Independent Commission on UK - EU Relations

UK-EU CYBERSECURITY COOPERATION

in the context of the Trade and Cooperation Agreement: implementation, impact and proposals for renegotiation

ABOUT

INDEPENDENT COMMISSION ON UK-EU RELATIONS

The Independent Commission on UK-EU Relations is a timebound commission which examines the impact of the Trade and Cooperation Agreement (TCA) and Northern Ireland Protocol (NIP) on the UK.

As well as looking at impacts on different sectors of the economy we look more broadly at impacts on sectors including security and defence, health, education and human rights.

There are 13 members of the Commission from business, journalism, civil society and academia, along with a team of advisors. The intended outcome of the Commission is to recommend changes to the TCA and Protocol which, if implemented, would improve outcomes for UK sectors and the people who live and work in the UK.

There recommendations will be developed in collaboration with UK and EU politicians and relevant officials. We confer with parliamentarians from all parties as well as with regional and devolved and local politicians and party staff.

As well as informing parliamentarians and political parties the Independent Commission will inform the public of its work, both to highlight and explain challenges created by current arrangements and potential amendments.

For further information see **www.ukeucommission.org**

COMMISSION CO-CHAIRS

Mike Clancy: Co-Chair, Independent Commission on UK-EU Relations

Janice Hughes CBE: Co-Chair, Independent Commission on UK-EU Relations

CONTACTS

Mike Buckley: Director, Independent Commission on UK-EU Relations – mike@ukeucommission.org

AUTHOR

Helena Farrand Carrapico: Professor of International Relations and European Politics, Northumbria University – helena.farrand-carrapico@northumbria.ac.uk

The author would like to thank Dr Gemma Davies, Dr Nick Wright, Mr Mike Buckley, Dr Tim Stevens, Professor George Christou, and Professor Ben Farrand for their extremely helpful feedback on earlier drafts of this policy paper. She would also like to thank the interviewees that provided the evidence this policy paper is based on.

CONTENTS

SUMMARY

Although the UK-EU Trade and Cooperation Agreement (TCA) presents cybersecurity as a priority area in future UK-EU relations, the legal and political avenues are now narrower when compared to the pre-2020 relationship. The TCA has brought about a de facto decrease in information exchange, a limited participation of the UK in EU cybersecurity bodies, and a reduced capacity to influence the direction of the EU cybersecurity policy. UK practitioners are worried about what they perceive as lowered cybersecurity standards, more restricted data exchange, increased costs stemming from needing to cater for different jurisdictions, limited capacity to attract cybersecurity talent, and a consequent reduction in the UK's capacity to evaluate the cyber insecurity landscape. This policy paper identifies the main differences between the pre-TCA cybersecurity relationship and the current one, and puts forward recommendations to address the negative impact of the TCA implementation.

INTRODUCTION

Over the past three decades, cybersecurity has become one of the most crucial policy areas of the United Kingdom, ensuring the protection of citizens, companies and State institutions from cyber criminals and cyber attacks.

Given the ubiquitous presence of digital products, digital forms of working, and online services, as well as a growing societal reliance on technology, cyberspace plays a crucial role in the UK's economy and security. When compared to EU Member States, the UK has the largest internet-based economy as a percentage of GDP, and is at the forefront of global cybersecurity efforts (Carr and Tanczer, 2018). Not only has it consistently made large investments in the field (the first UK National Cybersecurity Strategy- 2011/ 2016 was underpinned by an investment of £860 million, the second - 2016/ 2021 by £1.9 billion, and the third - 2022-2030 by £2.6 billion), it also has the most dynamic cybersecurity market and industry of the EU27+UK (Stevens and O'Brien, 2019). In 2022, the UK Cybersecurity Sectoral Analysis estimates that the UK has 1,838 firms providing cybersecurity services and products, representing 9% of all UK employment, with an annual revenue of £10.1 billion, and an annual sectoral growth of 16% (Donaldson et al. 2022). Historically, the UK's early interest in cybersecurity, combined with its investment, market presence, and cybersecurity capabilities, enabled it to play a crucial role in the emergence and development of the EU's cybersecurity policy.

The TCA, however, has introduced important changes to the UK-EU relationship, reflecting the UK's position as a third country. If, on the one hand, the new partnership is characterised by a positive outlook on future cybersecurity relations, on the other hand, it brings about a reduction in data exchange, in the UK's participation in EU cybersecurity governance, and in its capacity to shape EU policy. UK cybersecurity practitioners have expressed their concern at the consequences of the implementation of the TCA in this policy area, namely in terms of more limited access to data, slower communication channels, and higher production costs.

This policy paper compares the current UK-EU cybersecurity relationship with the pre-2020 one, identifying areas where the implementation of the Trade and Cooperation Agreement is limiting UK cybersecurity, and therefore need to be re-negotiated.

UK-EU CYBERSECURITY COOPERATION

Concerns over an expanding panoply of malicious activity, including cyber crime, State and non-State sponsored cyber attacks on critical information infrastructures, fake news, and disinformation campaigns, have long served as a basis for the development of a comprehensive and coherent UK cybersecurity policy. Understood in a narrow sense, the latter includes the fight against cybercrime by law enforcement, the protection of critical information infrastructures, cyber defence and cyber diplomacy (Carrapico and Barrinha, 2017). In a wider sense, however, cybersecurity policy is one of the most cross-cutting and broader policy areas implemented by the UK, with its effects being felt in sectors as different as education, trade, and fisheries. At the heart of this policy lies the need to cooperate with other States and international/regional organisations by exchanging information, sharing best practices, and conducting joint operations in a space where national borders and national jurisdictions bear little resemblance to the physical world (UK National Cyber Strategy, 2022).

UK-EU cybersecurity relations pre-2020

Although cybersecurity continues to be characterized by national competence, the EU is rapidly becoming an international cybersecurity actor in its own right, supported by an expanding toolkit of strategies and legislation focusing on achieving cyber resilience and stability, through cyber capacity building and facilitating cooperation between Member States, institutions and the private sector (Carrapico and Farrand, 2020; Christou, 2016). This trend has reflected itself, for example, in the rapid expansion of the EU cybersecurity architecture, where dedicated agencies such as the EU Agency for Cybersecurity (ENISA), Europol's European Cybercrime Centre (EC3), the EU Agency for the Operational Management of Large-Scale IT Systems (eu-LISA), and the European Defence Agency (EDA), work together with other EU institutions and bodies, such as the Computer Emergency Response Team (CERT-EU) to support the work of Member States in the field of cybersecurity and the resilience of the EU more generally.

Traditionally, the UK has been perceived as a key actor in the development of the EU's cybersecurity policy, shaping new instruments and policy decisions, and ensuring the maintenance of a high level of coordination among EU member states, and with the private sector (Stevens, 2021). Examples of the UK's leadership in this area include the work it developed on attribution of large cyber attacks, creating contingency plans, and sanctioning those responsible; its assessment regarding dependence on non-EU technology and the resulting exposure to foreign interference; the shaping of legislation such as the EU Network and Information Systems Directive; the provision of staff and expertise on cybercrime to EU bodies; and its support of a Europe-wide network of cyber incident response teams (Templeton and Dewar, 2021; King, 2020; Christou, 2016).

Cybersecurity in the context of the current UK-EU relationship

Since 2016, discussions regarding UK-EU post-Brexit cybersecurity relations have remained largely limited to practitioners and think tanks. Law enforcement expressed its concern over future effectiveness in addressing cybercrime in a context of reduced cooperation with the EU (Kahn, 2019), and private companies discussed their future capacity to attract and recruit new experts, as well as a possible regulatory gap that might impact on their products and services (Curry, 2019). Other narratives have presented a more optimistic view of the future relationship emphasising that the UK and EU will continue to exchange cybersecurity-related intelligence. The UK will still be capable of shaping EU standards and incident responses, as other formal and informal channels will be used to cooperate in cybersecurity beyond the EU ones, including bilateral agreements with EU Member States, the Five Eyes framework, and NATO (Martin interview by Clarke, 2018).

A quick analysis of the Trade and Cooperation Agreement (TCA) would seem to support this more optimistic view. Cybersecurity occupies a place of particular relevance in the TCA. Included in Part IV - Thematic Cooperation - it is one of only two areas that were specifically selected for prioritisation (the other area being Health Security) due to its recognised topical relevance and transnational nature. The Agreement foresees four important cooperation elements:

1. the maintaining of a high-level dialogue,the exchange of best practices and of policy developments on a range of cybersecurity topics, including cybercrime, cyber defence, internet governance and emerging technologies;

2. close cooperation between the EU Computer Emergency Response Team (CERT-EU) and its UK counterpart – the National Cyber Security Centre - enabling the exchange of information on general threats and vulnerabilities, techniques, tactics, procedures, and best practices;

3. the opportunity to take part in the Cooperation Group aimed at facilitating strategic cooperation between Member States in relation to the security of network and information systems;

4. the possibility for the UK to take part in EU Agency for Cybersecurity (ENISA) activities in the field of capacity building, knowledge and information exchange and education (EU-UK Trade and Cooperation Agreement, 2021: Part IV).

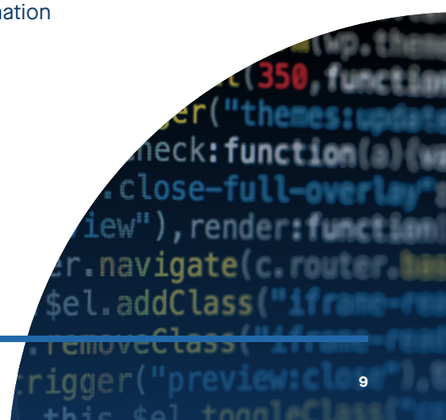
Despite this optimistic outlook, cybersecurity practitioners are nonetheless increasingly concerned about the implementation of the TCA in this area, which they perceive as leaving the UK exposed to greater cybersecurity threats. More specifically, according to a survey developed by CyberArk (a private company offering cybersecurity solutions), 97% of those surveyed are worried about lowering standards of cybersecurity, navigating the differences between UK and EU legislation in order to continue to access the Digital Single Market, being able to hire individuals with appropriate skills, and reduced collaboration with EU partners (Scroxton, 2022). A closer reading of the TCA reveals two crucial differences in relation to the pre-2020 relationship, which are resulting in a reduced level of influence and diminished operational coordination.

1. The first difference regards the reduction in information exchange.

a. As can be noted in Part IV, although the TCA refers to a number of cybersecurity exchanges, these are not related to specific threats or operational data, but rather to best practices, educational training, and general information.

b. Furthermore, the implementation of Part III of the TCA, on Police and Judicial Cooperation, also has important consequences for cybersecurity in the sense that it limits the UK's access to EU law enforcement data, which is crucial in addressing cybercrime (Hadfield et al., 2022). In particular, the loss of access to Schengen Information System II real time data constitutes a real challenge that cannot be easily compensated by alternative mechanisms or platforms, such as the Interpol 24/7 system, bilateral (Davies, 2020), UK-Member States agreements, or even the UK-EU Security of Information Agreement, which allows for the exchange if classified information but only on a case by case basis (SOIA, 2021).

c. In addition, even if the TCA foresees some level of cooperation through instruments such as the Prum Framework, Passenger Name Record, and a replacement for the European Arrest Warrant, it is very much dependent on future EU data adequacy decisions on the UK's handling of data, meaning that this limited access could be further curtailed (House of Lords, 2021). Any limitation in access to information reduces the UK's capacity to address cyber insecurity.



2. The second difference regards the UK's participation in agencies and bodies that support EU cybersecurity.

a. Although the UK maintains a presence in Europol and in the European Cybercrime Centre, namely through the secondment of liaison officers and continued joint operations within the Joint Cybercrime Task Force (J-CAT), it no longer has a say on the direction of the EU's law enforcement agency. Similarly, the UK no longer sits on the management board of ENISA, which supports and advances cybersecurity resilience and cooperation, nor does it take part in the Network and Information Society-established Cooperation Group, which provides strategic guidance to the EU in this policy field.

b. The absence of the UK at the decision-makers' table reduces its capacity to influence medium and long-term strategic decisions and to take part in the development of the EU's cybersecurity actorness. This absence is particularly visible given the recent developments and plans within EU cybersecurity policy, namely the 2020 EU Cybersecurity Strategy and the EU Cybersecurity Certification Framework, as well as a wide range of legislation currently under discussion, such as the Chips Act, the Cyber Resilience Act, the Digital Operational Resilience Act, and the Network and Information Society Directive 2.

c. These developments are indicative, not only of a very dynamic cybersecurity environment, but also of the EU's intention to introduce higher security requirements for producers, products, and supply chains, and greater reporting obligations in the event of cyber incidents. These are requirements that the UK industry needs to cater for, if it wishes to continue exporting digital products and services to the EU, which currently constitutes the main destination for 78% of all UK cybersecurity industry (Donaldson et al. 2022). In practice, these changes create substantial disruption for UK companies, which need to adapt to different jurisdictions with increasingly distinctive cybersecurity requirements (Walden and Michels, 2019).

d. Furthermore, there is the risk that this situation may worsen if the UK and the EU's regulation on cybersecurity further diverge from each other, in particular in light of the EU's declared objective to reinforce its digital sovereignty and reduce its level of dependence on non-EU countries and producers (Von der Leyen, 2019).

e. Ultimately, the reduced UK participation in EU cybersecurity agencies and bodies has consequences for the country's capacity to influence the direction of the EU cybersecurity policy, which, in turn, partially shapes the landscape UK industry operates in. This reduced influence has also been taking place in a wider context defined by political tensions between the UK and the EU, as well as by a strategic distancing between the two partners – the National Cyber Strategy 2022, for example, only refers to the EU once in its main text. Policy makers and practitioners have highlighted the reduced influence and the strategic distancing as contributing to a narrowing and bureaucratisation of communication with their counterparts in the EU, and to a need to identify new avenues to influence EU cybersecurity policy and practices.

CONCLUSION AND RECOMMENDATIONS

The present policy paper has highlighted the differences in the UK-EU relationship before and after the TCA's entry into force, as well as the consequences that the agreement is having on UK cybersecurity. In particular, it focused on the reduction in information exchange and in UK participation in EU cybersecurity governance, and reflected on the consequent concerns expressed by practitioners for their capacity to understand the cyber insecurity landscape and to maintain their position within the cybersecurity market. Bearing these concerns in mind, the paper recommends several avenues for improving cooperation. Some of these relate to the re-negotiation of parts of the TCA, whereas others fall outside of the remit of the agreement.

TCA-related recommendations:

1. Build on the cooperation introduced by Parts III and IV of the TCA by signing working arrangements with EU cybersecurity agencies and bodies (in particular ENISA, CERT-EU, EDA, and eu-LISA) that will expand operational cooperation, following the example of the Working and Administrative arrangement signed between Europol and the National Crime Agency in September 2021;

2. Continue to explore, in dialogue with the EU, alternative forms of access to Schengen Information System (SIS II) data;

3. Maintain convergence with EU data, privacy and cybersecurity standards to ensure positive EU data adequacy decisions and continued data exchange;

4. Finalise UK participation in EU science and research programmes (namely, Horizon Europe, Digital Europe, Connecting Europe Facility 2) so UK companies and research bodies can benefit from the cybersecurity funding and knowledge exchange;

5. Promote a closer oversight of the TCA implementation, namely by ensuring that the Specialised Committee on Law Enforcement and Judicial Cooperation meets at regular intervals to monitor the implementation of Part III of the TCA (meetings have so far been taking place on an annual basis only), and that a new specialized committee is created for cybersecurity;

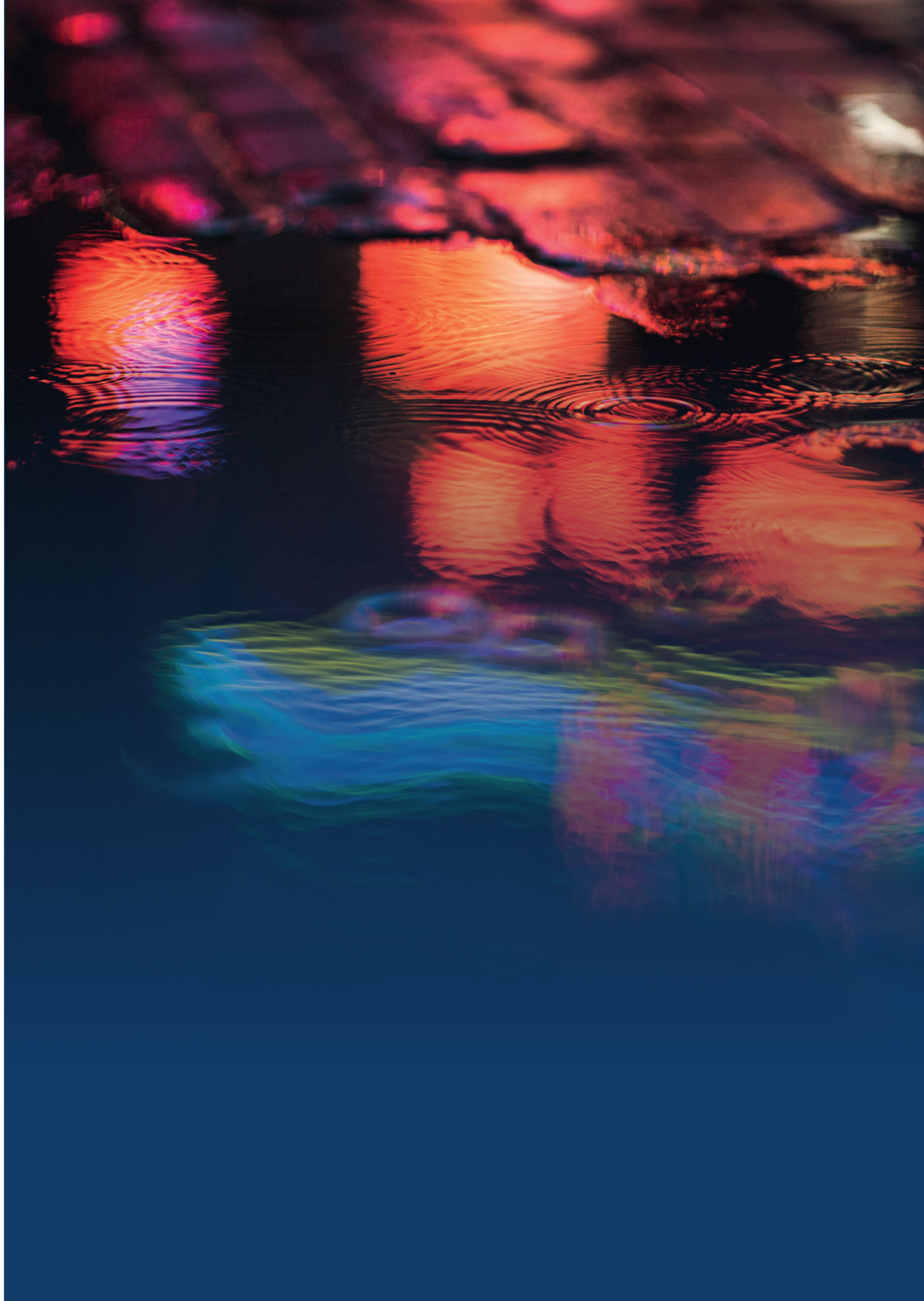
Non-TCA-related recommendations:

1. Expand the UK's insight into the impact of the TCA on the cybersecurity industry and its capacity to navigate the UK and EU jurisdictions through dedicated Parliamentary inquiries. Our current knowledge remains insufficient to properly ascertain the impact;

2. Encourage a broader scrutiny of EU documents in the context of the House of Commons' European Scrutiny Committee. Although the reforms introduced in October 2022 to scrutiny arrangements are very welcome, they risk not including documents impacting on UK cybersecurity as they might not be considered as having a direct effect on the UK under the Withdrawal Agreement and the TCA;

3. Promote a greater focus on the EU within UK cyber diplomacy and UK cybersecurity strategy, given the importance of continued security and economic links to the EU;

4. Identify non-EU platforms that would enable the UK to continue to influence the direction of EU cybersecurity policy, by leading by example on the adoption of cybersecurity standards. Such platforms could include ETSI, ITU, OECD, and the Council of Europe.



UK-EU CYBERSECURITY COOPERATION

in the context of the Trade and Cooperation Agreement - Implementation Impact and proposals for re-negotiation

UKEUCommission
uk-eu-commission
@UKEUCommission

ukeucommission.org

The Commission is run by UK EU Future Ltd, based at Aizlewoods Mill, Nursery Street, Sheffield S3 8GG

Company number **13742325**