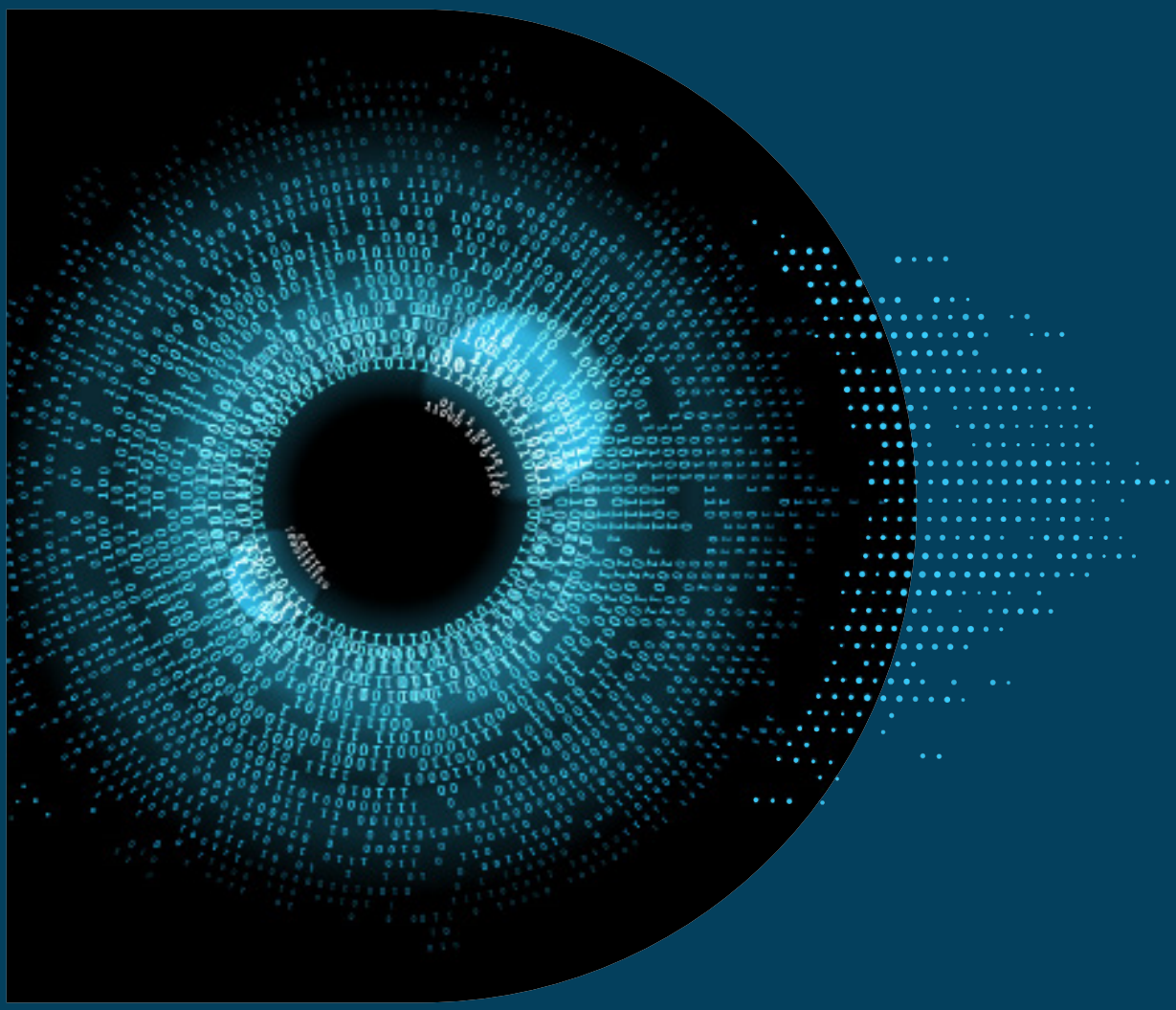
Security for one is security for all

Understanding the importance of international cyber capacity building



Digital Intelligence

BAE SYSTEMS

Executive Summary

International cyber capacity building does what it says on the tin: it strengthens the cyber ecosystems of developing nations to allow them to better deliver cybersecurity.

Having national 'cyber capacity' is important, since it enables states to harness the benefits of digitisation, while protecting a country's assets and resilience.[i] Indeed, cyber capacity is defined by five dimensions that, together, enable a nation to exercise its autonomy in and through cyberspace. These include higher level policies, strategies and legal frameworks; people-orientated awareness raising and skills development; as well as the deployment of technologies themselves.[ii]

With this in mind, many of the world's 'cyber powers' are now directing attention and resources to international cyber capacity building – that is, assisting partnered and neighbouring nations to develop their own national cyber capacity. However, although there is a growing awareness of how nations can deliver 'cybersecurity', and how important it is to secure domestic systems, the return on investment received from efforts abroad is less immediately visible. This paper will therefore articulate why international capacity building is a worthwhile investment, and outline the value it adds to the ecosystems of beneficiaries and donors alike.

The paper argues in line with the well-versed mantra that cyberspace is only as resilient and prosperous as its weakest link. An ever-growing number of nations are centring digital technologies in their national security and economic development strategies.

However, if these visions do not sufficiently account for the cyber requirements of these systems, digital transformation risks increasing the entire digital community's exposure to threats and vulnerabilities. Investment in the overall health of global cyberspace is therefore important to the stable functioning of societies, economies and political systems all around the world.

Introduction:
International cyber capacity building – so what?

Governments, businesses and societies are becoming increasingly well-versed in the domestic benefits that digital connectivity brings. From improving healthcare and the potential for reducing emissions, to more inclusive economic growth and evidence-driven governance, digital transformation has afforded a structural shift that shows little signs of slowing.

This shift has necessitated a dramatic rethink in how nations approach the issue of national security and economic wellbeing. Realising the developmental benefits of cyberspace requires more than just 'getting online' – it requires a holistic understanding and management of the risks associated with digital connectivity.

Yet this appreciation of the *importance* of cybersecurity has not uniformly followed digitisation. Indeed, too few states are prioritising security-related thinking, and too many are finding themselves fighting a rising tide of threats and vulnerabilities with scarce resources and time.[iii] As shown by the increasing frequency and severity of malicious cyber activity worldwide, cybersecurity is a long way off being mainstreamed into developmental thought – especially in sectors not traditionally 'digital'.[iv]

Compounding this challenge is the fact that cyberspace is neither nationally-contained, nor a domain that specialists can manage at the purely technical level. Rather, it is a 'shared space' that is cohabited by actors from all over the world, ranging from governments and organisations to individual users with varying levels of technical know-how.

In this context, the security of one depends on the security of all: as increasingly complex networks of information technologies expand across the globe, so the opportunities for attackers to capitalise on weak links grow.[v] The security and prosperity of domestic and international communities will suffer when countries are not equipped to handle cyber threats.[vi]

Cyberspace is only as resilient and prosperous as its weakest link.

Cyber power and cyber capacity

International cyber capacity building is one answer to these challenges. As articulated in great length in the UK government's National Cyber Strategy, a secure cyber domain is integral to the healthy functioning of a nation's economic and political systems. Crucially, the strategy's notable step up from 'cybersecurity' to 'Cyber Power' – which retains security and resilience as its core strategic tenets, but widens its scope of objectives – highlights how the ability to protect and promote national interests in and through cyberspace is as much contingent on international factors as our own domestic maturity.[vii]

Furthermore, there is a growing consensus among global partners that becoming a more secure, resilient and prosperous nation means that Cyber Power must be a whole of society effort that covers law, policy and user skills; and is not merely reactive, but able to anticipate security issues and build resilience to them.[viii]

International cyber capacity building hence reflects a commitment to protect the benefits digital transformation offers for all. In practice, the term describes the cyber security-related development programmes being delivered by donors such as the United Kingdom, Australia[ix], the European Union[x] and many more, in developing countries. These consist of various combinations of technical training, institution building and policy development.[xi]

Collectively, they aim to mature critical cyber capabilities in recipient countries, and establish an inclusive, coherent set of international cyber policies in order to enhance the ability of international partners to meaningfully cooperate with each other. Though to date such programmes have represented a small proportion of international development budgets, investment into them is rapidly increasing.[xii]

There are significant benefits to be gained from these programmes to all parties involved.[xiii] Certainly, their value to recipient countries appear more palpable. Yet although the ways in which they benefit donors, especially at a time of wider economic challenges, has thus far been less clearly articulated, this paper aims to highlight that the benefits do not flow just from donors to beneficiary nations. Rather, they flow both ways. Cyber capacity building generates numerous returns for the wider community.

I. Capacity building ensures cyberspace itself is stable and reliable.

The rising instability of cyberspace has become a pressing issue across the world. 'Stability' is understood as having "reasonable confidence in the ability to use cyberspace safely and securely"; in other words, confidence in the availability and integrity of cyberspace at all times.[xiv] This confidence must account for the fact that both cyberspace itself, as well as users operating in it, are constantly evolving – meaning that 'stability' involves change to be "managed *peacefully*", and tensions between actors being resolved "in a non-escalatory manner".[xv] Instability is generated by malicious cyber activity, which in contemporary trends is heavily informed by the exploitation of global networks as attack vectors by criminals or states.[xvi] Given the transnational nature of cyberspace, achieving a nation's security objectives therefore requires collaboration with communities beyond the nation's borders.[xvii]

Cyber capacity building supports the stabilisation of cyberspace by enhancing the ability of partnered nations to contain malicious activity further upstream. One key dimension of this is the mitigation of disruption: as witnessed during the 2017 NotPetya attacks, disrupting critical infrastructure such as water or energy supplies through malicious cyber activity is becoming more common, and can have a devastating impact on the economic activity and safety of society at large.

Indeed, this is becoming more common as advancements in operational cyber capabilities are enabling cyber-attacks to become more sophisticated, difficult to mitigate, and damaging to the physical world.[xviii] Yet what was intended to disable Ukraine's energy grid had significant global knock-on effects.

For example, in Denmark, the headquarters of Maersk – responsible for approximately one-fifth of the world's shipping – was brought to a standstill by the malware. Disruptions affected port facilities worldwide, and resulted in $200 - $300 million worth of losses.[xix] Indeed, seemingly localised attacks all too often have unforeseen consequences; strengthening resilience against such attacks limits unforeseen damaging impacts elsewhere.

Capacity building also strengthens the ability of partners to detect and prevent transnational cybercrime. The transnational nature of cyberspace means that cybercriminals can be located outside national boundaries of their victims. Consequently, international relationships and capacity are often necessary to enable law enforcement.

Through developing or reforming legal frameworks in line with collaboratively agreed international standards such as the Budapest Convention on Cybercrime, the ability of criminal justice authorities, such as law enforcement and judges, to effectively investigate and prosecute cybercrime is drastically improved. Indeed, as digitisation is increasingly tied to social and economic development, so the possibilities for criminal activity increases.

Cybercrime is not only the fastest growing form of organised crime affecting the world; the rise of organised crime groups that offer underground hacking and disinformation services, for example, is also rapidly becoming the most serious financial threat to individuals and organisations in Western countries.[xx] The impact of this spectrum of offences, including extortion, IP theft and business disruption, is expected to cost the global community up to $10.5 trillion by 2025.[xxi]

Further damages include reputational damage and personal distress. Strengthening the ability of partner law enforcement agencies to address these threats enhances the security of both the host nation, as well as the broader international community, and in addition establishes more concrete prospects for reliable partnerships.

2. Capacity building facilitates international information sharing.

Closely related is the benefit of improved information sharing. This is critical to developing broader situational awareness of the threat landscape, and applies both to information exchange between nations, as well as between the public sector and private industry. Information sharing covers a range of information types, from atomised tactical information to aggregated, custom intelligence. It is an important practice, since effective prevention of, or response to, malicious cyber-attacks is in large part dependent on an understanding of which methods – or 'tactics, techniques and procedures' (TTPs) – malign actors are employing against their victims, as well as which organisational vulnerabilities they are exploiting.

Generally speaking, the efficacy of information sharing practices is limited by the maturity of a nation's digital ecosystem, with common barriers including a lack of harmonised regulations, unclear communication channels or uncertain delegation of responsibilities; such barriers, by extension, hamper effective collaboration on cyber threats.[xxii] Indeed, information exchange at both the operational technical and strategic levels enable decision-makers to understand the threat picture their organisations face, and be able to more effectively mitigate malicious cyber activity.[xxiii]

Threat information sharing is effective in a range of scenarios, such as financially-driven cyber-crimes, terrorism, hacktivism or state-sponsored espionage.[xxiv] For instance, some countries in receipt of capacity building may be on the 'front line' of conflict in strategically significant locations, and hence be frequent targets by adversaries seeking to test and refine their TTPs, and improve their general disruptive capabilities.[xxv]

Consequently, they harbour extensive knowledge of threat actors and attack vectors that may later be deployed against other nations.[xxvi] Sharing this intelligence with international partners, however, is contingent on the efficacy of *internal* information sharing, starting with the ability of nations to take analyse and aggregate incidents into useful, actionable and share-able intelligence.[xxviii] Developing these practices in line with international standards will, in the long term, enable partner nations to generate and share their own threat intelligence into the global community – to the benefit of all.

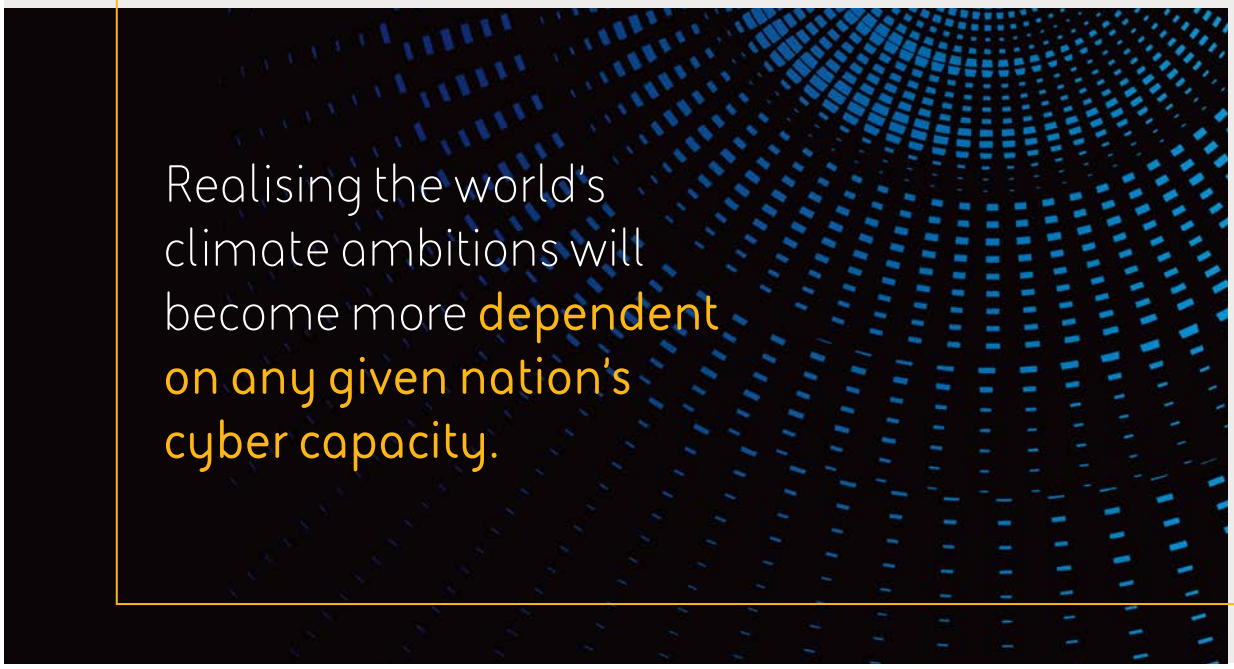
3. Capacity building is key to realising the world's climate goals.

Third, cybersecurity is an enabler of reliable and secure climate-friendly infrastructure.[xxviii] Climate change is one of the biggest threats to modern society, and facilitating the sustainable energy transition is become an important policy goal for governments around the world.[xxix] Against this backdrop, many are turning to innovative, climate-friendly technologies and other digital methods as a solution – meaning that realising the world's climate ambitions will become more dependent on any given nation's cyber capacity.[xxx]

Indeed, digital solutions to carbon emissions already exist in a range of sectors, including energy, transport, construction and agriculture, with the digital technology sector increasingly seen as world's most powerful influencer to accelerate action and stabilise temperatures.[xxxi] In instances such as sustainable smart agriculture or smart cities, for example, digitisation has afforded many benefits, such as increasing the efficiency of utility supplies, sustainable transport solutions and more.

However, this digital backbone offers another attack surface if it is insufficiently secured.[xxxii] As outlined above, the criticality of energy systems makes them a prominent target of malicious cyber activity. The shift towards renewables will induce greater reliance on smart electricity systems that must be resilient to such attacks.[xxxiii] Vulnerabilities may include human error, software failures or even unpredicted weather conditions. Threats arise from malicious actors aiming to financially benefit from their actions through ransomware or IP theft – or to cause social and political disruption.

As mentioned, companies and critical infrastructures may also be collateral damage in attacks launched elsewhere. In this context, cyber capacity building is both a national tool that will build up expertise and research in the evolving cyber risk of critical national infrastructure, and a mechanism for internationally and diplomatically driving interest in technical standards and secure development.[xxxiv] Thus, if technological advancement is to be the key to lowering carbon emissions, capacity building will be the backbone that enables these goals. This way, nations can ensure that novel systems develop in a manner that allows for resilience of the technology itself, and society more widely.



4. Capacity building is an enabler of international trade.

Fourth, the benefits of cyber capacity building also touch the economic domain, one dimension of which is in international trade. For example, maturing the cyber capacity of trading partners helps to ensure greater resilience of critical supply chains. A crucial dimension of this is managing the risks attached to supply chains, which increasingly includes *cyber* risk, such as innovation theft, financial and reputational damage or, in extreme cases, complete supply chain denial or disruption.[xxxv]

Cyber risk is especially difficult to manage: as organisations' understanding of threat activity, risk management and vulnerability identification has improved, so too has the ability of adversaries to compromise the confidentiality, availability and integrity of information systems.[xxxvi] The landscape is constantly evolving, and businesses may easily be on the back foot.

As highlighted by the SolarWinds breach, factors as mundane as weak internal passwords ('solarwinds123') have the ability to compromise entire supply chain systems.[xxxvii] Indeed, national reliance on international trade and global supply chains means that governments must understand the cybersecurity risks and vulnerabilities of partner businesses and organisations both at home and abroad.

Closely related is the role that cyber capacity building plays in confidence-building and trust development between trading partners.[xxxviii] In order to de-risk their supply chains, and reduce dependencies on any single source of import, many nations are adopting a strategy of diversified trade relations.[xxxix] In other words, the pursuit of new trading partners opens the possibility for new markets that – if trusted to meet adequate security standards, and thus invite certainty to trading relationships – can pave new paths to prosperity for partnerships.[xl]

Certainty is thus greatly improved through developing the cyber capacity of current and prospective trading partners: governments will be more incentivised to invest in regions that are well versed in national cybersecurity issues, industry standards and policies, and can thus comfortably grapple with cyber-related challenges. By collectively raising the bar to create trusted trading communities, cyber capacity building facilitates trade and investment to the benefit of all parties involved.

5. It strengthens national autonomy on the international stage.

Lastly, cyber capacity building offers an opportunity to ensure cyberspace remains open and free – thus safeguarding the ability of nations to act autonomously in and through it.[xli] The ubiquity of cyberspace in all facets of life has fostered a rethink of how it is to be governed. Increasingly, it is moving from an unregulated area, to one that is subject to internationally-agreed norms, standards and laws.[xlii]

Key debates that have emerged in this regard include the degree of oversight government should have over standards organisations, which standards forums are most authoritative, and which topics constitute 'cybersecurity' issues that should be tabled.[xliii] However, not all nations have equal footing in this debate, and many existing standards tend to reflect the cultural specificities of the nation in which the regulation and technology originated.

In other words, the variation in global capacity levels has enabled some to more strongly determine the governance of cyberspace than others.[xliv] In this context, the ability to respectably participate in these debates is key to ensuring nations can contribute to norm and law development, and safeguard their own values in and through cyberspace.

In the face of this, investing in international cyber capacity building helps strengthen the ability of nations to contribute to global cyber-norms and laws, and express their own values in and through cyberspace. Indeed, the rapid advancement of digital technology is swiftly outpacing society's understanding of how to harness cyber tools effectively, making societies deeply vulnerable to a range of threat actors.

Developing their maturity addresses these vulnerabilities, and reduces the external risk nations are exposed to. Indeed, relevant capacity building measures may include auditing access controls, improved cybersecurity hygiene and practises (such as patching and awareness raising), or greater capability to develop a comparative cyber-advantage. Thus, capacity building is a prerequisite to adopting and implementing norms that helps to ensure the stability of cyberspace. Developing cyber capacity abroad is central to maintaining national integrity, both in domestic and wider international contexts.[xliv]

Cyber capacity building offers an opportunity to ensure cyberspace remains open and free.

Conclusion

If the global community is to harness the positive economic and social potential of cyberspace without compromising the health and openness of our society, appropriate attention must be paid to associated challenges and risks. Both domestic and global security and prosperity suffer when countries are not equipped to handle cyber threats.

Through improving the understanding of, and enabling better participation by countries across the world, international capacity building will help implement internationally-agreed laws, norms, and confidence-building measures. In sum, these will lead to a more sustainable, stable and resilient cyberspace for all.

[i] https://gcscc.ox.ac.uk/the-cmm
[ii] https://gcscc.ox.ac.uk/the-cmm
[iii] https://www.baesystems.com/en/cybersecurity/threat-intelligence-insights
[iv] https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1948582
[v] https://hcss.nl/wp-content/uploads/2021/12/Painter.pdf
[vi] Ibid
[vii] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[viii] Ibid
[ix] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
[x] https://www.eucybernet.eu/about-project/
[xi] https://hcss.nl/wp-content/uploads/2021/12/Painter.pdf
[xii] For example, as described in the UK Innovation Strategy: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009577/uk-innovation-strategy.pdf
[xiii] https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1948582
[xiv] https://cyberstability.org/report/#2-what-is-meant-by-the-stability-of-cyberspace
[xv] Ibid
[xvi] https://032c.com/magazine/the-age-of-unpeace-mark-leonard-explains-how-connectivity-causes-conflict
[xvii] https://www.rusi.org/events/open-to-all/advanced-technology-international-partnerships-and-geostrategic-competition
[xviii] https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/
[xix] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=442996d24f9a
[xx] https://www.belfercenter.org/publication/cybercrime-hotspots
[xxi] Ibid
[xxii] https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide
[xxiii] https://www.csis.org/analysis/hidden-costs-cybercrime
[xxiv] https://www.gov.uk/government/publications/open-standards-for-government/exchanging-cyber-threat-intelligence
[xxv] https://www.washingtonpost.com/national-security/2022/05/11/ukraine-us-intelligence-sharing-war/
[xxvi] For instance, see here: https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/
[xxvii] https://www.mitre.org/sites/default/files/pdf/cyber_info_sharing.pdf
[xxviii] https://www.paconsulting.com/newsroom/expert-opinion/utility-week-robust-cybersecurity-is-an-enabler-of-net-zero-19-january-2022/
[xxix] As mentioned in the UK Integrated Review, for example. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy
[xxx] https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy
[xxxi] https://www.weforum.org/agenda/2019/01/why-digitalization-is-the-key-to-exponential-climate-action/
[xxxii] https://rusi.org/explore-our-research/publications/emerging-insights/securing-net-zero-future-cyber-risks-energy-transition
[xxxiii] https://rusi.org/explore-our-research/publications/emerging-insights/securing-net-zero-future-cyber-risks-energy-transition
[xxxiv] Ibid
[xxxv] https://www.gov.uk/government/news/new-plans-to-boost-cyber-resilience-of-uks-critical-supply-chains
[xxxvi] https://www.nist.gov/speech-testimony/solarwinds-and-beyond-improving-cybersecurity-software-supply-chains
[xxxvii] https://www.techuk.org/resource/securing-supply-chains-what-can-be-learnt-from-solarwinds.html
[xxxviii] https://www.csis.org/analysis/diversifying-supply-chains-role-development-assistance-and-other-official-finance
[xxxix] Ibid
[xl] https://thediplomat.com/2022/03/tilting-or-toppling-assessing-the-uks-indo-pacific-policy-one-year-on/
[xli] https://www.baesystems.com/en/cybersecurity/feature/government-insights-cyber-resilience-and-democracy
[xlii] https://rusi.org/events/open-to-all/advanced-technologies-and-geostrategic-instability-conversation-dr-ian-levy-obe/
[xliii] https://carnegieendowment.org/files/Good-Harbor_Securing-Cyberspace-Through-International-Norms_2013.pdf
[xliv] https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12281
[xlv] https://hcss.nl/wp-content/uploads/2021/12/Painter.pdf

We are Digital Intelligence

The UK security and resilience sector is world renowned, and along with Defence exports, has long been recognised as an export opportunity for economic growth; however it is distinct from Defence exports, particularly in that it is a sector largely dominated by small to medium sized enterprises (SMEs).

The recently published Integrated Review places strengthening security and resilience at home and overseas at its heart. The sector is therefore well placed to help strengthen the security and resilience of our partners and allies, and as a valued capability it could help expand UK influence abroad in a post-pandemic and post-Brexit era.

The UK Government already uses security and resilience SMEs to delivery capacity development to partners and allies, but the scale of its interventions are limited by its ability to manage and integrate the work of multiple SMEs.

BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra, ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
Suite 905 Arjaan Office Tower,
Dubai Media City
Dubai
T: +971 (0) 4556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

BAE SYSTEMS