BFPG British Foreign Policy Group

UK Plc and Supply Chain Cyber Security: Where in the World is my Data?

Professor Victoria Baines, Senior Research Fellow,
British Foreign Policy Group

April 2023

The British Foreign Policy Group

The British Foreign Policy Group (BFPG) is an independent, non-partisan think tank dedicated to advancing the UK's global influence, at a crucial time in the nation's modern history. Our core objective is to bridge the link between the domestic and international spheres – recognising that Britain's foreign policy choices are shaped by our social, economic and democratic landscape at home. BFPG works as the connective tissue between the UK's policy-makers, businesses, institutions, and ordinary citizens, to promote the connectivity and understanding needed to underpin Britain's national resilience and global leadership in the 21st Century.

The BFPG produces pioneering social research, which provides a holistic picture of the social trends shaping public attitudes on foreign policy and the UK's role in the world. Our annual public opinion survey has become the leading UK quantitative research project on foreign affairs and the UK's role in the world. Our National Engagement Programme provides a crucial bridge between HMG and citizens and stakeholders, in their own communities. In addition, the BFPG produces dynamic events and facilitates networks amongst stakeholders with a vested interest in Britain's international engagement – including co-convening the UK Soft Power Group with the British Council, which highlights the strengths and potential influence of the assets harboured within the UK's towns, cities and nations towards projecting our national cultural and diplomatic power.

The BFPG also monitors and interrogates the social, economic and political constraints of both our allies and adversaries, as a crucial resource of strategic foresight in a rapidly evolving global landscape. We believe that, harnessed with this knowledge, and with the full capabilities of our considerable assets, Britain will have the best chance to succeed in its ambitions to promote prosperity, peace, security and openness – both at home and abroad. Our mission supports Britain as a strong, engaged and influential global actor. We promote democratic values, liberal societies, and the power of multilateralism – and we recognise Britain's critical international responsibility to uphold and extend these throughout the world. The BFPG believes that a strong and united nation at home is the essential foundation of a confident and effective British foreign policy.

Executive Summary

As hardware and software supply chains become ever more complex, so too does the challenge of mapping and securing information assets. Audit of third-party suppliers and assurance of their security arrangements have become key cyber defence measures. At the same time, digital technology procurement is now a foreign policy issue which business cannot avoid. In order to remain trusted and competitive, British business needs to follow international best practice and to comply with internationally recognised cybersecurity standards. This is a challenge for the UK Government too, which must ensure that its efforts to certify the security of digital products are aligned with those of key trading partners and that the British voice is heard in key negotiations to improve supply chain security. A shared task for Government and business.

Staying Secure in a Constantly Changing Landscape

It has never been more important for businesses of all sizes and in all sectors to know where their data is and to assure themselves, their shareholders, their customers and their partners that their systems are secure. As a consequence of the General Data Protection Regulation (GDPR) in 2018, any organisation that processes and stores personal data is required to demonstrate that it has the requisite technical, human, and business process measures in place to minimise and mitigate risk, and to respond appropriately in the event of a breach. A crucial first step in achieving compliance for all businesses has been to locate and map all its data assets.

It is no coincidence that 'asset mapping' is also a key phase in cybersecurity practice. Cybersecurity and data protection are inextricably linked. A lapse in one can result in a breach of the other. Likewise, good practice in cybersecurity can strengthen data protection, and vice-versa. Just as one first has to know what data is held and where before one can identify vulnerabilities and deploy protective measures, so too cybersecurity specialists map and continuously monitor networks, systems and information assets for the same reasons.

In an era when businesses kept all their data and processing power on premises and retained full-time information security personnel, mapping those assets was a relatively straightforward, albeit time-consuming, task. A company's cybersecurity policies and controls could be implemented by its own employees. Audit and assurance was very much an in-house activity, with a realistic aspiration to uniformity.

The corporate landscape is now very different. The 'as a service' model dominates IT. Cloud processing and storage are now standard. The COVID-19 pandemic accelerated digital transformation that enabled a considerable expansion of remote working, often using personal devices in virtual workspaces designed primarily for personal (rather than business) use. For many organisations, data and tooling went 'off premise' for the very first time.

The Rise of Outsourced Cybersecurity 'as a Service'

A parallel trend for Cybersecurity as a Service can also be observed. Deloitte's regular Future of Cyber survey found in 2019 that 99 per cent of Chief Information Security Officers surveyed had outsourced some of their cybersecurity operations to third-party providers, including vulnerability management, threat hunting and intelligence, insider threat detection and incident response.[1] The virtual Security Operations Centre (SOC) is now a common presence. Prominent market offerings such as Identity and Access Management (IAM), Managed Detection and Response (MDR), and Security Information and Event Management (SIEM) imply third-party management and control.

When so much in the digital world is outsourced, asset mapping is necessarily more of a challenge. Following the same principle that one first has to know where something is in order to determine what should be done to protect it, very often businesses must look to audit and seek assurances about the security arrangements of third party suppliers. This is no small feat, particularly when teams routinely demonstrate a need for additional tools and when software suppliers are frequently subject to mergers and acquisitions. But it is essential, as high-profile case studies illustrate.

Supply Chain Security as a Foreign Policy Challenge

In 2017, the NotPetya virus spread through a backdoor in tax preparation software widely used by organisations with business in Ukraine. While at the time police suggested that the software developer would face criminal charges for neglect of its security duties, more crucially the impact was felt in organisations all over the world, from multinational law firm DLA Piper, shipping firm Maersk, logistics firm DHL, and advertising company WPP.[2]

As the NotPetya case illustrates, British companies doing business outside the UK may be exposed to cyber risks by virtue of their activities overseas and their statutory obligations in foreign jurisdictions. In jurisdictions such as China, whose Cybersecurity Law requires network operators to 'cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law' (Article 49), compliance with domestic obligations may itself constitute a security threat in the eyes of other governments. Accordingly, the United States Federal Bureau of Investigation has asserted that 'Beijing could likely use these authorities and policies to compel access to US commercial and sensitive personal data, including sensitive information stored or transmitted through Chinese systems'.[3]

[1] Deloitte. (2019). The Future of Cyber Survey 2019. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

[2] ABC News. (2017, July 3). Ukrainian software company will face charges over cyber attack, police suggest. https://www.abc.net.au/news/2017-07-03/cyber-attack-charge-ukarine/8675006

[3] Wallace, C, E. (2020, March 4). 'Dangerous Partners: Big Tech and Beijing' - Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, *Federal Bureau of Investigation*. https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing.

The reality of doing business internationally therefore entails navigating conflicts not only of jurisdiction but of competing security imperatives. Technology rivalry between the United States and China, with touchpoints in trade, national security, technology transfer sanctions and human rights, has transformed everyday IT procurement into a foreign policy issue. The UK government's issuing of legal notices for the removal of Huawei components from 5G networks by 2027, and the United States Federal Communications Commission's 2022 ban on approvals of new Huawei and ZTE telecoms components received considerable media attention, as have more recent bans on the use of TikTok on United States federal and EU institution staff devices.[4] Consequently, Chief Information Officers and Chief Information Security Officers are now asked by their boards whether company infrastructure contains any Russian or Chinese hardware or software.

Cybersecurity products are also under greater scrutiny than ever before. Russian provider Kaspersky's products have been banned on government devices in a number of EU countries and blacklisted by the United States Federal Communications Commission as a threat to national security, on the basis of the company's alleged ties to the Russian government.[5] A recent call by five EU Member States for a bloc-wide ban relates specifically to the company's reported continued provision of services to the Russian government following the invasion of Ukraine. The UK National Cyber Security Centre (NCSC) has so far stopped short of an outright ban, choosing instead to recommend that public sector organisations, providers of critical national infrastructure, and others 'reconsider their risk'.[6]

Cybersecurity providers are also not immune to supply chain attacks, as the 2020 compromise of SolarWinds' Orion software demonstrates. In addition to numerous United States federal, state and local government departments, cybersecurity vendors Mimecast, Palo Alto Networks, Qualys and Fidelis all confirmed that they had installed a trojanised version of the Orion app.[7] The cybersecurity firm which discovered the compromise, FireEye, did so while investigating the theft of its own 'red team' tools used to simulate attacks on enterprises.[8] In addition to proving that there is no such thing as absolute security, even for security specialists, the necessarily privileged access of cybersecurity tools to networks and systems present a different order of threat if compromised.

Businesses must also contend with sector-specific regulations. Among these, the much-heralded Digital Operational Resilience Act (Regulation (EU) 2022/2554), effective from January 2025, establishes an oversight framework for critical third-party ICT service providers to financial services institutions. The European Banking Authority (EBA), European Securities and Market Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA) are jointly designated Lead Overseer, with the power to recommend that financial entities refrain from subcontracting their ICT to a third-party provider established in a third country which provides a critical or important function, if it is assessed to be a clear and serious risk to the financial stability of the Union or to financial entities. Needless to say, British companies providing financial services in the EU are in scope. At the same time, British third-party ICT providers will be under greater scrutiny from EU supervisory authorities by virtue of the fact that they originate from outside the Union. They may as a result have to work harder to assure the EU that they can be trusted with its business.

[4] Department for Digital, Culture, Media and Sport. (2022, October 13). Huawei Legal Notices Issued. https://www.gov.uk/government/news/huawei-legal-notices-issued; Bartz, D., Alper, A., & Bartz, D. (2022, November 26). U.S. bans Huawei, ZTE equipment sales, citing national security risk. *Reuters*. https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/; Murphy, M. (2023, February 28). China hits out at US over TikTok ban on federal devices. BBC News. https://www.bbc.co.uk/news/world-asia-china-64795548; Chee, F. Y. (2023, February 28). European Parliament latest EU body to ban TikTok from staff phones. *Reuters*. https://www.reuters.com/technology/european-parliament-ban-tiktok-staff-phones-eu-official-says-2023-02-28/

[5] Federal Communications Commission. (2022, March 25). *FCC Expands List of Equipment and Services That Pose Security Threat*. https://www.fcc.gov/document/fcc-expands-list-equipment-and-services-pose-security-threat

[6] National Cyber Security Centre. (2022, March 28). *Use of Russian technology products and services following the invasion of Ukraine*. https://www.ncsc.gov.uk/blog-post/use-of-russian-technology-products-services-following-invasion-ukraine

[7] Cimpanu, C. (2021, January 26). Four security vendors disclose SolarWinds-related incidents. *ZDNet*. https://www.zdnet.com/article/four-security-vendors-disclose-solarwinds-related-incidents/

[8] Fireeye. (2020, December 8). Unauthorized Access of FireEye Red Team Tools. *Mandiant*. https://www.mandiant.com/resources/blog/unauthorized-access-of-fireeye-red-team-tools

What is Britain doing?

If it ever was, cybersecurity procurement is now no longer a matter simply of obtaining the best security with the budget available. How then are British businesses to navigate this uncertain and at times contradictory geostrategic landscape? Standards, guidance, and even regulation can help, provided that they do not put organisations under conflicting obligations. In this regard, the National Cyber Security Centre's (NCSC) *Supply Chain Security Guidance* is useful precisely because of its focus on principles rather than specifics.[9] Businesses are advised to:

1. Understand what needs to be protected and why
2. Know who their suppliers are and build an understanding of what their security looks like
3. Understand the security risk posed by their supply chain
4. Communicate their view of security needs to their suppliers
5. Set and communicate minimum security requirements for their suppliers
6. Build security considerations into their contracting processes and require that their suppliers do the same
7. Meet their own security responsibilities as a supplier and consumer
8. Raise awareness of security within their supply chain
9. Provide support for security incidents
10. Build assurance activities into their approach to managing their supply chain
11. Encourage the continuous improvement of security within their supply chain
12. Build trust with suppliers

Crucially, these principles frame effective supply chain security management not as a one-time compliance checklist but as a continuous exchange and iterative process. Granted that suppliers will often not be physically located in the UK, the need for security standards which are interoperable and internationally recognised is paramount. Against this backdrop, any UK regime should aim not only to be consistent and aligned with international standards. It should also actively resist the urge to be distinctive in material areas, however tempting it may be from a political perspective. While the fashionable, competitive rhetoric of 'world-leading' and 'world-beating' legislation belies the impracticality of imposing the UK's will on any global digital technology, it is positively disadvantageous to the aim of ensuring common standards of cybersecurity.[10]

[9] National Cyber Security Centre. (n.d.). *Assessing supply chain security*. https://www.ncsc.gov.uk/collection/supply-chain-security/assessing-supply-chain-security

[10] Landi, M. (2022, March 16). Updated Online Safety Bill will be "world-leading", Culture Secretary says. *Evening Standard*. https://www.standard.co.uk/news/uk/safety-nadine-dorries-culture-secretary-government-parliament-b988448.html

United States - European Union as the Key Global Nexus

As regards digital assurance measures, the UK will certainly need to take note of President Biden's 2021 executive order requiring a Software Bill of Materials (SBOM) to be provided to purchasers of software products.[11] Effectively an ingredients list, it aims to provide clarity on the provenance of software components, in turn enabling customers to conduct thorough security audits and seek more comprehensive assurance. While materials are liable to change over time, they are expected to be largely consistent across jurisdictions. It is therefore logical and perhaps inevitable that the SBOM will become the de facto international standard for mapping and declaring software components, with national authorities focused on overseeing security assurance and risk management appropriate to that provenance. Such a role would be consistent with that envisaged for national authorities in the EU Digital Operational Resilience Act (DORA) and the bloc-wide software certification framework set out in the EU Cybersecurity Act.

Mutual recognition of certification schemes is also essential. After the EU Cybersecurity Act entered into force in June 2019, the UK government issued a call for views. According to the government response issued in December 2019, the seventeen responses received highlighted the following themes:[12]

- 'General support for the UK Government's approach on EU Cyber Security Certification.
- Support for the proposed principles and actions as presented in the Call for Views, including our approach on mutual recognition.
- Encouraging UK commitment to continued enhancement of cyber security across Europe and ensuring the highest standards of cyber security.
- Alignment of future schemes to limit risk of regulatory divergence, preventing unnecessary market fragmentation and fostering innovation and competition.
- Reducing costs for consumers, ensuring no risks to industry and a role for industry in the creation of certification schemes.'

The government observed that these views were generally in line with the feedback they had received from industry through other means of engagement, and that they had helped to further inform the government's position. A lack of visible progress three years on is therefore a matter of some concern, not least because other countries such as Singapore are aggressively pursuing – and concluding – mutual recognition arrangements with EU Member States.[13]

Meanwhile, the United States and the EU have stepped up their strategic bilateral engagement. Established at the June 2021 US-EU Summit, the US-EU Trade and Technology Council (TTC) seeks to 'advance Transatlantic cooperation and democratic approaches to trade, technology, and security, with the goal of delivering benefits for people on both sides of the Atlantic.'[14] With Artificial Intelligence (AI) and semiconductors highlighted as of particular interest, the Council comprises ten working groups:[15]

[11] The White House. (2021, May 12). *Executive order on improving the nation's cybersecurity*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[12] Department for Science, Innovation and Technology, & Department for Digital, Culture, Media and Sport. (2019, September 11). *EU Cyber Security Certification (EU Exit) Call for Views*. GOV.UK. https://www.gov.uk/government/publications/eu-cyber-security-certification-eu-exit-call-for-views#full-publication-update-history

[13] CSA Singapore. (2022, October 20). *Singapore and Germany Sign Mutual Recognition Arrangement on Cybersecurity Labels for Consumer Smart Products*. https://www.csa.gov.sg/News-Events/Press-Releases/2022/singapore-and-germany-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-smart-products

[14] United States Department of State. (n.d.). *U.S.-EU Trade and Technology Council (TTC)*. https://www.state.gov/u-s-eu-trade-and-technology-council-ttc/

[15] European Commission. (2021, September 21). *EU-US Trade and Technology Council Inaugural Joint Statement*. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951

1. Technology Standards
2. Climate and Clean Tech
3. Secure Supply Chains
4. Information and Communication Technology and Services (ICTS) Security and Competitiveness
5. Data Governance and Technology Platforms
6. Misuse of Technology Threatening Security and Human Rights
7. Export Controls
8. Investment Screening
9. Promoting Small- and Medium-sized Enterprises (SME) Access to and Use of Digital Tools
10. Global Trade Challenges

A cursory review of this list reveals that at least half of the working groups (1, 3, 4, 6, & 7) touch on the subject of secure supply chains and procurement. That it is a priority for this high-level group, co-chaired by the EU Commissioners for Digital and Trade, the United States Secretary of State, and the United States Secretary of Commerce, is evidenced in the May 2022 agreement to develop a common early warning and monitoring mechanism on semiconductor value chains and a dedicated taskforce on public financing for secure and resilient digital infrastructure in third countries.[16]

Now considered by Chatham House to be 'the main platform for US–EU cooperation at the intersection of economics, technology and security', a bilateral focus is nevertheless insufficient to address global trade challenges.[17] While the UK does not enjoy direct representation on the Council, it should – perhaps alongside the other Five Eyes nations (Canada, Australia, and New Zealand) – seek to be considered as a trusted third-country partner. Indeed, it would seem sensible to promote aligned representation in this format, just as the Five Eyes and G7 members have done in their contributions to the process to elaborate a comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (UN Cybercrime Convention).[18] The successful adoption by Finance Ministers of recommendations by the G7 Cyber Expert Group suggests that there is scope to expand its work beyond the financial sector and for British cyber interests to be promoted in this forum.[19] In short, the UK would be well advised to exploit existing alliances to ensure that its experience in supply chain security management and expertise in security audit – as evidenced by the work of the NCSC's Huawei Cyber Security Evaluation Centre– is put to best use globally.[20]

[16] European Commission. (2022, May 16). EU-US Trade and Technology Council: strengthening our renewed partnership in turbulent times. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3034

[17] Schnieder-Petsinger, M. (2022, December). Strengthening US-EU Cooperation on trade and technology. https://www.chathamhouse.org/sites/default/files/2022-12/2022-12-08-us-eu-trade-and-tech-cooperation-schneider-petsinger.pdf

[18] United Nations Office on Drugs and Crime. (n.d.). Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[19] Deutsche Bundesbank. (2022, October 13). G7 countries adopt reports on cybersecurity. https://www.bundesbank.de/en/tasks/financial-and-monetary-system/international-cooperation/g7/g7-countries-adopt-reports-on-cybersecurity-764644

[20] Cabinet Office, & National Cyber Security Centre. (2021, July 20). Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2021. GOV.UK. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-hcsec-oversight-board-annual-report-2021

Conclusion: What Next?

Having ultimately come to terms with the fact that there is no such thing as absolute cybersecurity, leading international players have embraced security audit and assurance as key defence measures. Where securing physical and digital supply chains may once have been distinct concerns addressed by different personnel, the continued expansion of the Internet of Things – of physical objects with digital connectivity – promises an increased likelihood of cyber-attacks that impact on physical supply chains and product safety. The need for interoperability across functions and jurisdictions is therefore all the greater.

Given that the UK is outside the leading international cybersecurity regulatory and strategic initiatives, there is an urgent need for Britain to assure other jurisdictions of its continued strategic relevance, operational dependability and practical equivalence. With cyber insecurity consistently identified in its top ten global risks, the World Economic Forum is one setting in which cybersecurity vendors and British businesses can make their voices heard.[21] The Government, meanwhile, must now renew and accelerate efforts towards mutual recognition of national standards, active alignment with international certification and assurance mechanisms including the Software Bill of Materials and the US-EU Trade and Technology Council, and promotion of UK interests and expertise through existing alliances.

[11] World Economic Forum. (2023). *The Global Risks Report 2023 18th Edition*. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

The British Foreign Policy Group is an independent, non-partisan think tank dedicated to advancing the UK's global influence, at a crucial time in the nation's modern history. To achieve this, we produce dynamic events and high-quality research, and facilitate networks amongst stakeholders with a vested interest in Britain's international engagement.

Our core objective is to bridge the link between the domestic and international spheres – recognising that Britain's foreign policy choices and obstacles are shaped by our social landscape at home. Through pioneering research into the UK's social fabric, we seek to build understanding of the nuances of public opinion, and how our foreign policy can become more inclusive, responsive and relevant to citizens' lives.

BFPG British Foreign Policy Group