technology to the party – on the basis of exceptions or derogations? Or would that be a recipe for being gradually frozen out if the long-term vision of a ‘strategically autonomous’ Fortress Europe becomes a reality? Can the UK get itself a permanent exception or derogation on the grounds of indispensability? Or can it at least have prior arrangements grandfathered in? But if the British are cut some slack, how to resist US pressure for the same?

At the moment the UK is an important part of the EDTIB. If a combination of Brexit and the advent of the EDF exclude it, both parties will suffer.

## **Conclusion: A new security framework**

This paper outlines just how much is at stake in getting future security cooperation between the EU and the UK right. A continued commitment is needed from not only the UK, but from all European states, to serious investment in and engagement on their security, keeping in mind not only the 2 percent of GDP target for defence spending, but also the 0.7 percent target for overseas development aid. The following recommendations for a future framework would underpin European security.

- The UK has proposed a treaty on internal security and law enforcement. This proposal should go ahead. Such a treaty is necessary to maintain not only the deep links between the UK and the EU on issues from cyber, to police cooperation, to the intelligence underpinning sanctions, but also to maintain the speed of communication in these fields. This new pact should envisage ongoing political cooperation in relevant areas of internal security, rather than simply

naming and enabling specific current aspects, because the picture will not remain static.

- However, this treaty will take time to conclude, and the dynamics in the EU-UK relationship over the coming months may not be conducive to developing the deep, trust-based arrangements needed. A transitional arrangement would be best: as foreseen for the single market, current provisions would stay in place and apply from the date at which the UK leaves the EU, allowing the uninterrupted continuation of the EAW, data exchange, and seconding of UK staff to Europol.
- For external tools in foreign policy, defence, crisis management and aid, ad hoc arrangements will be more appropriate, and should operate on the basis that EU states will seek UK involvement where they deem it useful. At a more detailed level these creative solutions might include regular coordination meetings between UK and Council preparatory groups such as COPS/COREPER and with the EDA; coordination meetings with EU ambassadors and the UK at the UN, on Security Council matters and other issues; and specific coordination meetings on sanctions and development aid.
- The UK should demonstrate from the outset its intent to contribute actively in these forums, and also in non-EU settings, such as the European Intervention Initiative. All channels of European security cooperation, at bilateral and multilateral level, should remain very much open, to complement efforts within the EU structures.
- The Letter of Intent group is a forum which provides for ongoing collaboration between the UK and other EU member states on joint defence industrial projects from the point of conception, and ongoing engagement in this format would be of interest to all parties. [22] If the UK demonstrates goodwill in this setting, it is possible to envisage access to the EDF in the future.

## Biographies

## Reflection group

**Marta Dassù** is senior director of European affairs at the Aspen Institute and editor-in-chief of Aspen Institute Italia's journal, *Aspenia*. She was Italy's deputy minister of foreign affairs from November 2011 to February 2014. She is a member of the board of directors of Leonardo and Fondazione Eni Enrico Mattei and she is vice-president of the Center for American Studies in Rome. She is also a member of the Advisory Council of the European Policy Centre in Brussels and a member of the scientific committee of the LUISS School of Government in Rome. She is a columnist for the Italian newspaper *La Stampa* and is the author of various books and essays.

**Ambassador Wolfgang Ischinger** has been chairman of the Munich Security Conference (MSC) since 2008. A German career diplomat, he was state secretary (deputy foreign minister) from 1998 to 2001. From 2001 to 2006, he was the Federal Republic of Germany's ambassador to the United States, and from 2006 to 2008, to the Court of St James (the United Kingdom). He is a senior professor at the Hertie School of Governance, Berlin, and serves on the boards of numerous non-profit institutions, including SIPRI in Stockholm, SWP in Berlin, AICGS in Washington, DC, and the American Academy in Berlin.

**Pierre Vimont** was the first executive secretary-general of the European External Action Service (EEAS), from December 2010 to March 2015. During his 38-year diplomatic career with the French foreign service, he served as ambassador to the United States from 2007 to 2010, ambassador to the European Union from 1999 to 2002, and chief of staff to three former French foreign ministers.

**Robert Cooper** is a European diplomat. He was director general in the EU Council Secretariat under Javier Solana, and counsellor to Baroness Ashton during her time as EU high representative for CFSP.

## Editor

**Susi Dennison** is a senior policy fellow at ECFR and director of the European Power programme, which focuses on the strategy, politics, and governance of European foreign policy, at this challenging moment for the international liberal order. She previously led ECFR's European Foreign Policy Scorecard project for five years, and worked with ECFR's MENA programme on north Africa. Before joining ECFR in 2010, Susi worked for Amnesty International, in their European Union office. Susi began her career in HM Treasury in the United Kingdom.

## Contributing authors

**Manuel Lafont Rapnouil** is the head of the Paris office and a senior policy fellow at the European Council on Foreign Relations, where he also leads the New European Security Initiative. A French career diplomat, he has worked extensively on international peace and security issues, especially within the UN context. Between 2008 and 2010, he was a visiting fellow with the Center for Strategic and International Studies.

**Mark Leonard** is co-founder and director of the European Council on Foreign Relations, the first pan-European think tank. He writes a syndicated column on global affairs for Reuters.com and is Chairman of the World Economic Forum's Global Agenda Council on Goeconomics. Previously he worked as director of foreign policy at the Centre for European Reform and as director of the Foreign Policy Centre. Mark has spent time in Washington, DC as a transatlantic fellow at the German Marshall Fund of the United States, and in Beijing as a visiting scholar at the Chinese Academy for Social Sciences.

**Stefan Soesanto** is the cybersecurity and defence fellow at the European Council on Foreign Relations. Since joining in mid-2016 the team has, among other items,

designed and held a cyber wargame exercise in cooperation with Microsoft EMEA, and organised a closed cybersecurity and defence conference in Odense, together with the Center for War Studies at the University of Southern Denmark and the Office of the Danish Tech Ambassador.

**Lorenzo Vai** is a researcher at the Istituto Affari Internazionali (IAI) in Rome and an adjunct lecturer at the University of Turin. He holds an MA in EU International Relations and Diplomacy from the College of Europe in Bruges, an MA in International Relations from LUISS Guido Carli, and a BA in International Studies from the University of Turin. His research interests revolve around EU institutions and foreign policy. Currently Lorenzo is pan-European fellow at the European Council on Foreign Relations.

**Nick Witney** is a senior policy fellow with the European Council on Foreign Relations. He joined ECFR after serving as the first chief executive of the European Defence Agency (EDA). His earlier career was spent in British Government service, as a diplomat (in the Arab world and Washington, DC) and later with the Ministry of Defence.

**Pawel Zerka** is programme coordinator in ECFR, based in the Paris office. He coordinates the European Power programme and ECFR's New European Security Initiative. Pawel holds a PhD in economics and MA in international relations. His main areas of expertise include EU affairs, Latin American politics, international trade, and Poland's European and foreign policy.

[1] Contributing authors to this publication are: Manuel Lafont Rapnouil, Mark Leonard, Stefan Soesanto, Lorenzo Vai, Nick Witney, and Pawel Zerka

[2] "Security, Law Enforcement and Criminal Justice: a future partnership paper", 18 September 2017, DEXEU and Home Office, available at <https://www.gov.uk/government/publications/security-law-enforcement-and->

criminal-justice-a-future-partnership-paper; and ‘Foreign Policy, Defence and Development: a future partnership paper’, 12 September 2017, DEXEU, available at <https://www.gov.uk/government/publications/foreign-policy-defence-and-development-a-future-partnership-paper>.

[3] [PM Speech at Munich Security Conference](#), Prime Minister’s Office, 10 Downing Street, 17 February 2018, available at <https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018>.

[4] [Negotiating documents on Article 50 Negotiations with the United Kingdom](#), European Commission, March 2018, available at [https://ec.europa.eu/commission/brexit-negotiations/negotiating-documents-article-50-negotiations-united-kingdom\\_en?utm\\_source=POLITICO.EU&utm\\_campaign=76653d1b14-EMAIL\\_CAMPAIGN\\_2018\\_02\\_23&utm\\_medium=email&utm\\_term=0\\_10959edeb5-76653d1b14-189129745&field\\_core\\_tags\\_tid\\_i18n=351&page=1](https://ec.europa.eu/commission/brexit-negotiations/negotiating-documents-article-50-negotiations-united-kingdom_en?utm_source=POLITICO.EU&utm_campaign=76653d1b14-EMAIL_CAMPAIGN_2018_02_23&utm_medium=email&utm_term=0_10959edeb5-76653d1b14-189129745&field_core_tags_tid_i18n=351&page=1).

[5] [European Council \(Article 50\) 23 March 2018 Draft Guidelines](#), 7 March 2018, available at <https://www.scribd.com/document/373207329/European-Council-Art-50-23-March-2018-Draft-guidelines>.

[6] [Speech by Michel Barnier at Berlin Security Conference, European Commission, 29 November 2017](#), available at [http://europa.eu/rapid/press-release\\_SPEECH-17-5021\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-17-5021_en.htm).

[7] Boris Johnson, “Uniting for a Great Brexit”, [Foreign & Commonwealth Office and Department for Exiting the European Union](#), 14 February 2018, available at <https://www.gov.uk/government/speeches/foreign-secretary-speech-uniting-for-a-great-brexit>. This figure was confirmed in interviews

by both UK and non-UK officials.

[8] The UK, which already had a bigger staff than its EU partners on sanctions policy, has recently further grown its sanctions team to almost 100 personnel, in the FCO and HM Treasury in particular. Even before that, it already had a significantly bigger and more professionalised (eg. on legal or intelligence issues) staff than its EU partners, including France, the other major country involved in sanctions policy both at EU and UN levels

[9] “Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity”, European Commission, 6 July 2016, available at [http://europa.eu/rapid/press-release\\_STATEMENT-16-2424\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm).

[10] “Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity”, European Commission, 6 July 2016, available at [http://europa.eu/rapid/press-release\\_STATEMENT-16-2424\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm).

[11] “The Directive on security of network and information systems (NIS Directive)”, European Commission, 16 March 2015, available at <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive>.

[12] Glyn Moody, “Brexit: Trade deals will force UK to follow EU data privacy laws anyway”, ArsTechnica, 24 June 2016, available at <https://arstechnica.com/tech-policy/2016/06/brexit-trade-deals-will-force-uk-to-follow-eu-data-privacy-laws-anyway/>.

[13] “Opinion of advocate general Saugmandsgaard ØE”, European Court of Justice, 19

July 2016, available at

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclan>

[14] “JUDGMENT OF THE COURT (Grand Chamber)”, European Court of Justice, 21 December 2016, available at

<http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN>;

“Investigatory Powers Act 2016”, Home Office, 30 November 2017, available at

<https://www.gov.uk/government/consultations/investigatory-powers-act-2016>

[15] Jennifer Baker, “Watch out, Theresa May! Max Schrems is coming for your planned spy law”, 13 July 2016, available at [https://arstechnica.com/tech-](https://arstechnica.com/tech-policy/2016/07/max-schrems-theresa-may-privacy-brexit-investigatory-powers/)

[policy/2016/07/max-schrems-theresa-may-privacy-brexit-investigatory-powers/](https://arstechnica.com/tech-policy/2016/07/max-schrems-theresa-may-privacy-brexit-investigatory-powers/).

[16] Presidential Policy Directive 28 (PPD-28):

<https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>; Judicial Redress Act (HR1428):

<https://www.govtrack.us/congress/bills/114/hr1428/summary>; US Freedom Act (HR2048): <https://www.congress.gov/bill/114th-congress/house-bill/2048>

[17] “UK and US blame Russia for ‘malicious’ NotPetya cyber-attack”, BBC News, 15 February 2018, available at <http://www.bbc.com/news/uk-politics-43062113>;

Canada: Greta Bossenmaier, “CSE Statement on the NotPetya Malware”,

Communications Security Establishment, 15 February 2018, available at

<https://www.cse-cst.gc.ca/en/media/2018-02-15>.

[18] Australia: Angus Taylor, “Australian Government attribution of the ‘NotPetya’ cyber incident to Russia”, Government of Australia, 16 February 2018, available at

<http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx>; “New

Zealand joins international condemnation of NotPetya cyber-attack”, New Zealand:

Government Communications Security Bureau, 16 February 2018, available at

<https://www.gcsb.govt.nz/news/new-zealand-joins-international-condemnation-of-notpetya-cyber-attack/>.

[19] Mary-Ann Russon, “France, Germany, and Italy to develop European Surveillance Drone by 2025”, IB Times, 18 May 2015, available at <https://www.ibtimes.co.uk/france-italy-germany-develop-european-surveillance-drone-by-2025-1501880>.

[20] “European Defence Fund and EU Defence Industrial Development Programme”, European Commission, available at [https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-294\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-294_en).

[21] “European Defence Fund and EU Defence Industrial Development Programme”, European Commission, available at [https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-294\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-294_en).

[22] “Letter of Intent: restructuring the European defence industry”, Ministry of Defence, 12 December 2012, available at <https://www.gov.uk/guidance/letter-of-intent-restructuring-the-european-defence-industry>

---

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU’s member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with

ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Emma Bonino and Mabel van Oranje.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.
- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and “friends of ECFR” gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions.  
[www.ecfr.eu](http://www.ecfr.eu)

The European Council on Foreign Relations does not take collective positions. This paper, like all publications of the European Council on Foreign Relations, represents only the views of its authors. Copyright of this publication is held by the European Council on Foreign Relations. You may not copy, reproduce, republish or circulate in any way the content from this publication except for your own personal and non-commercial use. Any other use requires the prior written permission of the European Council on Foreign Relations. © ECFR Mar 2018 ISBN: 978-1-911544-48-7. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London London W1W 5PA, United Kingdom