Rashid, A., Hankin, C., & Schneider, S. (2020). *The future of the UK's Cyber Security Research Position in the World*.

The future of the UK's Cyber Security Research Position in the World

Professor Awais Rashid University of Bristol, UK
Professor Chris Hankin Imperial College London, UK
Professor Steve Schneider University of Surrey, UK

University of BRISTOL

Imperial College London

UNIVERSITY OF SURREY

The future of the UK's Cyber Security Research Position in the World

Professor Awais Rashid University of Bristol, UK
Professor Chris Hankin Imperial College London, UK
Professor Steve Schneider University of Surrey, UK

Executive Summary

Cyber security is one of the major challenges facing our modern connected digital world. As we build ever more connected infrastructures and digital services, not only the security of the data in our digital economy, but also the safety and continued operation of critical systems such as water, power and transportation, rely on them being cyber secure. The National Security Strategy has a goal to make the UK the safest place to do business online in the world. Research at UK universities plays a leading role in meeting this goal – anticipating the cyber security challenges of emerging and future technologies and identifying methods, tools and technologies to mitigate the risks of harm.

The UK is currently recognised as one of the leading countries in the world in cyber security research. This is evidenced by research outputs in leading international venues, research collaborations with major international centres and global industry organisations and key UK researchers acting on the international advisory bodies of major research centres worldwide and global policy forums.

Is this global position sustainable? Or, as other countries up their game and invest heavily in cyber security, do we risk falling behind if comparable level of investment in research on cyber security are not made by the UK?

We have identified and characterised, where possible, the strategic investments in cyber security research made by some of the leading research nations in the world, namely, the UK, USA, EU Horizon 2020 programme, France, Germany, Israel and Singapore[1]. We have analysed funding allocated from 2012–2019 through strategic calls for research grants and large centres in these countries to evaluate and compare the types and values of those strategic investments, with particular context given to the current and planned future investments in cyber security research in the UK. Through this analysis we provide an evidence-based perspective on whether the nature and rate of investment made in UK cyber security research will remain at par with our major competitors worldwide and, if not, identify the risks of not doing so for the future of UK research and innovation – and its global leadership in this critical sector.

Findings

- Significant capacity has been developed in the UK between 2012 and 2019 through the 19 Academic Centres of Excellence in Cyber Security Research (ACE-CSRs), the four EPSRC-NCSC Research Institutes, the four Centres for Doctoral Training, the Centre for Security Information Technologies (CSIT) and the PETRAS National Centre of Excellence in Cyber Security of Internet of Things.
- However, major long-term investments in other nations, especially, the USA, France and Germany, are leading to the development of large clusters of research excellence. These pose risks not only with regards to brain drain from the UK but also, based on levels of investment from 2012–2019 and continuing investments beyond 2019, to maintaining the UK's position as a leading nation for research and innovation in cyber security.
- In absolute terms, and as a percentage of GDP, UK investment in cyber security research falls significantly behind our major competitors. There is a need for a step change in investment in cyber security research in various forms – strategic clusters of excellence, doctoral training and the creation of national research facilities – in order to sustain and maintain the UK's cyber security research position in the world.

[1] Relevant information on strategic cyber security investments in Belgium were not available publicly so have not been included. Most research grant funding in this area is concentrated, with KU Leuven particularly prominent.

Recommendations

Based on the detailed analysis presented in this report, we make three recommendations:

Recommendation 1: The UK needs to make long-term large-scale investments in developing clusters of research excellence in cyber security.

The ACE-CSR scheme has defined a substantial community of UK cyber security researchers and the four EPSRC-NCSC research institutes have delineated sub-communities within this group. However, compared with large long-term investments in the USA (e.g., the NSA Lablets), France (e.g., through INRIA) and Germany (e.g., through large centres such as ATHENE in Darmstadt, CISPA in Saarbrucken, Kastel in Karlsruhe and Max Planck in Bochum), the UK needs to develop similar clusters of excellence. These could take the form of *Regional Clusters of Excellence* whereby strategic investment in ACE-CSRs in particular regions enables them to come together with industry to sustain and grow world-leading research competence. These may also take the form of *Mission-based Clusters of Excellence* whereby strategic investments on the basis of long-term research missions mobilise a range of ACE-CSRs into sustaining and growing world-leading research capability.

Recommendation 2: The long-term health of UK cyber security research requires significant growth in capacity building through strategic investment in doctoral research funding to train future R&D leaders in cyber security.

The UK has built a strong community of doctoral researchers through investment in Centres for Doctoral Training funded by EPSRC and through the NCSC-funded doctoral studentships in ACE-CSRs. This differs from competitor nations internationally where funding for doctoral students often forms part of core research funding to institutions. The current funding for Centres for Doctoral Training in cyber security is £17.8M. This contrasts with £100M for doctoral training in AI – another important area for R&D capacity building. The NCSC-funded studentships have helped grow capacity in ACE-CSRs but, in real terms, the investment has shrunk as the number of ACE-CSRs has grown from an initial eight to 19. As we build increasingly complex, interconnected infrastructures, the long-term goal of making and sustaining the UK as the safest place to do business online in the world requires significant investment in the next generation of researchers. This is critical in order to meet the growing shortage of highly-skilled personnel in this topic of major national and global importance.

Recommendation 3: National research facilities are critical for researchers to validate their ideas on large-scale experimental platforms – providing a competitive edge for innovative products and services that are evidence-based and globally leading in enhancing cyber security of emerging hyperconnected environments.

Longer-term funding in other countries, most notably Singapore, has supported the creation of national facilities. In the UK some unique facilities have been developed through investment via small grants, internal resourcing from universities and through collaboration with industry. Long-term investment in innovative products and services requires facilities on a scale that enables empirical validation of innovative research ideas in real-scale environments. A step change is needed in investment in experimental research facilities – both with regards to linking and opening up existing facilities into a national resource and development of new facilities where such capacity currently does not exist. This provides an opportunity to establish a globally-leading position for the UK.

Methodology

The analysis presented in this report focuses on *strategic investments* in the various countries between 01 January 2012 and 31 December 2019. Only investments made by states into cyber security research at academic research institutions were included.

Strategic investments that started before 2012, e.g., Centre for Secure Information Technologies (CSIT) Phase I (Tranche 2) are pro-rated versus the estimated value during the period 2012-2019, while CSIT Phase II funding is included in full. Similarly, where the allocated funding lasts beyond 2019, the figure for 2012-2019 includes the pro-rated values while the total investment from 2012 includes the figures from 2012 until the end of the award period. EU Horizon 2020 funding has been included in each state where funding was allocated to a university within it. This takes the direct allocation plus a percentage proportion (derived from allocation) of administration funding.

Note, funding that has been announced before 31 December 2019 but where awards won't start until 2020 is not included in the analysis, e.g., in the case of the UK, the UKRI Digital Security by Design and AI for Security/Security of AI funding calls. The same restrictions were applied to any funding for other countries.

Definition of Strategic Investment:
This is considered as any funding provided by a state (or relevant EU Horizon 2020 funding) specifically for cyber security research. This may be through targeted calls for research grants, establishing centres or through funding initiatives, e.g., for doctoral training, to increase cyber security capability. We recognise that a number of research projects are funded in the UK and in other countries through *responsive mode* or generic calls. However, these are not considered strategic investments and are not included in this analysis. For example, in the UK context, the data includes the Digital Economy Trust, Identity, Privacy and Security (DETIPS I and II) funding calls but not any responsive mode ICT grants or centres such as CREST (which is generally focused on behavioural sciences approaches to security rather than a specific focus on cyber security). Similarly, in Germany, for instance, we do not include the CROSSING centre at TU Darmstadt – although it is focused on Cryptography-based Security Solutions, the award was through a general competitive call for centres rather than a specific strategic call on cyber security.

Country	Total Validated Investments from 2012	Total Investment between 2012 - 2019
France	£103,649,423	£97,367,302
Germany	£454,097,364	£110,790,338
Israel	£30,177,390	£24,220,398
Singapore	£81,196,500	£63,542,357
UK	£126,062,760	£77,368,991
USA	£527,578,080	£356,028,268
EU Horizon 2020	£54,688,818	£13,213,658

Table 1: Strategic cyber security investments by country

The data for each country was collected from public information sources and cross-validated with funders' online databases, wherever such cross-validation was possible. The data collection was undertaken by two researchers who cross-checked and validated each other's work and assisted each other in further data collection and source validation in order to ensure the fullest coverage possible. Where needed, we also sought advice and confirmation for data sources from colleagues in relevant countries. As not all countries maintain centralised government or funder databases, the cross-validation was more rigorous in the case for the UK, Singapore and the USA due to the existence of funder databases. The full list of sources consulted during data collection and completeness of that information is included in the *Appendix* to this report.

Potential under-assessment of strategic investment internationally
The most complete data in our analysis comes from the UK – in part due to our familiarity with the research funding landscape and partly due to the policy of research funding openness, which makes finding and tracking strategic investments easier. The incompleteness of data for several countries means that we may be under-assessing their true strategic spend. For instance, for all countries (apart from the UK), strategic investment in doctoral training is difficult to ascertain as this is part of core grants to universities, unlike the strategic or competitive nature of Centres for Doctoral Training in the UK (and also the Doctoral Training Grants to universities which are determined based on research grants awarded to institutions).

Furthermore, in countries such as Germany and France, the national grant awards are primarily for the *additional costs* of salaries for postdoctoral researchers rather than on a *full economic costing* basis, as is the case for the UK. Therefore, the funds are utilised for building additional capacity rather than also funding core academic staff and facilities as in the full economic costing model in the UK.

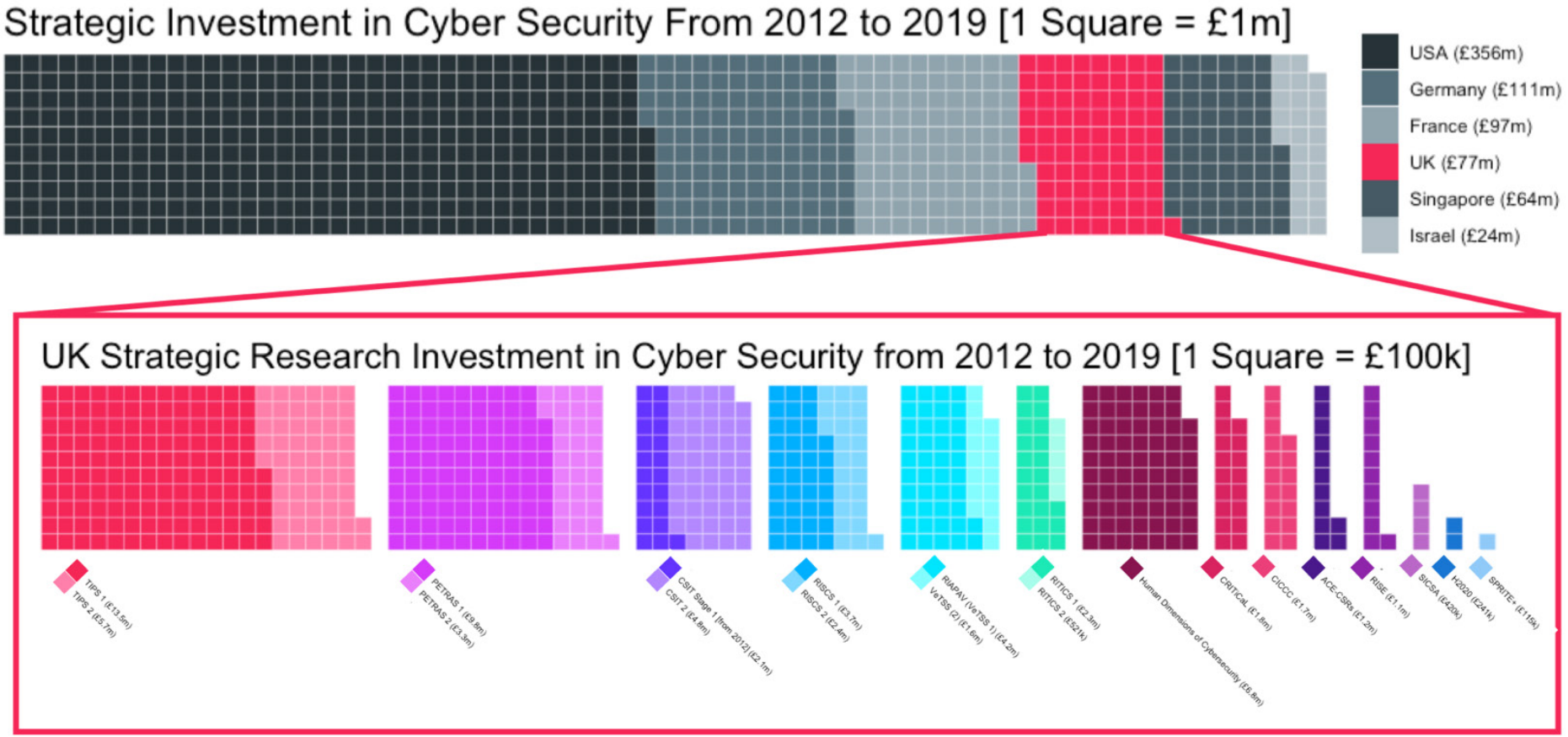

Figure1: Strategic investment in cyber security per country, with expansion to a detailed view of UK strategic investment in cyber security.

How does the UK approach contrast with research capacity building internationally?

The UK's approach to research capacity building takes three primary forms:

- Investments through strategic funding calls for research projects, for example, DE TIPS I and II, and Human Dimensions of Cyber Security, which aim to address specific research questions through projects, and also lead to training of postdoctoral researchers;
- Centres and Research Institutes, for example, the PETRAS National Centre of Excellence on Cyber Security of Internet of Things, the four EPSRC-NCSC Research Institutes, as well as the Academic Centres of Excellence in Cyber Security Research (ACE-CSRs) programme;
- Strategic training of future R&D leaders in cyber security through Centres for Doctoral Training (CDTs) – initially there were two such centres at Royal Holloway, University of London and University of Oxford. At the time of this report two additional cyber security CDTs have been awarded at University of Bristol (jointly with University of Bath) and University College London. There has also been a programme of competitively-funded PhD studentships from NCSC through the ACE-CSRs.

This is in contrast to most other states where the primary strategic investment is in research funding (at postdoctoral level) with doctoral training regularly funded through core PhD funding programmes to universities. This provides a regular and growing pool of cyber security researchers to fulfil the workforce needs in academia, industry and education whilst maintaining a steady level of research-only / blue-sky research investment. However, some specific training-focused investments or mixed investments that support both research and training exist. For instance, in France, there are strategic initiatives funded in Brittany to increase the regional number of Master's and PhD level graduates in cyber security. In the USA, the NSA Lablets support both research and doctoral training, and the same is the case for strategic investments by the Israel National Cyber Bureau (INCB).

Importance of doctoral training in capacity building
The Centres for Doctoral Training in the UK represent a significant investment to develop a critical mass of doctoral researchers through a cohort-based approach and interdisciplinary research training. Long-term support and maintenance of such strategic investments is essential to continue to develop cohorts of PhD graduates capable of working in and leading interdisciplinary research in order to meet industry R&D demand. Furthermore, such targeted doctoral centres need to be complemented by strategic core doctoral training funding to universities demonstrating research excellence in cyber security in order to maintain and grow the UK's research capacity in the face of sustained core investment in such training internationally.

In contrast to the UK – where a mixed portfolio of calls for research grants and centres operates – Germany has taken a primarily centre-based approach establishing large clusters of research excellence, for instance, ATHENE in Darmstadt, CISPA in Saarbrucken, Kastel in Karsruhe and Max Planck in Bochum, all a step change in the approach to research capacity building. These four centres on their own represent a strategic investment in Germany between 2015 and 2019 of over £100M. This contrasts with a total combined investment in the UK between 2012 and 2019 in larger initiatives – the four EPSRC-NCSC Research Institutes, CSIT and PETRAS – of £34M. Though the collective ACE-CSRs programme has attracted £1.2M of funding, the individual Centres of Excellence have received investments in the range of £20K–£80K which have been ringfenced for the organisation of events and engagement with government and industry, and do not include support for core research.

Critically, the investments in centres in other countries, such as Germany, France and the USA are long term investments – the NSA Lablets programme in the USA has been running for 10 years and the investment in centres such as ATHENE, CISPA, Kastel and Max Planck is earmarked to grow further on a per annum basis beyond 2019. For example, ATHENE is expected to grow from £10M per year to £32M per year, while CISPA is expected to grow to £43M per year.

Need to grow strategic investment
The UK has built significant capacity over 2012-2019, especially through the ACE-CSRs, and complemented by other investments such as PETRAS and EPSRC-NCSC Research Institutes. There is a need to strengthen the strategic investment in the research excellence developed by the ACE-CSRs through support for research capacity building that will enable them to sustain and continue to compete with major international centres where strategic investments in cyber security research capacity are already being made.

Comparative levels of investment

The data collected with respect to investment over the period 2012–2019 allows a comparison of strategic investment in cyber security research across the key countries we have considered. In the UK £77M of investment has been made across a broad range of academic institutions through competitive research calls in strategic areas. With the exception of CSIT (11% of the total), the centres and research institutes receiving focussed investment are consortia of institutions, thus the strategic investment has been spread widely, across nearly 40 UK universities.

The investments in France and Germany were larger than the UK's, at £97M and £111M respectively. When considered as a proportion of GDP, France's investment was 34% and Germany's 7% greater than that of the UK. The investments in France and Germany over the period have been more targeted than in the UK - much of the investment in France was through INRIA, the Institute for Research in Computer Science and Automation, and in Germany the majority was through large Centres and Institutes.

Israel and Singapore made smaller strategic investments in absolute terms than the UK, at £24M and £64M respectively, but as a proportion of GDP these were substantially greater, with Israel at 2.3 times and Singapore at 6.5 times that of the UK's. Israel's investment was concentrated into the establishment of six centres, importantly leveraging an equivalent amount from industry. Singapore's investments were split – with almost half being significant investments into specific institutions and the other half allocated through competitive cyber security calls.

Finally, the investment in the USA as a proportion of GDP was 62% that of the UK's, but in absolute terms the value of £356M was nearly five times that of the UK. The major sources for this funding were DARPA (Defense Advanced Research Projects Agency), NSA (National Security Agency), DHS (Department for Homeland Security), and the NSF (National Science Foundation). Funding from DARPA, DHS and NSA totalled £69M in large, targeted, strategic investments. NSF managed significant volumes of investment through competitive calls: Secure and Trustworthy Cyberspace (£225M); and Cybersecurity Innovation for Cyberspace (£62M), both of which provided funding for projects across a wide range of institutions.

Maintaining UK research's international competitiveness

In absolute terms and as a percentage of GDP, UK investment in cyber security research falls way behind our major competitors. In order to maintain the UK's leading position in cyber security, the level of investment should be enhanced, particularly in view of the fact that other nations are further increasing their strategic funding.

Since 2019, the step-change in investment by Germany stands out, with a projected commitment, post-2019, of hundreds of millions of pounds. This level of future investment has not been seen in the other countries in our comparator group, however, the available evidence indicates that commitments in those countries have continued on a level broadly similar to the period 2012–2019.

Need for a step change

The US (NSF only) and UK funding landscapes share some similarities in that the available funds have been dispersed over a large number of relatively small projects. While this has been beneficial in terms of capacity building, the larger, longer-term awards in other countries, such as Germany, offer a major boost to cyber security capacity in those nations for the medium and long term. This is also the case for the US, where, as noted above, investments made in centres are widely spread, but they are also much larger than those in the UK.

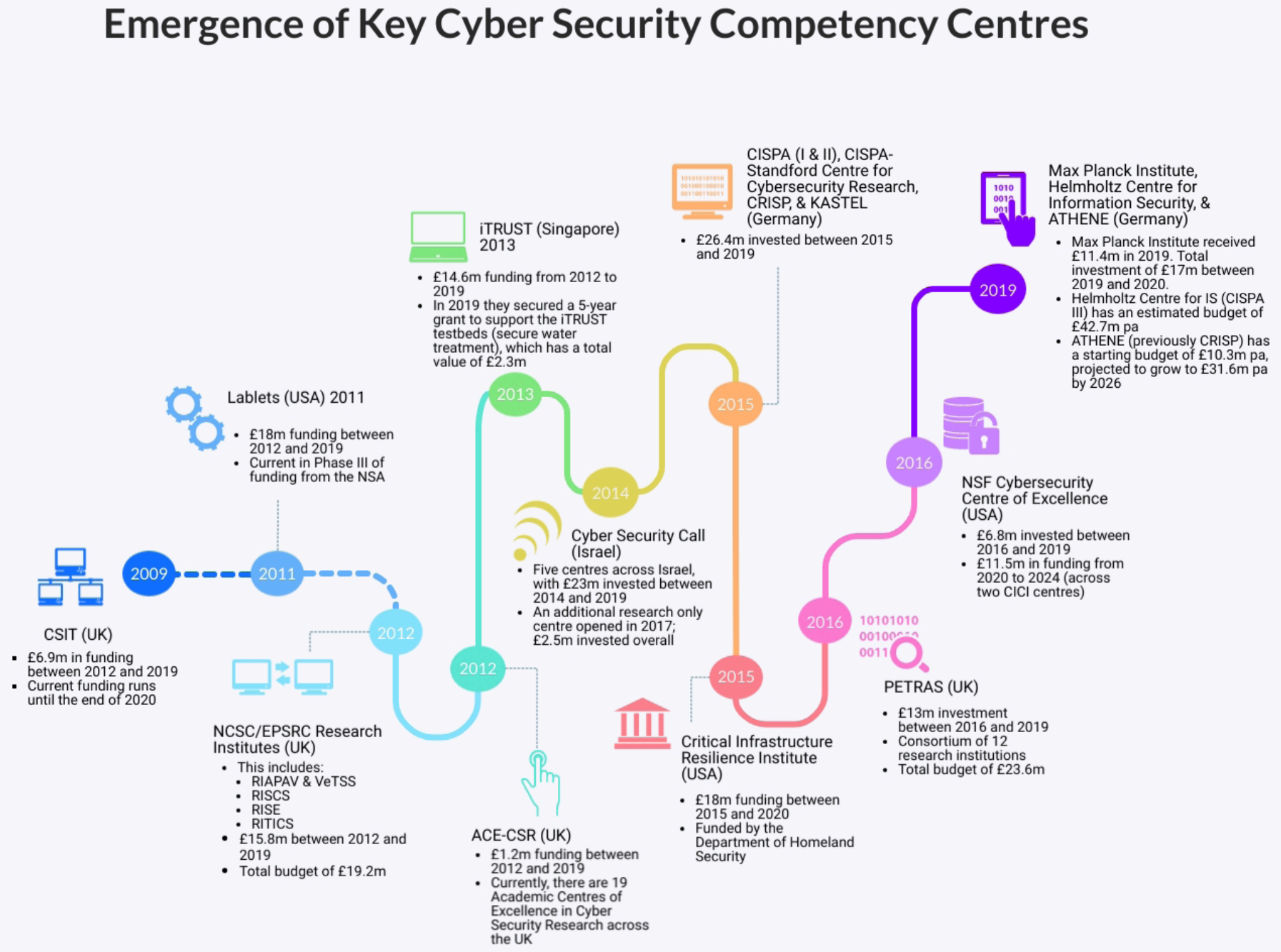

Figure 2: The emergence and evolution of key cyber security competence centre investments over the period 2012-2019.

Longevity and scale of investment

The primary sources of funding for cyber security research in the UK have been the research councils (notably EPSRC, part of UKRI since 2018) and GCHQ (since 2016, primarily through the National Cyber Security Centre, NCSC). UK computer science academics have traditionally bid for projects of 36-month duration. The two phases of the National Cyber Security Programme have helped combat this tendency - while the first phase of each of the first three research institutes encouraged 36-month research projects, the second stage has established each institute for a further five-year period. The majority of the UKRI funds for this second phase have been to support the Director (e.g., salary) and the infrastructure to sustain the relevant communities – this contribution has been capped at approximately £1M full economic cost. There has been an additional £500K per year from the NCSC for each of the institutes in support of research projects. In contrast, the PETRAS Research Centre is funded as a national research centre for cyber security of Internet of Things. The first 36-month phase received £9.8M of public funding, with a further £13.8M in the second phase from 2019-2023 – the most significant public investment in the UK cyber security sector. PETRAS, however, considers broader issues including privacy, trust and ethics. With the exception of CSIT, the other large investments in cyber security have been fragmented across multiple projects.

In France, the majority of research funding is through INRIA (estimated at £80.9M between 2012 and 2019). The INRIA model of funding is mainly through project teams which are established for up to 12 years with a review every four years. In the US, DARPA and Government agency (NSA Lablets and DHS) projects tend to run for four–five years with multi-million pounds of funding. NSF funding profiles are more comparable to UKRI (EPSRC), for example, the Secure and Trustworthy Cyberspace programme funds activity across many universities with projects of three–four years in duration and funding levels ranging from £25K to £7M. The EU Framework Programmes have also been a major source of funding for European cyber security research. There are four current strategic projects in this area involving collaborations between industry and academia, piloting a European Cybersecurity Competence Network. All started in 2019, with the spend in the first year amounting to approximately £13M and a further £41M committed to these projects up until 2023. These projects involve collaborations between industry and academia, where the academic component is a varied proportion of the overall budget (ranging from 42% to 72%).

Elsewhere in Europe and in the US, there is a much more diverse landscape of funders, some of which are providing substantial and longer-term support for cyber security research. In Germany, funders include DFG, the Federal Ministry of Education and Research (BMBF), the Helmholtz Association and the Max Planck Foundation. Our data shows an investment of over £100M between 2012 and 2019 which includes the establishment of three competence centres in IT Security, a Max Planck Institute for Cyber Security and Privacy and a National Research Centre for Applied Cyber Security. There will be further investments of hundreds of millions in just these centres alone for the next six years.

Importance of long-term investment at-scale

The creation of the ACE-CSRs, the research institutes and other strategic initiatives over the last eight years have had a major impact in establishing and growing cyber security research capacity in the UK. This is far from a self-sustaining eco-system and strategic investment is critical beyond the end of the current National Cyber Security Programme. Such investment will need to take a long-term view of maintaining and growing the UK's research capacity. Critically, it would need to do so in the presence of large-scale long-term investments in major competence centres in other parts of the world.

Longer-term substantial investment fosters the creation of national facilities (such as the iTrust testbeds in Singapore) that offer an opportunity to significantly raise the level and quality of research in this area and become a global leader. Whilst the UK has a number of such facilities (for example, the industrial control systems and IoT testbed at University of Bristol; the Cyber Range at Cardiff University and Autonomous Vehicles testbed at University of Warwick), they have largely been funded through small grants and institutional support. Though such facilities are accessible to researchers nationally, the lack of core long-term funding limits their growth and role as national facilities.

Need for national facilities for cyber security research

The UK cyber security research community has now grown to a size where serious consideration should be given to what strategic investment is needed to support the creation of national facilities. This will establish the UK as the global leader in such large-scale facilities and, critically, in innovative products and services emerging from the research conducted in these globally unique research infrastructures.

Appendix: Data Sources

The following data sources were used for verification and validation of information from centre or project websites or press releases.

Country	Data Sources
EU H2020	EU's official CORDIS website
France	There was no information available from centralised government sources. For all funding we used the project websites and the INRIA figures are estimated from annual reports.
Germany	Federal ministry website for official figures including BMBF or the DFG. This information was not available for ATHENE, Helmholtz (CISPA III) and Max Planck. The figures for those centres come from media sites or the centres' websites.
Israel	There was no information available from centralised government sources. The figures are primarily derived from a news article, apart from The Center for Cyber Law and Policy at the University of Haifa, where we used a report from the University's President.
Singapore	National Research Foundation's website
UK	EPSRC Grants on the Web and UKRI Gateway to Research. The exceptions are: 1) the SICSA funding that is reliant on a figure in a document from the Scottish Funding Council; 2) for the two recent ACE-CSRs at De Montfort University and Northumbria University no figures were available. Based on previous ACE-CSR funding, we assumed them to have a proportional allocation, which is included in the UK figures.
USA	The vast majority were cross-referenced and derived from the National Science Foundation's website, with extra validation from the USA Spending website. Those from DARPA were derived from USA Spending (but are likely missing some data and hence should be assumed to be a lower bound rather than an upper bound). The Lablets were identified primarily through university websites (similar to DARPA, these should be assumed to be a lower bound rather than an upper bound).

Table 2: Summary of data sources used for verification and validation.

Funding for this research

The research presented in this report was funded by the National Cyber Security Centre (NCSC).

Conflict of interest statement

The work is strictly the authors' own and no influence has been exerted or input provided by the NCSC on the analysis, recommendations or any parts of the text. The authors are active researchers in the field of cyber security and receive funding from various sources, including the NCSC and EPSRC. In order to avoid bias, only data and sources for which we could find traceable evidence are included in the analysis and recommendations limited to the trends and themes observed in the data.

Acknowledgements and credits

The authors are thankful for the contributions made by Dr. Andrew Dwyer, Dr. Brittany Davidson and Dr. Louise Evans, all from the Bristol Cyber Security Group at the University of Bristol. Drs. Dwyer and Davidson undertook data collection, initial analysis and prepared various visualisations (including the ones included in this report) to support the analysis. Dr. Evans managed the project, coordinated the work of the project team and provided comments on the report.

Notes