GCSP
Geneva Centre for Security Policy

AUGUST 2021 | ISSUE 17

Strategic Security Analysis

The post-Brexit EU-UK Relationship: An Opportunity or Challenge for Cyber Security?

Ellie Templeton and Dr Robert S. Dewar

www.gcsp.ch

Key Points

- The United Kingdom (UK) officially exited the European Union (EU) on 31 January 2020, nearly four years after a polarising Brexit referendum. Following extended negotiations on future relations, two key agreements entered into force on 1 May 2021 containing sections on trade, cooperation, and security, with the latter including cyber security.
- These new agreements are a positive step towards a new cooperative model, but questions remain over what type of relationship the EU and UK will have in reality when it comes to cyber security.
- Three potential pathways for this future relationship are possible, with each pathway presenting both new opportunities and new challenges for cyber security. These pathways are as follows:
    - *a completely autonomous UK*, which would encourage home-grown national security advances, but would discount the view of cyber security as a collective concern;
    - *increased international dependence for the UK*, which would facilitate greater collaboration with the wider cyber community, but would not acknowledge the unique value of regional coordination; and
    - *the replication of the pre-Brexit EU-UK partnership through the establishment of new bilateral relations* that will preserve the security relationship, but demote Britain's former leadership status within EU agencies and initiatives to that of a third party.
- The most positive outcome would be a relationship in which both the EU and UK contribute to a professional, transparent and non-political cooperative model that would build on the recent agreements, while remaining open to flexible support in the future given the unpredictable and complex nature of cyber threats.
- If the relationship outcome proves operationally successful, it could be a potential model for non-EU-member entities also seeking cyber security cooperation with the EU.

About the Authors

Ellie Templeton is a Cyber Security Project and Research Officer working for the Cyber Security Cluster at the GCSP. Ellie has an International Master's Degree in Security, Intelligence and Strategic Studies from the University of Glasgow, Dublin City University and Charles (Prague) University, and an LLB from the University of Birmingham.

Dr Robert S. Dewar is the Head of Cyber Security at the GCSP, leading the Centre's cyber security activities and executive education courses. He engages in international dialogue activities and conducts research into cyber security and defence policy, security studies, active and blended learning, the EU, and historical institutionalism. He also specialises in designing, developing and staging policy-based cyber security simulations. He has a PhD in EU Cyber Security Policy, an MSc in Global Security from the University of Glasgow, and an MA (Hons) in Modern History from the University of St Andrews.

Introduction

The second anniversary of the UK's formal exit from the EU will occur on 31 January 2022. Since the 2016 referendum both parties have been sailing through "uncharted waters" in their negotiations to establish a constructive post-Brexit relationship in a range of sectors, including security and intelligence.[1] A significant step towards this was taken on 1 May 2021, when the newly negotiated EU-UK Trade and Cooperation Agreement and additional Security of Information Agreement came into force.[2] On the surface, these agreements signify the launch and successful implementation of a new bilateral EU-UK security relationship. However, when considering the relatively sparse content of these agreements and recent remarks at the operational level, it is clear that questions remain over what type of future cyber security relationship will emerge.

Due to recent increases in cybercrime during the COVID-19 pandemic, cyber security is widely recognised as a *collective* agenda that requires partnerships, cooperation and common norms.[3]

Due to recent increases in cybercrime during the COVID-19 pandemic, cyber security is widely recognised as a *collective* agenda that requires partnerships, cooperation and common norms.[3] The UK is a global cyber leader and the EU is an important regional hub for cyber security partnerships.[4] This Strategic Security Analysis (SSA) therefore asks: How will the EU-UK relationship develop in a future increasingly characterised by cyber security threats and risks?

There are three possible directions for this relationship. Firstly, a more digitally autonomous Britain could develop, one where the country "goes its own way" in terms of cyber security policy and operationalisation. Secondly, we could see the UK being increasingly dependent on, and have greater interaction with, other international allies and partners such as NATO. Finally, new bilateral relations with relevant EU agencies and states may emerge that could replicate pre-Brexit cyber security dynamics. Each type of relationship presents both opportunities and challenges for cyber security.

Following a brief introduction to the EU's cyber security position, the UK's involvement in that position as a former member state, and the operational changes experienced so far on the Brexit journey, this SSA will consider what opportunities and challenges each pathway may afford for cyber security, as well as if each pathway could establish a replicable framework for other non-EU-member entities seeking cyber security relations with the EU.

The EU and cyber security

According to the Lisbon Treaty, security is and will remain a "cornerstone" of state sovereignty.[5] This means that, theoretically, EU membership should make no difference to member state security considerations or policy. At the time of the Brexit referendum in 2016, Ciaran Martin, former chief executive officer of the UK's National Cyber Security Centre, stated that it was "objectively true" that the majority of Britain's cyber functions fell "outside the scope of EU competence".[6] Accordingly, some considered the prospect of Brexit impacting Britain's cyber security as being insignificant.[7] There are two reasons why this was not the case. Firstly, cyber threats are trans- and multinational due to the architecture of the internet and the world wide web. A cyber incident in one part of the world can easily affect digital assets in another region. Secondly, it is evident that as emerging cyber threats became increasingly placed at the forefront of national security concerns, this priority has also increasingly integrated itself more into core EU security policy and operations.[8]

As emerging cyber threats became increasingly placed at the forefront of national security concerns, this priority has also increasingly integrated itself more into core EU security policy and operations.[8]

For many years European member states have utilised EU mechanisms in the cyber security field by supporting the establishment of new information-sharing platforms, regulatory and legislative frameworks, operational initiatives, and cyber-specific institutions.[9] In particular, regulatory frameworks at the EU-level have been instrumental in ensuring that all member states endorse strong and unified cyber security practices. The most significant regulations have been the General Data Protection Regulation (GDPR) dealing with privacy and data protection; the EU Security of Networks and Information Systems (NIS) Directive focusing on cyber resilience across key systems; and the EU Cybersecurity Act, which aims at strengthening cyber-based EU agencies and establishing a cyber security certification framework for products and services.[10]

Five agencies demonstrate the EU's development as a cyber security partnership hub: the EU Agency for Network and Information Security (ENISA), the European Defence Agency (EDA), Europol's European Cybercrime Centre (EC3), the Computer Emergency Response Team (CERT-EU) for EU institutions, agencies and bodies, and the EU Agency for the Operational Management of Large-Scale IT Systems (eu-LISA). The increasing focus on cyber security was addressed in the EU's 2014 Cyber Defence Policy Framework, which called for greater "synergies with wider EU cyber policies, relevant EU institutions and agencies" and led to the first four institutions listed above signing a memorandum of understanding (MoU) in September 2017.[11] The MoU set out a cyber security cooperation framework that was considered to be "an important step" towards achieving *joint* cyber resilience.[12] This has continually been built upon, with further MoU's being adopted to enhance coordination between EU security agencies. Another agreement between ENISA and CERT-EU was signed on 15 February 2021[13] and a cooperative agreement was established between ENISA and eu-LISA on 8 January 2021 – all joining together in support of "a more digitally resilient Europe".[14]

At the operational level, several of these EU agencies have played crucial roles in ensuring British security, particularly Europol in the fight against organised crime. According to the UK's National Crime Agency, the country frequently used and benefitted from "widespread operational use of Europol's analytical and coordination services across all serious and organised crime threat areas".[15] The UK also played a leading role in Europol, with British director Sir Rob Wainwright holding his position from 2009 to 2018. There was a strong UK presence in a range of Europol activities, e.g. involvement in 170 operational meetings in 2019,

66 of which were led by British representatives.[16] While few statistics are available that can quantify member states' engagement with EU agencies, based on the EC3 being part of Europol and from remarks at the operational level, the UK also appears to have both actively benefitted from and contributed to the EC3's forensics, strategy and operations.[17]

This is also the case for ENISA. The UK was considered to be a "strong lead in Europe on tackling cybercrime", providing expertise and staff to support policy, cooperation and capacity-building activities.[18] Regarding other EU agencies such as CERT-EU (staffed by IT security experts helping member states respond to information security and cyber incidents), eu-LISA (responsible for the operational management of IT systems and information exchange platforms) and the EDA (focusing on EU defence initiatives), there has been consistent reference to their contribution to both national and regional security in Britain.[19]

Brexit was expected to reduce "operational effectiveness", require a reallocation of resources, and add further uncertainty to a range of security and policing areas.[23]

As an EU member state, the UK was also compliant with EU-level regulatory frameworks and supported EU strategy. The EU's GDPR and NIS Directive was transposed into UK law in 2018, becoming known as the Data Protection Act and NIS Regulations and acting as foundational frameworks for national data privacy and cyber security practices. The EU's Cybersecurity Act that came into effect in June 2019 and is due for full implementation across the EU from June 2021 has had a limited impact on UK certification frameworks. However, UK legislation was considered to be a core architectural base for the Act's initial development.[20] With Sir Julian King also being the European Commissioner for the Security Union in the period 2016-2019, the UK was closely involved in the EU's security agenda and strategy development.[21] Based on these contributions, resources and leadership, there was pre-Brexit optimism that a relationship pathway would be found to ensure the continuation of these constructive EU-UK exchanges and influences in the security sector.[22]

What has changed for UK cyber security since Brexit?

The UK formally left the EU on 31 January 2020. While this would not have irreversibly damaged either British or EU-level cyber security (as a national competence), it was expected to reduce "operational effectiveness", require a reallocation of resources, and add further uncertainty to a range of security and policing areas.[23] Between January 2020 and May 2021 both sides likely felt these effects, with no formal cooperative arrangements in place. Instead, various negotiations went ahead between relevant EU and UK representatives and bodies, which involved numerous setbacks, unsuccessful proposals and renegotiation talks before any final agreements were made.[24]

A significant step towards the new relationship was made with the resulting Trade and Cooperation Agreement and complementing Security of Information Agreement, which both entered into force on 1 May 2021. The new agreements set out how the EU and UK can securely exchange classified information going forward, providing initial insight into their future relationship on paper.[25] The Trade and Cooperation Agreement includes a section on "Law Enforcement and Judicial Cooperation", which essentially confirms that the UK will continue to work with the EU in combatting crime by retaining access to important critical information databases and exchange platforms.[26] Crucially, the agreement establishes a working relationship with Europol (including the EC3) and Eurojust,

the EU's law enforcement agencies, for information sharing and joint investigations, operations and prosecutions.[27]

In the final Trade and Cooperation Agreement there is also a small section under "Thematic Cooperation" on *cyber* security. The content is brief, stating that "the parties shall *endeavour* to establish a regular dialogue in order to exchange information" and "where in their *mutual* interest, the parties shall cooperate in the field of cyber issues".[28] Regarding EU agencies, the agreement explicitly refers to cooperation with CERT-EU and ENISA, with information exchange being on a "voluntary, timely and reciprocal basis".[29] It confirms that the UK may participate in a limited number of ENISA activities, including capacity building, information sharing, awareness raising and education, but this is "subject to prior approval" and there must be an appropriate financial contribution.[30] The agreements are a step closer to a new cyber security relationship, but provide few details on operational logistics, with day-to-day arrangements still subject to discussions between the EU agencies and relevant UK national bodies.[31]

The agreements are a step closer to a new cyber security relationship, but provide few details on operational logistics.[31]

At the time of writing, the UK has continued to enforce EU cyber security regulations, with national compliance with specific standards also being a condition for post-Brexit involvement in some key EU agencies. Notably, the UK must comply with the GDPR and the European Convention on Human Rights in order to work with the EU's law enforcement agencies (including Europol).[32] Despite the UK expressing interest in adapting its national cyber security frameworks post-Brexit, this is expected to be a longer-term move, one contingent on the extent to which EU regulations are currently embedded in national legislation and the uncertainty of what will happen regarding security, commerce and EU cooperation if standards begin to diverge.[33] As Sir Julian King stated, the agreements enforced on 1 May 2021 have "addressed only some of the serious question about future security cooperation … many challenges lie ahead".[34]

Brexit: opportunity or challenge?

Despite this uncertainty there are three possible relationship pathways for future EU-UK engagements. This section will consider the opportunities and challenges for cyber security of each pathway and whether they could constitute an effective and replicable partnership model for non-EU entities.

1. An autonomous Britain

a. An opportunity for UK national advancement

Despite cyber security remaining a national competence, following the 2016 referendum British security dialogue was quick to categorise the EU's growing contribution and leadership in the field as moving at "the speed of a tortoise", not a "fox".[35] With the most prevalent risk from a state perspective considered as "weak cyber security", the UK could have regarded Brexit as a welcome escape from weak networks and an opportunity to refocus resources and capacities on national cyber resilience.[36] Brexit was also seen as an opportunity to accelerate national initiatives, particularly those that had previously lacked EU support. For example, during its membership Britain sought to extend telecommunication standards in preparation for 5G expansion, with its preferred "evidence-based approach" going unsupported in EU discussions.[37]

With the signing of the new Security Agreement, it appears that another step has been taken to establish a more autonomous Britain. Instead of being part of the EU, the UK will now enter into a cooperative arrangement with the Union on its own national governance terms. This is not the same level of engagement the UK once had, with the new terms largely based on an "overarching mutual self-interest".[38] At the time of writing, the new agreements point to a voluntary and transactional arrangement between two autonomous parties rather than any form of trusting partnership. If this strategic model is retained, the autonomous capabilities that Britain has gained through Brexit can be seen as an opportunity that allows for both the national determination of cyber security practices *and* cooperative support when required by both sides. For any non-EU entity, self-interest will likely constitute a key feature for both itself and the EU in finding value in a prospective strategic relationship.

As global digitalisation accelerates into the fourth industrial revolution, nations, organisations, and entities are increasingly coming together in support of shared goals in the areas of cyber resilience and digital governance.

b. A challenge for collective cyber security

Increased autonomy may improve national standing, but it can also pose a challenge if cyber security is considered as a collective risk. Here, the EU cyber security agencies demonstrate their value and purpose with the aim of "joining forces" and "putting experiences and the knowledge of all" together.[39] Since 2016 the global cyber threat landscape has dramatically expanded and become more complex. The COVID-19 pandemic has generated a new era of digitalisation, which in turn has attracted an unprecedented level of cybercrime and online threats. Conditions like these, together with increasingly multifaceted and malicious cyber operations, have forced the world to reassess the boundless nature of cyber threats and the importance of digital security in everyday – not just geostrategic – activities.[40] As global digitalisation accelerates into the fourth industrial revolution, nations, organisations, and entities are increasingly coming together in support of shared goals in the areas of cyber resilience and digital governance. On the political surface, Brexit undermined this growing drive – and *necessity* – to collaborate.

Although an initial EU-UK security agreement has been reached with some reference to cyber security, the difficulties of the Brexit process have not helped a key aspect of cyber security cooperation in this digital age – that of *trust*. In the policy and political sphere, trust and trustworthiness are at a premium due to the high number of malicious cyber operations currently being observed, located in or associated with a range of nations.[41] As the directors of the four EU institutions emphasised when signing the 2017 MoU, *trust* and *shared responsibility* are vital to ensure cyber security.[42] In light of the current geopolitical trajectory, a foreseeable challenge for the UK is that trustworthiness will be a conditional factor for any non-EU entity to be invited to contribute to or benefit from the EU's *shared* agenda.

2. Increased international dependence

a. An opportunity to strengthen international partnerships

For some in the UK, Brexit was considered an opportunity to strengthen Britain's commitment to wider non-European security partnerships. Notable examples include bilateral relations with the United States (US) and membership involvement in NATO and intelligence platforms such as Five Eyes (Australia, Canada, New Zealand, UK and US), Nine Eyes[43] and the SIGINT Seniors Europe.[44] These relationships have been fundamental to the UK's security capabilities, with Five Eyes viewed as the UK's sector-

leading intelligence alliance securing national resilience to *global* threats.[45] The UK's active involvement in other international entities, such as the United Nations and the Organisation for Security and Cooperation in Europe and the fact that NATO enforces its own cyber security agenda, provides some explanation as to why the UK has so far been reluctant to establish a formal agreement with the EU in the area of foreign policy and international security.[46]

Instead, these wider security alliances could foreseeably act as the UK's key communication channels in its efforts to achieve foreign policy and security goals, with the cohort of allies also including EU member states. With the UK's cyber security strategy also having a heavy international dimension, the redistribution of commitment and resources to these broader organisations has been viewed as a way of better supporting national cyber strategy.[47] This opportunity, however, risks operationally and politically impacting on the new cooperative EU-UK relationship: without each party adding direct value, a strategic relationship based on "mutual interest" could be rendered useless. Any non-EU entity would need to consider which international partnerships can best stipulate opportunities for cyber security and, if the EU can contribute, whether the entity can also provide equivalent value to the Union. For the UK, if the nation can leverage its sharing of technical expertise or information to multiple platforms, it may be able to both strengthen its international partnerships *and* maintain a strategic relationship with the EU.

Without each party adding direct value, a strategic relationship based on "mutual interest" could be rendered useless.

b. A challenge to replicate the multidimensional membership

It is not a foregone conclusion that Brexit would *not* negatively impact the dynamics of the UK's international partnerships. An important element of Britain's value within these alliances was its bridging role between the US and EU. Without this role the UK risks becoming a "second-rate power", which would make it not inconceivable that international partners could turn to other leading countries as their more direct European intermediaries.[48] Moreover, with a new US political administration and NATO's focus on military strengths, the UK may face unexpected challenges without an involvement in the full range of EU cyber activities. A current example of this emerging challenge has been the UK's loss of access to information systems under the operational management of eu-LISA, including the main database for instant operational alerts on the movement of people and objects, i.e. the Schengen Information System 2, or SIS2.[49] Although a law enforcement issue, this loss of access has been considered the biggest "operational gap" affecting security.[50] As a mechanism that also contributes to the prevention and prosecution of cyber criminals, this has the potential to negatively impact cyber operations at both the UK and EU levels.

Additionally – and perhaps more significantly – Brexit did not only entail UK departure from *formal* cyber security structures, but also the *informal* networking that occurs within the wider "jigsaw puzzle" of the EU's multidimensional architecture.[51] These informal channels of communication can provide secure cross-European exchanges, which can be inherently valuable in time-critical sectors such as cyber security. Closer partnerships with international alliances could generate enhanced security opportunities and a new type of relationship with EU member states. However, it should not be assumed that these partnerships are capable of replicating the region-specific and internally secure dynamics currently operating within the EU. This would also be a challenge for any non-EU entity, particularly those who may be highly engaged in EU-level cyber activities but still fall short of Union membership.

3. Replicated European bilateral relations

a. An opportunity to replicate membership through bilateral relations

The recent agreements making explicit reference to engagements with Europol, ENISA and CERT-EU demonstrates the potential for a former EU member state to replicate some level of operational coordination with EU agencies through bilateral relations. The UK appears to be aiming for a similar standing to that of Iceland or Norway, countries that have set precedents for non-member state involvement in EU-level bodies.[52] With the new Security Agreement confirming that parties will only coordinate "on matters of common interest" and that the UK must be *invited* to take part in ENISA and CERT-EU activities, we are yet to see the operational level of engagement from both sides.[53] If both parties continue to employ similar strategies and can demonstrate value added through resources or intelligence, it is conceivable that Britain could be regularly invited to join EU-level initiatives in order to increase collective resilience.

In addition to EU agencies, EU member states are free to collaborate on bilateral and multilateral bases to enhance their national security. In these instances, cooperation is sought for a specific purpose – when a national lack of capacity or information exists. European bilateral partnerships can and do exist in the normal security discourse, as is evident in the UK's current engagements with national agencies in France and the Netherlands, and intelligence exchanges with Germany and Poland.[54] Depending on the state of cyber security capabilities in Europe, there may be opportunities to expand on these European bilateral partnerships in the immediate future. With the UK expressing direct interest in this model,[55] this pathway has the potential to be a beneficial and accessible model for any non-EU entity to externally replicate informal EU networking channels.

b. A challenge to find value in a "third-party" status

There are, however, legal, political and practical difficulties to establishing and maintaining these bilateral relations, which could foreseeably become a much "more fragile, ad hoc and less accountable" process.[56] Complications may arise if Britain, over time, decides to adopt new regulatory frameworks, such as revising privacy and data protection standards that could then conflict with the EU's GDPR. These legal divergences constitute one of the main obstacles for non-EU entities to join EU-level initiatives or build bilateral state partnerships with countries that firmly endorse pan-European standards.[57] Similar challenges will likely be faced in the UK's future engagements with the EU. As the UK Metropolitan Police commissioner stated, post-Brexit cooperation on crime prevention will be "clunkier, clumsier and more expensive".[58] The new Security Agreement itself states that "the Parties shall cooperate as far as *reasonably practicable*",[59] implying that once Britain (and possibly any non-EU entity) diverges from EU cyber standards, partnerships with EU agencies or member states could quickly be termed a non-practicable option going forward.

It is also important to consider that the UK's re-engagement with EU agencies is now on a *third-party* basis. The new "secondary position"[60] significantly changes Britain's former leadership position in EU security – an influencing role that it does not currently enjoy in the international US-led alliances. Having lost a platform to lead collective and regional cyber security practices, the UK may face substantial obstacles in finding value in a third-party status. In the future, what could be key to attaining a mutually valuable cooperative model for any third-party entity with the

What could be key to attaining a mutually valuable cooperative model for any third-party entity with the EU is *flexibility* – i.e. remaining open to flexible support in light of the unpredictable and complex nature of cyber threats.

EU is *flexibility* – i.e. remaining open to flexible support in light of the unpredictable and complex nature of cyber threats. The biggest challenge to this will be ensuring that both politics and conflicting legal frameworks do not prevent this strategic pathway from being termed "practical" when needed.

Conclusion

With multiple post-Brexit pathways that could still be pursued following the recent adoption of the new security agreements, the EU-UK cyber security relationship is still evolving. Value must be placed on collaboration to tackle shared cyber threats, the role EU institutions play in bringing cyber security actors together, and Britain's former contribution to European security. These factors strongly indicate that, although new opportunities may present themselves, there will likely be irreversible losses for collective cyber resilience due to Brexit. In order to work towards a new, valuable relationship model, it is recommended that both the EU and UK uphold professional, transparent and non-political security cooperation going forward, whilst remaining open to flexible operational support in the unpredictable and ever-changing cyber threat landscape. Ultimately, within an international system affected by "instability, insecurity and uncertainty",[61] it remains to be seen what opportunities and challenges arise, and if the resulting relationship, whether based on one specific pathway or a combination of all three, could constitute an effective EU relationship model for non-EU entities in the cyber security field.

Value must be placed on collaboration to tackle shared cyber threats, the role EU institutions play in bringing cyber security actors together, and Britain's former contribution to European security.

Endnotes

1. I. Konstantopoulos and J. Nomikos, "Brexit and Intelligence: Connecting the Dots", *Journal of Intelligence History*, Vol.16(2), 2017, p.100-107.
2. EU and UK, Trade and Cooperation Agreement, *Official Journal of the European Union*, L149/10, 30 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:149:FULL&from=NL>; EU and UK, Agreement Concerning Security Procedures for Exchanging and Protecting Classified Information, Official Journal of the European Union, L149/2540, 30 April 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22021A0430(02)&from=EN.
3. R. Dewar and E. Templeton, "#OnlyTogether Can We Enhance Our Resilience against Cybercrime", GCSP, 4 November 2020, https://www.gcsp.ch/global-insights/onlytogether-can-we-enhance-our-resilience-against-cybercrime.
4. J. King, "What's the Price of a UK/EU Security Agreement?", *UK in a Changing Europe*, 17 August 2020, https://ukandeu.ac.uk/what-price-a-uk-eu-security-agreement/.
5. I. Konstantopoulos and J. Nomikos, 2017, p.104.
6. W. Ashford, "UK Committed to Working with EU Cyber Security Partners", *Computer Weekly*, 21 February 2019, https://www.computerweekly.com/news/252458102/UK-committed-to-working-with-EU-cyber-security-partners.
7. N. Inkster, "Brexit, Intelligence and Terrorism", *Survival*, Vol.58(3), 2016, p.24.
8. Europol, "Four EU Cybersecurity Organisations Enhance Cooperation", Press Release, 23 May 2018, https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation.
9. C. Hillebrand, "With or Without You? The UK and Information and Intelligence Sharing in the EU", *Journal of Intelligence History*, Vol.16(2), 2017, p.96.
10. T. Stevens, "Brexit and Beyond: Cyber Security", King's College London, 5 February 2021, https://www.kcl.ac.uk/cyber-security-brexit-and-beyond.
11. Europol, 2018.
12. Ibid.
13. ENISA, "ENISA and CERT-EU Sign Agreement to Start Their Structured Cooperation", Press Release, 2 March 2021, https://www.enisa.europa.eu/news/enisa-news/enisa-and-cert-eu-sign-agreement-to-start-their-structured-cooperation.
14. ENISA, "ENISA and eu-LISA – Cooperation for a More Digitally Resilient Europe", News Item, 8 January 2021, https://www.enisa.europa.eu/news/enisa-news/enisa-and-eu-lisa-2013-cooperation-for-a-more-digitally-resilient-europe.
15. I. Hargreaves, "Cross-Border Criminal Cooperation in a Post-Brexit World", *Lexology*, 27 January 2021, https://www.lexology.com/library/detail.aspx?g=6a964051-a653-49af-ba9f-34f5c964df35.
16. Ibid.
17. TechMonitor, "Cryptocurrency Arrests Sees [sic] UK and Europol Haul in Six for the Theft of £21 Million", 1 July 2019, https://techmonitor.ai/techonology/cybersecurity/uk-europol-cryptocurrency-arrests.
18. J. King, "Cybersecurity after Brexit", *UK in a Changing Europe*, 6 November 2020, https://ukandeu.ac.uk/cybersecurity-after-brexit/.
19. HM Government, "EU Exit: Assessment of the Security Partnership", Cm 9743, November 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759760/28_November_EU_Exit_-_Assessment_of_the_security_partnership__2_.pdf.
20. T. Stevens, 2021.
21. R. Singh, "Julian King: Bold EU Action Is Required to Address Cyber Vulnerabilities", *The Parliament*, 21 November 2017, https://www.theparliamentmagazine.eu/news/article/julian-king-bold-eu-action-is-required-to-address-cyber-vulnerabilities.
22. C. Hillebrand, 2017, p.91.
23. T. Stevens, 2021.
24. European Council, "EU-UK Negotiations on the Future Relationship", 4 May 2021, https://www.consilium.europa.eu/en/policies/eu-uk-negotiations-on-the-future-relationship/.
25. European Commission, "The EU-UK Security of Information Agreement", 1 May 2021, https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement/eu-uk-security-information-agreement_en.
26. EU and UK, Trade and Cooperation Agreement, 2021.
27. J. King and J. Scarlett, "The Future of UK-EU Security Cooperation", RUSI, 18 January 2021, https://rusi.org/commentary/future-uk-eu-security-cooperation.
28. EU and UK, Trade and Cooperation Agreement, 2021; emphasis added.
29. Ibid.
30. Ibid.
31. J. King and J. Scarlett, 2021.
32. T. Stevens, 2021.
33. Ibid.
34. J. King and J. Scarlett, 2021.
35. As Dr Sajjan Gohel states in I. Konstantopoulos and J. Nomikos, 2017, p.104.
36. W. Ashford, 2019.
37. Ibid.
38. J. King and J. Scarlett, 2021.
39. Europol, 2018.
40. R. Dewar and E. Templeton, 2020.
41. R. Dewar and E. Templeton, "The Impact of Regulatory Frameworks on the Global Digital Communications Industry", Policy Brief, GCSP, October 2020, https://dam.gcsp.ch/files/doc/the-impact-of-regulatory-frameworks-on-the-global-digital-communications-industry.
42. Europol, 2018.
43. Five Eyes members plus Denmark, France, the Netherlands and Norway.
44. Nine Eyes members plus Belgium, Germany, Italy, Spain and Sweden.
45. C. Hillebrand, 2017, p.93-94.
46. Federal Foreign Office, "Brexit: The Trade and Cooperation Agreement Formally Entered into Force on 1 May – What Are the Future Foundations of Relations between the EU and the United Kingdom?", 1 May 2021, https://www.auswaertiges-amt.de/en/aussenpolitik/europa/brexit-where-are-we-now-what-next/2204138.
47. Ibid.
48. C. Walton, "Little Britain: Brexit and the UK-US Special Intelligence Relationship", *Prospect*, 10 August 2016, https://www.prospectmagazine.co.uk/world/little-britain-brexit-and-the-uk-us-special-intelligence-relationship.
49. J. King and J. Scarlett, 2021.

50. Ibid.

51. I. Konstantopoulos and J. Nomikos, 2017, p.100.

52. G. Segell, "Intelligence Cooperation between the UK and the EU: Will Brexit Make a Difference?", *Journal of Intelligence History*, Vol.16(2), 2017, p.85.

53. EU and UK, Agreement Concerning Security Procedures, 2021.

54. G. Segell, "Post-Brexit: British Intelligence and Security Cooperation with European Union States Including Greece", Research Institute for European and American Studies, 2 January 2017, http://www.rieas.gr/images/editorial/grukbrexit.pdf.

55. W. Ashford, 2019.

56. C. Hillebrand, 2017, p.91.

57. A. Glees, "What Brexit Means for British and European Intelligence Agencies", *Journal of Intelligence History,* Vol.16(2), 2017, p.73, 75.

58. T. Stevens, 2021.

59. EU and UK, Agreement Concerning Security Procedures, 2021; emphasis added.

60. A. Glees, 2017, p.75.

61. I. Konstantopoulos and J. Nomikos, 2017, p.102.

GCSP
Geneva Centre for Security Policy

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-303-8