ktn Global Alliance

UKRI Innovate UK

Connecting for
Positive Change
–
ktn-uk.org/Global

Global Expert Mission US East Coast Cybersecurity 2019

Contact
Dr Nee-Joo Teh
Head of International and Development
neejoo.teh@ktn-uk.org

Aline Martins
KTM – International & Development
aline.martins@ktn-uk.org

Cyber Attack!

Contents

Welcome

Innovate UK global missions programme is one of its most important tools to support the UK's Industrial Strategy's ambition for the UK to be the international partner of choice for science and innovation. Global collaborations are crucial in meeting the Industrial Strategy's Grand Challenges and will be further supported by the launch of a new International Research and Innovation Strategy.

Innovate UK's Global Expert Missions, led by Innovate UK's Knowledge Transfer Network, play an important role in building strategic partnerships, providing deep insight into the opportunities for UK innovation and shaping future programmes.

In September 2019 the United States East Coast Cybersecurity Global Expert Mission travelled to Washington DC, Virginia and Maryland to better understand the cybersecurity landscape in the US, benchmarking it against the UK's capability.

This report summarises the information and insights gathered during the mission.

1. Introduction

"The US has traditionally been protected from external harm by the physical barriers afforded to it by the Atlantic and Pacific oceans. These physical attributes do not exist in cyberspace, leaving us more vulnerable to attack than at any time in our nation's history."
Larry Clinton - President, Internet Security Alliance (ISA).

The US has long been a world leader in scientific discovery and innovation. It continues to be so today in numerous areas that impact everyone's everyday lives – addressing issues such as cybersecurity, artificial intelligence (AI) and automation. This innovation has been a key driver for economic growth and has helped to address key global challenges, be it poverty alleviation, healthcare or sustainable development. This report identifies the structures, priorities and processes by which the US funds and supports innovation in the key field of cybersecurity. In doing so, it explores the innovation landscape across federal, state-level, research base and private investment communities of the Eastern US.

Background

In recent years, the US has witnessed a shift in how innovation is funded, with the private sector now playing the main role. However, the government still plays a fundamental role as a buyer, operator and regulator of emerging technologies.

The private sector has tended to focus on later-stage development and return on investment, whilst the federal government has maintained an interest in funding basic and early-stage applied research[1].

According to the Information Technology & Innovation Foundation, "private sector firms do not fund basic research because it is high risk—it doesn't readily translate into products in the short term. Firms are simply financially unable to address foundational research problems; research addressing basic and broad research questions lies outside the scope of most private investment." Without federal investments in these research categories, the pipeline of discoveries that enable later-stage development would dry up[2].

Battelle[3] and R&D Magazine[4] projected the 2017 US innovation investment to reach $465 billion, which represents 2.8 per cent of GDP. Industry remains the predominant source (66 per cent) and performer (71 per cent) of US research and development (R&D), with the federal government a distant second at 26 per cent and 12 per cent (when including Federally Funded Research and Development Centres [FFRDCs]), respectively. America's research universities serve a dual role in the national innovation ecosystem as they perform 60 per cent of the nation's basic research and also train the nation's future innovators[5].

The federal government has chosen to make a strategic investment in cybersecurity against a backdrop of increasing threats to both critical national infrastructure and civil society. From 2011 onwards the federal government has developed a strategic plan for research and development in cybersecurity to address some of the underlying fundamental systemic vulnerabilities. This plan is regularly updated through dialogue with all federal agencies through the inter-agency working group.

The mission took place in Washington DC and the states of Maryland and Virginia in the East Coast of the US. This region is one of five cybersecurity clusters in the US and activity in this particular cluster is focused around national security and critical infrastructure, primarily due to the proximity of the federal government and its agencies.

[1] https://www.mitre.org/sites/default/files/publications/pr-15-3060-innovation-landscape-government-future-role_0.pdf
[2] https://www.itif.org/publications/2019/06/13/national-innovation-policies-what-countries-do-best-and-how-they-can-improve
[3] https://www.battelle.org/
[4] https://www.rdmag.com/
[5] https://www.mitre.org/sites/default/files/publications/pr-15-3060-innovation-landscape-government-future-role_0.pdf

The mission sought to meet with members of federal agencies to understand precisely how cybersecurity strategy is guided and more importantly, how innovation takes place and is funded. In so doing, the mission sought to identify where collaboration takes place and how, if it all, it would be possible for the UK and the US to work together. The meetings were with the following government agencies:

- The National Institute of Standards and Technology (part of the United States Department of Commerce)
- The White House Office of Science and Technology Policy (OSTP)
- United States Cyber Command and DreamPort
- Defence Advanced Research Projects Agency (DARPA)
- National Science Foundation (NSF)
- National Security Agency (NSA).

The activities and initiatives undertaken by the state of Maryland and local collaborations have aided success in growing the cybersecurity activity and innovation in the area. The meetings held with the state (both public and private sector actors), were aimed at gaining an understanding of the mechanisms and policies put in place to enable the required collaboration and funding to bring about a critical mass of activity in a region.

This report starts by providing an overview of some of the critical actors within the United States (especially at the federal level). It then looks into some of the activities taking place based on the meetings held during the mission; the sort of funding available and the opportunities for collaboration.

The findings in the report are based on discussions held during a single week with a small number of representatives of the government and private sector in Washington DC and Maryland and Virginia. They constitute a snapshot of the state-of-play in the US cybersecurity market.

2. The United States Cybersecurity Market

Cybersecurity is a big market in the US. In 2013, Americans spent $79 billion on cybersecurity, when the cybersecurity expenditure for the rest of the world was only $83 billion. For the US, this figure gradually increased to $109 billion at the beginning of 2016, due to increased awareness and threats.

The US is expected to spend upwards of $130 billion on cybersecurity tools and services by 2020[6].

There are a number of reasons why cybersecurity is important in the US, especially in today's advanced technology scenario:

- hacks into large companies lead to a loss of revenue and public trust
- seven per cent of organisations in the US lost at least $1 million from cybercrime in 2013 alone
- companies rely on IT systems to protect and relay sensitive information
- Ecommerce is a vital platform in the US that transmits billions of dollars' worth of transactions
- sixty-eight per cent of Americans believe that cybersecurity is important, especially when money and identity theft are on the line.

Due to certain crimes that were committed online, US companies have greatly increased their budgets in cybersecurity to guarantee that the information they store is safe and protected. Every time a cybercrime is committed, it costs, on average, millions of dollars.

Research on a sample of national and multinational companies in 2014[7] in the US shows that the average costs per company of cybercrime can be substantial. The costs specified below are a snapshot of the sample of multinational companies by sector and the average costs incurred by the companies within each of those sectors.

Sector	Costs per company
• Utilities and energy	• Approximately $27 million. This industry is a common target for hackers since it has the potential to disrupt the US economy.
• Defence	• Approximately $22 million.
• Financial services	• $20 million. This sector is often targeted by hackers. Thus, $2,500 per employee is invested in cybersecurity and 5.5 per cent of the industry's IT budget is dedicated to it.
• Technology	• About $14 million.
• Communications	• Approximately $13 million.
• Transportation	• $10 million.
• Services	• $9 million.
• Retail	• $8 million. Players invest $400 per employee in cybersecurity and devote 4 per cent of their IT budget to cybersecurity.
• Industrial	• $8 million.
• Education	• $8 million.
• Public sector	• $8 million. According to Chief Information Officers, 75 per cent of sector players feel that cybersecurity is a top priority and they would gladly increase the expenditure to support the initiatives.
• Consumer products	• $7 million.
• Healthcare	• Around $6 million. This industry allocates its largest share of IT budget to cybersecurity at 5.6 per cent compared to other industries.

[6] https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/
[7] https://www.allianceexperts.com/en/knowledge/countries/america/the-cybersecurity-market-in-the-us/

The US federal cybersecurity market is valued at $65.5 billion cumulatively over five years (2015-2020)[8]. According to the Networking and Information Technology Research and Development (NITRD) Program, it is the nation's primary source of federally-funded work on advanced information technologies in computing, networking and software[9]. NITRD's cybersecurity and information assurance R&D investments totalled approximately $800 million, or about 20 per cent of its overall budget across the National Science Foundation (NSF), the United States Department of Defence (DoD), DARPA, the United States Department of Energy (DOE), NIST and the United States Department of Homeland Security (DHS). Some of these investments are for developing scientific foundations (both science of security and cross-cutting foundations), maximising research impact (supporting national priorities) and accelerating the transition to practice. The remaining investments are directed towards inducing change in four areas: tailored trustworthy spaces, moving target defence, cyber economic incentives and designed-in security.

During the period 2006 to 2013, the federal spend on cybersecurity measures was $78.8 billion. There have been budget cuts since 2011. However, the current and previous administrations have continued to invest in cutting-edge technology for cybersecurity[10].

Replace para with: In the 2019 Financial Year (FY) the President's Budget included $15 billion of budget authority for cybersecurity-related activities. The US Department of Defence contributed the largest amount to this total. In particular, the DOD reported $8.5 billion in cybersecurity funding in FY 2019, a $340 million (4.2 per cent) increase above the FY 2018. The estimate is that at an aggregate level, civilian cybersecurity spending increased 3.9 per cent in the FY 2019 President's Budget[11].

The US accounts for almost 40 per cent of the global market, with four of the top five global cybersecurity companies headquartered in the US (Symantec, Intel Security, IBM Security and Dell EMC)[12].

Gartner identifies cybersecurity market leaders as companies that have both vision and excellent execution. To keep up with this rapidly evolving market, the top players are likely to be making heavy investments in R&D. Gartner has segmented cybersecurity products into categories. The network security segment dominates the market with a share of 35.1 per cent, with data security (28.4 per cent) and identity and access (19.4 per cent) as the next biggest segments. The cloud security market is growing at a healthy pace. Mobile security is increasingly becoming a much higher priority.

There are 20 major global players in cybersecurity and 15 of these firms are located in North America, namely:

Company	Description
Raytheon	The Raytheon Company is a major US defence contractor and industrial corporation with core manufacturing concentrations in weapons and military and commercial electronics[13].
Symantec	Symantec Corporation is an American software company headquartered in Mountain View, California. The company provides cybersecurity software and services. Symantec is a Fortune 500 company and a member of the S&P 500 stock-market index[14].
Northrop Grumman	Northrop Grumman is an industry leader in all aspects of computer network operations and cybersecurity, offering customers innovative solutions to help secure national critical infrastructure. They employ approximately 120,000 people providing innovative systems, products and solutions in aerospace, electronics, information systems, shipbuilding to governments and the private sectors across the world[15].
Booz Allen Hamilton	Booz Allen Hamilton Inc[16], is a management and information technology consulting firm, headquartered in McLean, Virginia, in Greater Washington DC, with 80 other offices around the globe. The company's stated core business is to provide consulting, analysis and engineering services to public and private sector organisations and not-for-profits. Bloomberg named it "the world's most profitable spy organisation". According to an Information Week piece from 2002, Booz Allen had "more than one thousand former intelligence officers on its staff".

[8] Market Research Media; US Federal Cybersecurity Market Forecast 2017-2022; 23 February 2016. [Online]. Available: http://www.marketresearchmedia.com/?p=206. [Accessed 18 April 2016].
[9] The Networking and Information Technology Research and Development Program; Supplement to the President's Budget, FY 2014; May 2013. [Online]. Available: https://www.nitrd.gov Publica¬tions/PublicationDetail.aspx?pubid=48. [Accessed 19 April 2016].
[10] https://www.allianceexperts.com/en/knowledge/countries/america/the-cybersecurity-market-in-the-us/
[11] https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf
[12] https://www.austrade.gov.au/australian/export/export-markets/countries/united-states-of-america/industries/cyber-security-to-the-united-states
[13] https://www.raytheon.com/
[14] https://www.symantec.com/
[15] https://www.northropgrumman.com/Pages/default.aspx
[16] https://www.boozallen.com/

Company	Description
Cisco Systems	Cisco Systems, Inc[17] is an American multinational technology conglomerate headquartered in San Jose, California, in the centre of Silicon Valley. Cisco develops, manufactures and sells networking hardware, telecommunications equipment and other high-technology services and products. Cisco provides both technology and services to support the cybersecurity requirements of both the public and private sectors and is one of the key suppliers to the US federal government and its agencies.
Dell	Dell[18] is a US multinational computer technology company that develops, sells, repairs and supports computers and related products and services. Dell provides a host of endpoint security solutions along with support services, training and audit.
General Dynamics	General Dynamics is a US multinational IT services provider. They help agencies defend themselves from the increasing intensity of cyberattacks with specialist personnel, key partnerships and a focus on emerging technology and game-changing innovations.
IBM	International Business Machines Corporation[20] is an American multinational information technology company headquartered in Armonk, New York, with operations in over 170 countries. They are one of the most recognisable names in the industry and have prospered through the many IT revolutions to come out continuously as a leading brand. From strategic advisory consulting, incident response, design and deploy services to cloud and managed security services; IBM provides the expertise to stay ahead of cybercriminals. Their security services enable customers to activate global intelligence and innovate.
HPE	Hewlett Packard Enterprise[21] is a US multinational that has seen significant change and growth over the years. It has made a number of acquisitions that see it as it is today – they include Electronic Data Systems and Computers Sciences Corporations, both of whom were technology multinationals in their own right. They provide services for enterprise security and adaptive protection that fortify data's confidentiality, integrity and availability in hybrid IT and at the edge.
Intel	Intel[22] is a US multinational with its origins in the manufacturer of chipsets that form the basis of almost every computer today. Intel provides different security capabilities to secure reconfigurable logic designs, systems and data. These include secure fuse-based and battery-backed root keys, encrypted design bitstream and other key protection, data erasure and glitch-protection features[23].
L-3 Harris Technologies	L-3 Harris Technologies is a merger of L-3 and Harris Technologies. They combined to form the sixth-largest defence company in the United States and the tenth-largest in the world. They provide mission-critical solutions to connect, inform and protect critical systems and networks. They are a leader in tactical communications, electronic warfare and intelligence.
Leidos	Leidos[24], formerly known as Science Applications International Corporation, is an American defence, aviation, information technology and biomedical research company headquartered in Reston, Virginia, that provides scientific, engineering, systems integration and technical services.
Lockheed Martin	Lockheed Martin Corporation[25] is an American global aerospace, defence, security and advanced technologies company with worldwide interests. It was formed by the merger of Lockheed Corporation with Martin Marietta in March 1995. It is headquartered in North Bethesda, Maryland, in the Washington DC area.
Palo Alto Networks	Palo Alto Networks[26] is an American multinational cybersecurity company with headquarters in Santa Clara, California. Its core products include a platform that includes advanced firewalls and cloud-based offerings that extend those firewalls to cover other aspects of security.

[17] https://www.cisco.com/c/en/us/solutions/industries/government/defense-cybersecurity.html

[18] https://www.dell.com

[19] https://www.gdit.com/capabilities/technology-solutions/cyber/

[20] https://www.ibm.com

[21] https://www.hpe.com/uk/en/services/consulting/security.html

[22] https://www.intel.com/content/www/us/en/homepage.html

[23] https://www.intel.com/content/www/us/en/security/products/programmable/overview.html

[24] https://www.leidos.com

[25] https://www.lockheedmartin.com

[26] https://www.paloaltonetworks.com/

The cybersecurity needs of cyber-physical systems (CPS) are also driving innovation. In 2014, Lockheed Martin acquired a cybersecurity company called Industrial Defender that is widely recognised as a leader in securing the control systems managing critical industrial infrastructure. Other leaders in this space include IBM, Siemens, Dell/Secureworks, McAfee and Symantec.

Another key trend in the industry at large is protecting managed security services; according to Gartner "by 2018, more than half of organisations will use security services firms that specialise in data protection, security risk management and security infrastructure management to enhance their security postures"[27]. Over the last five years the United States has seen growth in solutions and services within these areas. This trend is driven by two primary factors:

- Firstly, many organisations lack the sophisticated cybersecurity skills needed to define, implement and operate effective security controls, so they must hire security consulting firms specialising in the required skills.
- Secondly, there is a clear movement away from a protection paradigm, towards a detect-and-respond paradigm, which has resulted in significant growth of man¬aged security services that specialise in mitigation and incident response.

2.1.1 Academic Landscape

A decade ago, there was just a handful of universities that were recognised academic centres of excellence in cybersecurity. The explosive demand for cybersecurity solutions has resulted in vibrant research activities at numerous academic institutions across the US. To date, no clear leader from academia has emerged. Rather, the research landscape has become fragmented, with local connections often setting the direction of academic research and development. For the most part, academia has taken on the role of a fast-follower in many areas (e.g. mobile security) focusing primarily on incremental innovations.

John Hopkins University and the University of Maryland and Baltimore County have (within the state of Maryland) been very successful at supporting the local need from the federal agencies in the state and nearby Washington DC. This has been further enabled by initiatives undertaken by the state government and private industry in the area. NYU, the Universities of Austin and San Antonio, MIT, North Eastern University and Stanford continue to support the local ecosystems and clusters that have formed for cybersecurity in the US.

2.1.2 Active Company Investors in Cybersecurity in the US

Investments into start-ups building technologies supporting and/or enabling the global data revolution have traditionally been strong in the US. This includes investments in innovative start-ups targeting AI, autonomous technology, datacentre and cloud, 5G, next-generation computers and a wide range of other disruptive technologies.

Venture capital investment has been on the rise for cybersecurity companies and, in 2018, it hit $5.3 billion, up 20 per cent from 2017[28].

Other activity to suggest sustained investor appetite includes:

- 2019 YTD saw a total of 105 merger and acquisition (M&A) transactions, totalling $20.9 billion.
- Globally, cybersecurity M&A accounted for a record proportion of information technology deal volume in 2018 and 2019 YTD hitting 5.4 per cent and 5.5 per cent respectively.
- Deal-making in cybersecurity is booming as a result, both in the US and globally – 2018 set a volume record for global cybersecurity M&A at 283 transactions for $49.7 billion.
- Private equity activity has surged even faster than broader M&A. 117 deals closed in 2017 up from 80 in 2016[29].

Some of the key most-active investors include:

Investor	Description
Intel Capital	Intel Capital[30] is a division of Intel Corporation, set up to manage corporate venture capital, global investment, mergers and acquisitions. Since 1991, Intel Capital has invested $12.4 billion in 1,544 companies in 57 countries. In that time frame, 670 portfolio companies have gone public or participated in a merger.
GV	GV[31], formerly Google Ventures, is the venture capital investment arm of Alphabet Inc and provides seed, venture and growth-stage funding to technology companies. The firm operates independently from Google and makes financially-driven investment decisions. One of the areas where their investments are focused is "frontier tech" which means funding a future which will be shaped by advances in AI, robotics and hardware, quantum computing, cybersecurity, food and agriculture and deep tech.

[27] Gartner, Inc.; Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Per cent in 2014 as organisations Become More Threat-Aware; Gartner, 22 August 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2828722. [Accessed 19 April 2016].

[28] Reuters Technology News, January 17th, 2019.

[29] https://www.lincolninternational.com/key-trends-in-cybersecurity-dealmaking/

[30] https://www.intelcapital.com

[31] https://www.gv.com/

Investor	Description
Qualcomm Ventures	Qualcomm Ventures[32] is the investment arm of Qualcomm Incorporated. Founded in 2000, Qualcomm Ventures is a corporate venture capital fund with 140+ active portfolio companies.
In-Q-Tel	In-Q-Tel[33], formerly Peleus and known as In-Q-It, is an American not-for-profit venture capital firm based in Arlington, Virginia. IQT invests in commercially-focused, venture capital-backed start-ups to identify and adapt "ready-soon" technology – off-the-shelf products that can be modified, tested and delivered for use within 6 to 36 months. This ready-soon focus means IQT finds and delivers critical, innovative technology quickly and cost-effectively. They have a specific focus on mission-critical areas including cybersecurity, artificial intelligence and machine learning.
NTT DoCoMo Ventures	NTT DoCoMo Ventures[34] is the gateway for the start-up and venture community in NTT Group. They bring together people of diverse interests in order to create new infrastructure. They offer strong business support and collaboration for the passionate and creative people working at start-ups everywhere. By shoring up efforts together, the aim is to create new value that changes established thinking around the world.
Siemens Venture Capital	The Industry Sector and the Venture Capital Unit of Siemens have launched a new $100 million venture capital fund. Their objective is to identify innovative solutions from which Siemens and its clients can benefit and strengthen business partnerships with key players in industry.

Cyber Security Global Deal Share By Country 2013-2017

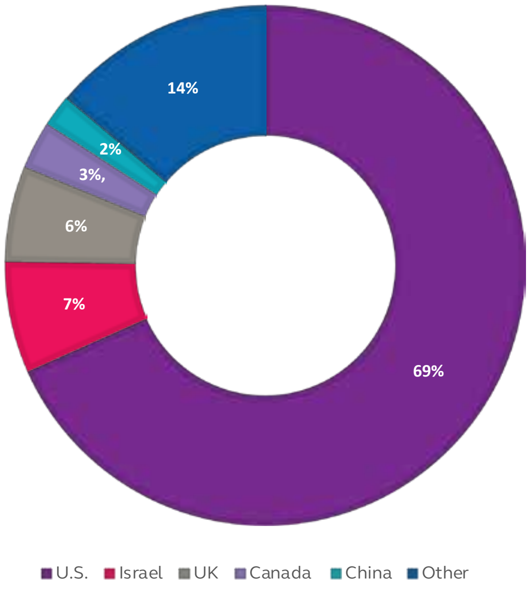


Figure 1 Global Deal Share.
Source: CBInsights, 2018

The US still receives the largest amount of private investment within cybersecurity, with Israel second.

The cybersecurity start-up landscape remains strong with a good spread of companies across the US successful in gaining funding from private and institutional investors.

[32] https://www.qualcommventures.com/
[33] https://www.iqt.org/
[34] https://www.nttdocomo-v.com/en/

2.2 Opportunity

The main opportunities exist across four verticals, primarily:

- Government/defence.
- Financial services.
- Healthcare.
- Critical infrastructure.

The federal government's initiatives to enhance cybersecurity for critical national infrastructure means that they are the biggest spender in the country. Financial services are the largest non-government spender for cybersecurity. The spending in this area is expected to exceed $68 billion by 2020[35].

The impact on healthcare and hospitals from cyberattacks is considerable. The average healthcare organisation spent $1.4 million to recover from a cyberattack[36].

Critical infrastructure is the area with the greatest threat with the potential for the largest impact. The proposed budget for 2020 from the federal government indicates a spend of $20 billion[37].

The capital spent on cybersecurity across these industries is staggering and points to the sheer size and opportunity for companies entering the US market.

2.3 Competitive Environment

The US remains the global leader in cybersecurity. The main activity is focused around five key geographical clusters:

1. The San Francisco Bay area is primarily focused on the technology sector.
2. DMV (Washington DC, Maryland and Virginia) is primarily focused on the defence and government sectors.
3. Massachusetts (Boston) is primarily focused on the healthcare sector.
4. The New York tri-state area (New York, New Jersey and Connecticut) is primarily focused on the financial services sector.
5. The San Antonio-Austin corridor is primarily focused on the defence and infrastructure sectors[38].

Other cities seen as having the potential to reach a critical mass of activity are Phoenix, Arizona[39] and Atlanta and Augusta in the state of Georgia[40]. There are also emerging clusters in Chicago, Colorado (Boulder and Denver), Dallas, Houston, North Carolina (Raleigh-Durham-Chapel Hill), Pittsburgh, Seattle, Southern California (Los Angeles and San Diego) and Tulsa. Most of these are tied to strong research institutions or defence[41].

The emergence of a cluster is about the right blend of people, education and economic factors that leads to a network of businesses and institutions that becomes interwoven and interdependent.

While the US cybersecurity opportunities are abundant, it is a challenging landscape for niche and poorly-integrated solutions to gain traction in this lucrative market. Gartner forecasts a strong consolidation of security offerings in the market; therefore, it is key for organisations entering the space to have a product offering that easily integrates with current systems[42].

[35] https://www.austrade.gov.au/australian/export/export-markets/countries/united-states-of-america/industries/cyber-security-to-the-united-states

[36] https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery

[37] https://www.nextgov.com/cybersecurity/2019/03/trumps-2020-budget-requests-about-11-billion-cyber-defense-and-operations/155445/

[38] https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery

[39] https://www.gpec.org/connected-place/cybersecurity/

[40] https://fortune.com/2017/04/06/cyber-security-cities/

[41] Export markets - United States of America, Australian Trade and Investment Commission, May 2018.

[42] Source: Gartner Report Forecast Analysis: Information Security, Worldwide, 2Q15 Update

3. Background: Policy and Strategy

Roles and responsibilities for cybersecurity are somewhat unclear and fragmented within the US government and its respective agencies. Cyber vulnerability is one of the biggest strategic threats to the country. Whilst the Bush administration took steps to address cybersecurity policy on a national level, for example through the issuance of National Security Presidential Directive 54 in 2008, the issue remained somewhat obscure; indeed, a year later the topic was not even mentioned in President Obama's inaugural speech[43].

Over the following eight years the topic gained further attention, and the Obama administration took a number of great steps to implement a whole-of-government approach to dealing with the multi-faceted cybersecurity threat. Initiatives included the issuance of PPD-41 and Executive Order 13636. The first of these laid out the framework for the US government's response to significant cyber incidents; the second provided a risk-based approach for coping with cybersecurity threats.

Executive Order 13694, which was also issued under the Obama administration, enabled sanctions against malicious cyber actors. Obama used this new executive order to issue sanctions against various nation-state cyber actors, including against North Korea after the Sony hack and, most recently, against Russia for its cyber involvement in the US election. The administration also authorised high-profile prosecutions of nation-state-sponsored cyber actors. For example, the government indicted five Chinese military hackers for espionage against US nuclear, metal and solar companies and brought charges against seven Iranians working for the Islamic Revolutionary Guard Corps who carried out intrusions against the US financial sector and a dam in New York[44].

In addition, the last administration created a Commission on Enhancing National Cybersecurity, which recently issued its report containing useful recommendations to enhance the government's cybersecurity efforts. Others, including think tanks, commissions, commercial companies and academics, have studied the problem and contributed proposals. To date, however, political will has not yet coalesced around one preferred approach and the US government's response to cybersecurity challenges remains largely reactive[45].

A common theme emerging today amongst the federal government and its agencies is the foremost critical need to enhance workforce capability/skills and capacity. Numerous innovations and policy changes are being considered. Among them the following:

- Relaxation of a minimum academic requirement such as a first degree in computer science and moving the focus on to the presence of aptitude, enthusiasm and a willingness to learn.
- Incentivising students to study STEM subjects at university - "Optional Practical Training" for international STEM graduates has fuelled foreign interest in studying in the US over the past ten years. This programme is only a short-term fix, however, which would not be needed if the US talent pipeline were enhanced[46]. This programme gives international students the right to remain after completing their studies to gain practical experience with the hope that they will then stay permanently.
- Promoting and investing in technologies that will automate some of the work of cybersecurity analysts. The technology mentioned most often is AI and machine learning. However, this brings about its own issues – federal systems were not designed to provide the sort of data required; they were never built with AI in mind. Furthermore, there is a skills gap when it comes to data science as well.

[43] https://www.nsa.gov/news-features/speeches-testimonies/Article/1619236/confronting-the-cybersecurity-challenge-keynote-address/
[44] https://www.nsa.gov/news-features/speeches-testimonies/Article/1619236/confronting-the-cybersecurity-challenge-keynote-address/
[45] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf
[46] US Citizenship and Immigration Services; Extending Period of Optional Practical Training by 17 Months for F-1 Nonimmigrant Students With STEM Degrees and Expanding Cap-Gap Relief for All F-1 Students With Pending H-1B Petitions; Department of Homeland Security, 8 April 2008. [Online]. Available: http://www.uscis.gov/iframe/ilink/docView/FR/HTML/FR/0-0-0-1/0-0-0-145991/0-0-0-163040/0-0-0-164807.html. [Accessed 17 April 2016].

3.1 United States Federal Government

The United States National Cybersecurity Strategy of 2018[47] identifies the following priorities:

- Defend the homeland by protecting networks, systems, functions and data.
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation.
- Preserve peace and security by strengthening the ability of the US — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes.
- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable and secure internet.

Success will be realised when cybersecurity vulnerabilities are dealt with effectively through identification and securing of networks, systems, functions and data, as well as detection of and resilience against disruptive or otherwise destabilising malicious cyber activities.

3.1.1 Department of Homeland Security

The DHS Cybersecurity strategy provides a framework to fulfil cybersecurity responsibilities over the coming five years to keep pace with the evolving cyber risk landscape. This will work by reducing vulnerabilities and building resilience, impeding malicious actors in cyberspace, responding to incidents and making the cyber ecosystem more secure and resilient.

DHS has identified the need to find innovative ways to leverage its broad resources and capabilities across the department and the homeland security enterprise to strategically manage national cybersecurity risks.[48] The department has, accordingly, identified five pillars of a DHS-wide risk management approach. This allows them to work to ensure the availability of critical national functions and to foster efficiency, innovation, trustworthy communication and economic prosperity in ways consistent with national values and that protect privacy and civil liberties. These pillars are:

- Risk identification.
- Vulnerability reduction.
- Threat reduction.
- Consequence mitigation.
- Enable cybersecurity outcomes[49].

3.1.1.1 Cybersecurity and Infrastructure Security Agency

On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018[50]. This landmark legislation elevates the mission of the former National Protection and Programmes Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA). CISA[51] builds the national capacity to defend against cyberattacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the ".gov" networks, which support the essential operations of partner departments and agencies.

CISA is responsible for protecting the US critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organisations. Its main activities are:

- Comprehensive cyber protection.
- Infrastructure resilience.
- Emergency communications.
- National risk management centre (NRMC).

CISA performs a similar function in the US to that undertaken by the National Cybersecurity Centre (NCSC) in the UK. The NCSC also:

- Understands cybersecurity and distils this knowledge into practical guidance made available to all.
- Responds to cybersecurity incidents to reduce the harm they cause to organisations and the wider UK.
- Works in close coordination with industry and academic expertise to nurture the UK's cybersecurity capability.
- Reduces risks to the UK by securing public and private sector networks.

Both CISA and NCSC work very closely together as part of the "five-eyes" group of countries and also due to the shared interests and relationship that both countries have. Both countries and these respective agencies cite the following as the main nation threats:

- Russia seeking traditional political advantage by new, high-tech means.
- China conducting cyberattacks on commercial interests, which is being treated as business as usual.
- Intrusions from Iran and attempts to steal money by North Korea. "Both of these nations are prepared to launch aggression digitally in a way they never would dare physically"[52].

[47] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[48] US Department of Homeland Security Cybersecurity Strategy, May 2018.
[49] https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf
[50] https://www.congress.gov/bill/115th-congress/house-bill/3359
[51] https://www.dhs.gov/CISA
[52] https://www.infosecurity-magazine.com/news/ncsc-ceo-vigilance-four/

3.1.1.2 Science and Technology Directorate

The DHS Science and Technology Directorate (S&T) monitors threats and rapidly capitalises on technological advancements, developing solutions and bridging capability gaps at a pace that mirrors the speed of life.

S&T's mission is to enable effective, efficient and secure operations across all homeland security missions by applying scientific, engineering, analytics and innovative approaches to deliver timely solutions and support departmental acquisitions. Created by Congress in 2003, S&T conducts basic and applied research, development, demonstration, testing and evaluation activities relevant to DHS.

S&T strives to address current capability gaps while preparing for future challenges. Projects are organised into six primary focus areas that directly support DHS components, as well as federal, state and local first responders. This includes both cybersecurity and protection of critical national infrastructure.

With respect to cybersecurity, S&T's cyber mission contributes to enhancing the security and resilience of the nation's critical information infrastructure and the internet by:

- Developing and delivering new technologies, tools and techniques to enable DHS and the US to defend, mitigate and secure current and future systems, networks and infrastructure against cyberattacks.
- Conducting and support technology transition.
- Leading and coordinating R&D among the R&D community, which includes department customers, government agencies, the private sector and international partners.

S&T serves a wide range of customers by coordinating and cooperating with partners within DHS, other federal agencies, state and municipal administrations and first responders and private sector companies in a wide range of industries, internet security researchers around the world and universities and national laboratories. S&T creates partnerships between government and private industry, the venture capital community and the research community to build new cyber defence capabilities and identify potential new approaches[53].

To accomplish its mission and serve its customers, S&T funds a wide range of cybersecurity projects aimed at improving security in both federal networks and the larger internet.

Projects cover critical national infrastructure, first responders, federal networks, industrial control systems, supply chain security, 5G and many others[54].

3.1.2 Department of Defence

The Department of Defence's (DoD) cyberspace objectives are:

1. Ensuring the Joint Force[55] can achieve its missions in a contested cyberspace environment.
2. Strengthening the Joint Force by conducting cyberspace operations that enhance US military advantages.
3. Defending US critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident.
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks.
5. Expanding DoD cyber cooperation with interagency, industry and international partners.

The strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the department and cultivate talent[56].

The department recognises that it must innovate to keep pace with rapidly evolving threats and technologies in cyberspace. Success in this domain requires the department to innovate faster than their adversaries.

The private sector owns and operates the majority of US infrastructure and is on the frontline of nation-state competition in cyberspace. In coordination with other federal departments and agencies, the department aims to build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.

Many of the US' allies and partners possess advanced cyber capabilities that complement those held in the United States. The department is working to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities and perspectives. Information-sharing relationships with allies and partners are intended to increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture.

[53] https://www.dhs.gov/science-and-technology/cybersecurity-programs
[54] https://www.dhs.gov/science-and-technology/cybersecurity
[55] https://en.wikipedia.org/wiki/United_States_Joint_Forces_Command
[56] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

3.1.3 Department of Energy

The Department of Energy (DOE) Cybersecurity Strategy lays out a number of specific things that are required in order to ensure the enterprise-wide success of our collective cybersecurity mission:

- Sharing cyber threat data in near-real-time, as well as mitigating those threats by expediting and elevating the analysis of that data using US intelligence assets.
- Developing common identity services to allow better collaboration and visibility.
- Partnering with fellow federal agencies to identify and implement best practices.
- Fully implementing Continuous Diagnostics and Mitigation (CDM) tools across the enterprise to provide scalable, risk-based, cost-effective cybersecurity solutions.
- Enhancing DOE's Integrated Joint Cybersecurity Coordination Centre (iJC3) to ensure enterprise visibility in real-time to stay a step ahead of our adversaries.
- Working to build a system that connects everyone at DOE in the cloud, while safeguarding internal communications and sensitive data.
- Implementing a cyber risk management framework to prioritise investments and improve our responses to rapidly evolving threats.
- Continuing to identify, investigate and mitigate threats posed by individuals and organised threat actors.
- Combating targeted phishing, denial of service attacks and the introduction of malware into our systems.
- Continuing to leverage the work of our National Laboratories as they accelerate their development of innovative cybersecurity capabilities[57].

The Cybersecurity Strategy and Implementation Plan is designed to manage transformational change, improve outcomes and establish a sustainable cybersecurity future. This strategy is structured around:

- mission alignment
- customer and stakeholder alignment
- process alignment
- resource management alignment.

3.1.4 Department of Commerce

The Commerce Department Office of the Secretary, leveraging the expertise of the National Telecommunications and Information Administration (NTIA), the Patent and Trademark Office (PTO), the NIST and the International Trade Administration (ITA), has created an Internet Policy Task Force to conduct a comprehensive review of the nexus between privacy policy, copyright, global free flow of information, cybersecurity and innovation in the internet economy. Recognising the vital importance of the internet to US innovation, prosperity, education and political and cultural life, the Commerce Department has made it a top priority to ensure that the internet remains open for innovation. The newly created Internet Policy Task Force is working to identify leading public policy and operational challenges in the internet environment. The Task Force leverages expertise across many bureaus, including those responsible for domestic and international information and communications technology policy, international trade, cybersecurity standards and best practices, intellectual property, business advocacy and export control.

They are working to lay the foundation for a longer-term, more secure vision by working with industry to set expectations and back them up with the relevant tools. Government can play a key role in helping an organisation know what to do the first time someone knocks on their door and says "your technology is vulnerable"[58].

3.1.4.1 Aspirations

Traditional certification regimes are built around static risk. Cybersecurity risks constantly evolve; things that were certified as secure yesterday may well be insecure tomorrow. We need new mechanisms of governance and new market mechanisms to capture this evolving risk[59].

"Security by design" is a critical aspiration. The Department of Commerce has been working with industry to leverage existing forces towards a more secure ecosystem. Progress is envisaged once a clear pathway has been identified toward an adaptable, sustainable and secure technology marketplace.

3.1.5 Cybersecurity and Information Assurance Interagency Working Group

The Cybersecurity and Information Assurance Interagency Working Group (CSIA IWG) coordinates the activities of the CSIA programme component area. CSIA agencies focus on research and development to prevent, resist, detect, respond to and/or recover from actions that compromise or threaten to compromise the availability, integrity or confidentiality of computer- and network-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems,

[57] https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf
[58] https://www.ntia.doc.gov/speechtestimony/2018/remarks-deputy-assistant-secretary-rinaldo-oecd-global-forum-digital-security
[59] https://www.ntia.doc.gov/speechtestimony/2018/remarks-deputy-assistant-secretary-rinaldo-oecd-global-forum-digital-security

financial systems and air traffic control networks. These systems also support national defence, national and homeland security and other vital federal missions and they constitute critical elements of the IT infrastructure. Broad areas of concern include internet and network security, confidentiality, availability and integrity of information and computer-based systems, new approaches to achieving hardware and software security, testing and assessment of computer-based systems security and reconstitution and recovery of computer-based systems and data[60].

[60] https://www.ntia.doc.gov/speechtestimony/2018/remarks-deputy-assistant-secretary-rinaldo-oecd-global-forum-digital-security

4. Engagement Activity during the Mission

This chapter of the report highlights the mission's visits, with key areas of focus identified.

4.1 Federal

4.1.1 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST)[61] was founded in 1901 and is part of the US Department of Commerce. NIST is one of the world's oldest physical science laboratories. Congress established the agency to remove a major challenge to US industrial competitiveness at the time, a second-rate measurement infrastructure that lagged behind the capabilities of the UK, Germany and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials and computer chips, innumerable products and services rely in some way on technology, measurement and standards provided by NIST. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations.

NIST's cybersecurity programme is seen as supporting its overall mission to promote US innovation and industrial competitiveness by advancing measurement science, standards and related technology through research and development in ways that enhance economic security and improve quality of life.

The need for cybersecurity standards and best practices that address interoperability, usability and privacy continue to be seen as critical. NIST's cybersecurity programmes seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the ability to address current and future computer and information security challenges.

NIST runs open calls to encourage collaboration with the private sector, which mostly involves academic institutions. They engage with industry to understand what threats are concerning to industry and what additional aspects need to be covered by future versions of the Cybersecurity Framework.

The work of NIST is primarily guided by presidential executive orders to which is NIST is tasked with responding.

Key topics of interest in cybersecurity, according to NIST, are:

- supply chain risk management - specifically CNI
- quantum
- SME business engagement
- privacy
- IoT
- workforce and education
- reputational risk.

4.1.1.1 The NIST Cybersecurity Framework

The NIST Cybersecurity Framework[62] is made up of standards, guidelines and best practices to manage cybersecurity-related risk. The framework responds to a President-issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The order directed NIST to develop this framework and the Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 role in doing this work.

The framework seeks to address the lack of a comprehensive standard with widespread applicability when it comes to security. There are major differences in the way companies are using technologies, languages and rules to fight hackers, data pirates and ransomware.

The framework was only seen as a set of guidelines under the President Obama administration. However, under the President Trump administration and through his executive order, the standard is now mandatory for all public bodies and is being widely implemented in government offices and agencies.

The framework core[63] defines the activities that should be carried out in order to achieve the cybersecurity results. There are four specific elements to this core:

- Functions: The five functions outlined in the NIST Cybersecurity Framework are identify, detect, protect, respond and recover. These are the most basic cybersecurity tasks.

[61] https://www.nist.gov/about-nist
[62] https://www.nist.gov/cyberframework
[63] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- Categories: For each of the five functions, there are categories that are specific challenges or tasks that must be carried out.
- Subcategories: These are the tasks or challenges associated with each category.
- Informative sources: These are the documents/manuals that detail specific tasks for users on how to do things.

The framework further specifies four implementation tiers – each tier reflects a level of compliance.

NIST hosts events with stakeholders which help them to understand how people are using the framework and they welcome UK involvement from government and industry.

They provide support to industry not only via the framework but also the National Cybersecurity Centre of Excellence. This centre seeks to help industry find solutions using existing standards.

4.1.1.2 National Cybersecurity Centre of Excellence

The National Cybersecurity Centre of Excellence (NCCoE) is a centre within NIST. Its main purpose is to accelerate businesses' adoption of standards-based, advanced security technologies. The primary services provided by the centre include[64]:

- Consulting with IT security professionals and other leaders to identify the most pressing cybersecurity issues.
- Developing technical descriptions of the problems and mapping the desired solution to NIST and the most appropriate industry standards and best practices.
- Seeking engagement from the public to make the problem descriptions as broadly applicable as possible.
- Engaging with technology vendors to collaborate with them: The products form modules in the end-to-end example solutions that are built in the labs.

Each project results in a freely-available NIST Cybersecurity Practice Guide (Special Publication series 1800), which includes information and instructions organisations can use to implement an example solution for themselves. Organisations that want to adopt similar solutions can use products from the collaborating vendors, or products with similar characteristics that fit their budgets and IT infrastructure.

4.1.1.3 National Initiative for Cybersecurity Education

The aim of the National Initiative for Cybersecurity Education (NICE)[65] is to energise and promote a robust network and an ecosystem of cybersecurity education, training and workforce development. There are a number of goals:

- Accelerate learning and skills development.
- Nurture a diverse learning community.
- Guide career development and workforce planning.

The goals are intended to inspire a sense of urgency in both the public and private sectors, strengthen education and training to diversify the cybersecurity workforce and support employers (public and private sector) to address market demands.

The NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for consultation, communication and coordination of policy initiatives and strategic directions related to cybersecurity education, training and workforce development.

4.1.1.4 Applied Cybersecurity Division

The Applied Cybersecurity Division (ACD) is one of seven technical divisions in NIST's Information Technology Laboratory. Its remit is to implement practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the US to adopt cybersecurity capabilities. ACD is known for:

- establishing cybersecurity standards and guidelines in an open, transparent and collaborative way;
- cybersecurity testing and measurement (from developing test suits and methods to validating cryptographic modules);
- applied cybersecurity which applies NIST's research, standards and testing and measurement work.

4.1.1.5 Privacy Framework

The NIST Privacy Framework is under development. NIST envisions that it will be a voluntary tool for organisations to better identify, assess, manage and communicate privacy risks so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.

4.1.1.6 Small Business Cybersecurity Corner

The US Congress has given NIST responsibility to disseminate consistent, clear, concise and actionable resources to small businesses. All resources are free and draw from information produced by federal agencies, including NIST and several primary contributors, as well non-profit organisations and several for-profit companies.

4.1.2 Office of Science and Technology Policy (OSTP)

In 1976, Congress established the White House Office of Science and Technology Policy (OSTP)[66] to provide the

[64] https://www.nccoe.nist.gov/about-the-centre/strategy
[65] https://www.nist.gov/itl/applied-cybersecurity/nice/about
[66] https://www.whitehouse.gov/ostp/

President and others within the Executive Office of the President with advice on the scientific, engineering and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment and the technological recovery and use of resources, among other topics.

OSTP also leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of federal research and development in budgets and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans and programmes of the federal government.

There is coordination with the National Science and Technology Council (NSTC), where there are 12 working groups which meet monthly, with public reports available. This represents an opportunity for the UK. Cybersecurity and associated responsibility is fragmented in the US, and the NSTC presents an occasion when a lot of those responsible come together and therefore provides a single source with which to engage.

Under the Obama administration, there were approximately 250 people in the OSTP. Under Trump, it is down to around 70. This could highlight an opportunity for the OSTP to work more collaboratively with "friendly" international players, especially in areas such as cybersecurity and 5G.

The OSTP oversees the implementation of the Federal Cybersecurity R&D Strategic Plan Implementation Roadmap[67]. The plan is developed by the Networking and Information Technology Research and Development (NITRD) Program's Cybersecurity and Information Assurance (CSIA) Interagency Working Group (IWG).

The four strategic defensive elements of the strategic plan consist of deter, protect, detect and adapt, as defined below:

Deter	The ability to efficiently discourage malicious cyber activities by measuring and increasing the costs to adversaries who carry out such activities, diminishing their spoils and increasing risks and uncertainty of consequences for cyberattacks.
Protect	The ability of components, systems, users and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability and accountability.
Detect	The ability to efficiently detect and even anticipate, adversary decisions and activities, given that perfect security is not possible, and systems should be assumed to be vulnerable to malicious cyber activities.
Adapt	The ability of defenders, defences and infrastructure to dynamically adapt to malicious cyber activities by efficiently reacting to disruption, recovering from damage, maintaining operations while completing the restoration and adjusting to be able to thwart similar future activity.

[67] https://www.nitrd.gov/pubs/FY2019-Cybersecurity-RD-Roadmap.pdf

The strategic plan provides priorities for cybersecurity R&D in alignment with the NIST Framework for Improving Critical Infrastructure Cybersecurity[68], which provides guidance on managing and reducing cybersecurity risk confronted by businesses and organisations.

Artificial intelligence is part of the R&D strategic plan. An AI progress report is in the pipeline to explain what companies are doing today and what their intentions are in the medium-term i.e. the next five years. There is also the ambition for further work on 5G, quantum computing and strategic computing. Security within the context of the supply chain is seen as a major barrier and risk in the area of 5G.

4.1.2.1 Opportunities

The OSTP carries out two major activities of knowledge transfer and coordination. The recognition that cybersecurity is not something that can be tackled in silos and/or by any one nation on their own opens up opportunities for others, especially those in the five-eyes group of countries.

The OSTP regularly runs workshops that are open to others who have something relevant to contribute. The offer to attend was made during the meeting between the OSTP representative and the mission delegates.

4.1.3 National Security Agency

The National Security Agency/Central Security Service (NSA/CSS) leads the US government in cryptology that encompasses both signals intelligence (SIGINT) and information assurance (now referred to as cybersecurity) products and services and enables computer network operations (CNO) in order to gain a decision advantage for the United States and their allies under all circumstances[69].

The NSA is uniquely positioned to make key contributions to the nation's cybersecurity because, through its two missions of foreign surveillance and information assurance, it lives on the cutting edge of the global information space. These twin missions complement each other in a way that enhances the agency's ability to detect and prevent cyber threats.

NSA has end-to-end insight into malicious cyber activity, internet infrastructure and networks, the activities of hostile foreign powers and cyber best practices. Although significant cybersecurity expertise resides elsewhere in the federal government, NSA is often regarded as possessing the leading collection of information security talent in the US government based on the sheer breadth and depth of our focus on the subject[70].

NSA looks for internal partners when looking at cybersecurity. Their priority areas include:

- IoT and edge devices
- ICS – legacy systems and how to protect these
- federal organisations
- 5G
- resilience
- how to apply machine learning into traditional analyst functions.

To engage as a supplier with NSA, the organisation must meet a minimum set of standards, and federal government procurement makes this a requirement. The NSA has already had engagement with ARM and NCSC in the UK. The NSA sets a security profile which represents the minimum requirement for specific technology and encourages adoption by potential suppliers if they are to maximise the opportunity of take-up and endorsement from the NSA.

The NSA needs to have a very close relationship with DHS and OSTP amongst others. These relationships remain unclear in many cases.

NSA R&D funding is targeted at very specific priorities. This is strategic and not necessarily focused on the long-term. Driven by the need to tackle adversaries, the NSA time horizon is always two years or less. Incremental innovation that allows them to "do things better than we have now…" is the main aim.

The growing awareness of China's intelligence and R&D activities has directed the NSA's focus towards 5G. 5G will be huge and hence the security is important.

4.1.3.1 Opportunities

The NSA uses white papers to point to best practice and to indicate what the right approach might be. The UK Industrial Strategy Challenge Fund Initiative on "Digital Security by Design", and more specifically at addressing cybersecurity by making the fundamental infrastructure secure, is seen by the NSA as one of those things that it would be willing to point to in one of its white papers. These white papers often go on to form part of and/or contribute to the standards worked on by NIST.

The NSA works closely with all of its counterparts in the five-eyes countries. The NSA uses testbeds for the evaluation of new technologies, and it has a dedicated research organisation that looks at problems in different areas, for instance, in the fields of assurance and cryptography. This work is often by

[68] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[69] https://www.nsa.gov/about/

[70] https://www.nsa.gov/news-features/speeches-testimonies/Article/1619167/judicial-oversight-of-section-702-of-the-foreign-intelligence-surveillance-act/

commissioning universities and world-leading academics. The NSA would be keen to see this done with the other partners of the five-eyes countries. There is also recognition within the NSA and other federal agencies that they should stay away from looking for solutions where industry can do better.

Another means by which the private sector (national or international) can engage with federal agencies such as the NSA is through collaboration between AI specialists and data scientists for the goal of better-improved intelligence. The NSA is a custodian of considerable data. The DARPA Joint AI Centre is seen as a good example of this form of collaboration.

The NSA also invests in companies that are addressing and/or working on developing solutions that are in line with the federal agencies' strategic agenda. In-Q-Tel is the arm of the NSA that works on these sorts of investments. In-Q-Tel was founded by the CIA. It functions as a not-for-profit and is separate from government, investing in and supporting innovative start-ups who address challenges from the security and intelligence community.

In-Q-Tel has a base in London, so this represents a significant opportunity for new cybersecurity companies in the UK with a focus on addressing challenges relating to national security.

The NSA is interested in how it can engage more on 5G and specifically those organisations and individuals involved in standards like 3GPP. They believe there is the potential for threats to emerge as a result of these standards and are keen to work with those involved to mitigate any risks.

4.1.4 United States Cyber Command

The United States Cyber Command (USCYBERCOM) is one of the eleven unified commands of the US' DoD. It unifies the direction of cyberspace operations, strengthens the DoDs capabilities and integrates and bolsters DoD's cyber expertise. USCYBERCOM is tasked with coordinating the planning and directs, synchronises and coordinates operations to defend and advance the US national interests in collaboration with domestic and international partners.

The five-eyes countries are seen as key partners in the effort to "be the best in this war". Technology transfer agreements already exist with the UK and Australia.

The command has three main focus areas:

- Defending the DoD Infrastructure.
- Providing support to combatant commanders for execution of their missions around the world.
- Strengthening the nation's ability to withstand and respond to a cyber-attack.

USCYBERCOM enhances:

- Capabilities to operate resilient, reliable information and communication networks, counter cyber space threats and assure access to cyber space.
- The cyber force structure, training requirements and certification standards that should enable the services to build the cyber force required to carry out assigned missions.

There is an established process for engagement and partnerships which is invaluable if an external organisation has an offering that meets USCYBERCOMs strategic needs.

4.1.4.1 DreamPort

DreamPort is a combination of state-of-the-art facilities, innovative programmes and imaginative people charged with finding that spark that leads to unparalleled capability for USCYBERCOM and the war-fighters at large[71].

DreamPort is a not-for-profit organisation surviving through donations from its supporters. They tend to work with early-stage companies and/or with products that still need some development to work within the military operational environment. They publish challenges regularly based on their requirements from the agencies which they serve.

The challenge problems can be divided into functional capability (e.g. vulnerability research) and enabling technologies (e.g. machine learning). They are ultimately looking for functional capability, but the underlying solution should integrate one or more of the enabling technologies. DreamPort has an interest in solutions that explicitly demonstrate innovation in artificial intelligence, machine learning, zero-trust networking and quantum computing.

USCYBERCOM issues a set of technical challenges (unclassified) that DreamPort is tasked with fulfilling and engaging with solution providers wherever necessary. These unclassified technical challenge problems are informed by operators who work on the highest priority missions. The technical challenge problems are not requirements for which solutions exist today. Rather, they are significant challenges which will require developers to use existing capabilities in novel ways, add new features, innovate or drive new research.[72] They engage non-traditional organisations to

[71] https://dreamport.tech/

[72] https://www.cybercom.mil/Portals/56/Documents/Technical%20Outreach/Technical%20Challenge%20Problems.pdf?ver=2019-07-02-151118-497

"enable the war-fighter". Whether they come from individuals, small companies, large ones and academia doesn't make a difference.

When tasks and challenges come in, the aim is to return with an answer to US Cyber Command in 2 to 90 days. About 25 to 30 tasks are undertaken in six months. Rapid prototyping is a critical component of this process. This takes the form of a "hackathon with consequences". If you are a UK business and win or exceed criteria, you could get a direct contract with Cyber Command. Jazz Networks[73] is an example of a UK group that; they are being helped through state compliance.

4.1.5 Top Government Cyber Priorities Panel

The delegates attended the Billington Cybersecurity Summit where they heard a panel of representatives of federal government highlight training and skills as the key priority. The efforts to resolve this include:

- Multidisciplinary intake on university security courses is important - looking at people from non-computer science backgrounds - with the aptitude and willingness to take on new skills. They are also tapping into talent from outside the US.
- An increased focus on two-year college and vocational programmes as well as university degrees.
- They are up-scaling the existing workforce to keep in step with the changing threat landscape.
- DHS-Cyber Talent Management System: An agile and innovative personnel system that better-equips DHS to compete for cyber talent with the private sector — speeding up the hiring process, attracting talent from non-traditional educational backgrounds, using innovative tools to assess applicants and offering more flexible performance-based compensation.
- It is critical to encourage personnel to gain private sector experience.
- There is a need to make federal salaries more comparable to what industry pays.
- Hire more veterans and disabled personnel who show aptitude for cybersecurity.
- Find better ways of engaging the workforce such as gamification and experiential learning.

4.2 Academia

4.2.1 John Hopkins University (Institute for Assured Autonomy)

The Institute for Assured Autonomy (IAA) is a national centre of excellence working to ensure the safe, secure, reliable and predictable integration of autonomous systems into society by covering the full spectrum of research across the three pillars of technology, ecosystem and policy and governance. The goal of the IAA is to ensure that autonomous systems will be trusted to operate as expected, to respond safely to unexpected inputs, to withstand corruption by adversaries and to integrate seamlessly into society.

The IAA is leveraging the excellence and knowledge within Johns Hopkins University in autonomous systems alongside creating strategic collaborations with external partners to provide breadth and depth of expertise to accomplish the vision of a trusted autonomous future. They are open to collaborations irrespective of geographical jurisdiction.

There are three core research areas:

- Transport (especially aviation) with organisations like Amazon and Uber. Working towards a certification process with some help on foundational work from NIST.
- Health.
- Smart Cities.

4.2.2 University of Maryland Baltimore County – Centre for Cybersecurity

The University of Maryland Baltimore County Centre for Cybersecurity (UCYBER) is an interdisciplinary university-level centre that unifies UMBC's many cybersecurity capabilities. The centre aims to provide Maryland, the country and their partners with academic and research leadership, collaboration, innovation and outreach in cybersecurity. This is done by streamlining their academic, research, and workforce development and technology incubation activities to advance their position as a leading research university in cybersecurity-related disciplines.

Their approach to cybersecurity is based upon three pillars:

- Education: Providing quality undergraduate and graduate education and workforce development in cybersecurity-related fields.
- Research: Conducting innovative, interdisciplinary and collaborative enquiry into cybersecurity issues from both the technical and social science perspectives.
- Entrepreneurship: Working with industry partners locally and around the world to incubate and grow new cybersecurity companies offering innovative products and services and transfer intellectual capital from research to practice.

UMBC ranks fourth among US research universities in the production of IT degrees and certificates, and it is the largest producer of such graduates within Maryland, Washington DC and Virginia. Thousands of UMBC graduates work in the intelligence community for key federal agencies and their partners[74].

[73] https://www.jazznetworks.com/

[74] https://www.ntia.doc.gov/speechtestimony/2018/remarks-deputy-assistant-secretary-rinaldo-oecd-global-forum-digital-security

4.3 State-level Innovation Support

4.3.1 Maryland

The state of Maryland is promoting itself as the US Capital for Cybersecurity[75]. The following claims are made:

- First in STEM job concentration.
- First in the proportion of high-tech businesses of all businesses in the state.
- Second in the percentage of professional and technical workers.
- Over 35 incubators and research parks.

With Washington DC as the neighbour, Maryland businesses appear to have an edge in federal funding and research. Maryland ranks first among the states in federal R&D obligations and is home to more than 60 federal agencies and twice as many federal laboratories (74) as any other state.

Maryland business people enjoy immediate access to key government decision-makers, foreign embassies and international business leaders. The Baltimore-Washington DC Metropolitan area is the fourth-largest market within the US[76].

Maryland is successful as a cyber cluster, not just for historical reasons and proximity to the military and centre of government, but also because it has evolved over time to successfully align the following:

- academia
- private/public investment
- customers (both federal and public/private military contractors)
- supply chain integration (via Northrop or Dreamport into CyberCommand)
- incubators/accelerators
- focus on industrial challenges via CyberCommand.

The approach taken by the state of Maryland can be seen as a model that the UK and its regions can learn from, (rather than replicate), on aspects such as:

- support to new businesses and start-ups
- policy and incentives to bring a critical ecosystem together
- investment (through the business life cycle)
- academia and its integration with government departments and agencies.

The Maryland Office of Commerce has a Memorandum of Understanding (MOU) with the Midlands Engine in the UK and with Northern Ireland. This agreement facilitates tech start-ups and SMEs from these areas of the UK doing business in Maryland and vice-versa.

4.3.1.1 Cybersecurity Association of Maryland

The Cybersecurity Association of Maryland is a not-for-profit trade association. It plays a facilitating role which allows for:

- interactions between buyers and sellers
- companies looking to hire cyber employees
- speed networking
- thought leadership events (usually in partnership with big businesses like IBM)
- large stadium-size events for buyers and sellers
- helping industry find small companies to work with
- providing help to entrepreneurs to start a business and find buyers - similar business basic to the Cyber 101 programme in the UK
- serving small Maryland based companies e.g. construction companies wanting information on cybersecurity.

The state of Maryland also has a tax-credit scheme which is run through this association.

4.3.1.2 Funding

Maryland companies can tap into a variety of funding and incentive programmes offered by the Maryland Department of Commerce and other partner organisations throughout the state[77].

TEDCO provides entrepreneurial business assistance and seed funding for the development of start-up companies in Maryland's through a variety of programmes. The organisation's mission is to enhance economic development growth through the fostering of an inclusive entrepreneurial and innovation ecosystem. The aim is to discover, invest in and help build Maryland-based technology companies.

TEDCO has a programme to support advanced technology development and commercialisation from research stages through company formations and growth.

The various funding streams include:

- Research grants to universities and certain federal laboratories.
- Applied grants for pilots and proof of concepts before commercialisation of technology.
- Pre-seed, seed, gap and Series A in Maryland based companies.

The funding is intended to be aimed at covering the full technology stack. TEDCO also has a mission to create programmes for where gaps exist in the entrepreneurship ecosystem. TEDCO facilitates expos to showcase Maryland innovation and stimulate further growth.

[75] https://open.maryland.gov/industries/it-cybersecurity/
[76] https://open.maryland.gov/why-maryland/our-strategic-location/
[77] https://businessexpress.maryland.gov/grow/funding-and-incentives

The funding is split in the following way:

- Two pre-seed funds of $25K to $50K – one targeted at rural parts of the state and the second at underrepresented groups i.e. women, veterans and ethnic minorities.
- Seed fund of between $100K and $500K which includes a cybersecurity investment fund.
- A gap fund.
- Evergreen Venture Fund where the early rounds are “convertible notes”[78] and the final funding rounds take equity from the start, although TEDCO never looks to be the main investor or equity holder.

4.3.1.3 Cyber Incubator

The Cyber Incubator is a business incubation programme that offers cybersecurity-related businesses a place to grow. Located at the UMBC research park, the incubator offers technical support from a dedicated entrepreneurial services team, as well as office space that is conveniently located within the Baltimore/Washington corridor. The incubator is primarily aimed at early-stage companies.

4.3.1.4 Cync Program

The Northrop Grumman Cync Programme is a partnership between Northrop Grumman and UMBC, aimed at commercialising technology to help provide protection from a growing range of cyber threats. The programme is designed to build on UMBC’s successful business-incubation framework by offering a “scholarship programme” for companies with the most promising cybersecurity ideas.

Northrop Grumman funds the programme and is a strategic partner, utilising its resources and applying them in a focused way to cultivate companies to develop solutions to counter global cyber threats. The programme is aimed at high-potential, early-stage companies from across the country looking to commercialise and develop their technologies.

4.3.1.5 Soft Landing Programs

iCyberCenter@bwtech[79] is the Global EPIC[80] Soft-Landing programme that offers companies from the other Global EPIC keystones an opportunity to “soft-land” for a trial period. It is located in the Cyber Incubator within the bwtech@UMBC Research & Technology Park. The programme offers:

- Support to access financial resources, engagement with strategic partners and help with updating business models for market opportunities in the US.
- Exposure to global partners and opportunities to pursue clients.
- Advice on market circumstances, academic engagements, immigration considerations and other practical administrative issues.
- Access to shared co-working space and conference rooms.

4.4 Private Sector Support for Innovation

4.4.1 Internet Security Alliance (ISA)

ISA is an association representing a large number of sectors, and members include some of the world’s largest multinationals:

- Unisys
- Raytheon
- Starbucks
- Vodafone
- GE
- Northrop Grumman
- Thomson Reuters
- SAP.

ISA’s mission is to combine technology, public policy and economics to create a sustainable system of cybersecurity. ISA is unashamedly pro-market when it comes to cybersecurity. They believe that government’s traditional regulatory model can never stay ahead of quickly evolving cyber threats. The job must be handled by the market, where a “bottom-line” incentive fuels the work. This viewpoint does have some credibility, in so far as the fact that standards and regulation represent the present day only and cannot be treated as a sole solution.

Regulation and/or standards have to be seen as a starting point and baseline for protection against an increasingly complex threat landscape. The argument made by ISA rests on the fact that the economic incentives for committing a cyber attack are attractive enough for the “threat actors” to continue to “innovate” in order to keep compromising systems for financial gain. There is a need, therefore, to incentivise the private sector to do better in terms of building infrastructure and systems that are inherently secure. Incentives do need some form of government intervention through the creation of either public policy or directives that bring about these incentives.

ISA pushes the notion of a “social contract” as a means of bringing about a public-private partnership. The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity was written and published by ISA in 2016. It covers a range of cross-cutting issues such as educating corporate boards of directors, reforms to the cybersecurity auditing process, how insurance could best be used to transfer risk, how the United States federal government should be restructured for the digital age, resolving tensions between privacy and security and improving public-private partnerships.

It is an attempt to provide a coherent and systemic framework for collaborative action. The overwhelming takeaway is the

[78] A convertible note is a form of short-term debt that converts into equity, typically in conjunction with a future financing round

[79] https://www.bwtechumbc.com/global-epic-soft-landing/

[80] Global community of innovation ecosystems who will collaborate on projects and share expertise through an expanding network of diverse organisations (https://globalepic.org/HomePage)

belief from the authors that advanced technology needs to be integrated with practical economics and thoughtful public policy to create a sustainable system of cybersecurity.

There are clear contradictions in the approach being proposed by ISA. The central tenet of the argument is that government intervention does not work and that the market should be allowed to solve the agreed problems. However, the approach also proposes the need for public policy with respect to incentives and the fostering of public-private partnerships to bring about change at scale.

ISA also fundamentally believes in collaboration, not just within the US but internationally. It is of the view that the current and evolving threats are not going to be solved by any one organisation or nation alone.

5. Primary Public Funding

Funding for R&D comes from multiple sources depending on the particular federal department or agencies strategic objectives or remit. This means that innovation for cybersecurity is funded by numerous entities, including a number of those mentioned in Section 3. Whilst innovation funding from a number of these agencies is strategic for solutions to very specific problems relating to national security and the protection of critical infrastructure, DARPA and NSF have, and continue to fund, more long-term fundamental research with a hope that this work will have a transformational impact.

5.1 Defence Advanced Research Projects Agency

For the last sixty years, the Defence Advanced Research Projects Agency (DARPA) has held a singular and enduring mission; to make landmark investments in breakthrough technologies for the enhancement of national security. Working with innovators inside and outside of government DARPA has managed to deliver on that mission and continues to work to that end.

DARPA aims to explicitly reach for transformational change as opposed to incremental advances. It was at the forefront of the early advances in AI in the 1950s and 60s and supported some of the founding fathers of AI (Marvin Minsky and John McCarthy) in all their early work. It works and operates within an innovation ecosystem that includes academic, corporate and governmental partners.

DARPA programme managers define and propose new programmes they believe promise revolutionary change. Today DARPA is focusing on strategic investments in four main areas:

- Re-think complex military systems: Making weapons systems more modular and easily upgraded and improved.
- Master the information explosion: Deriving insights from big data. They are also developing technologies to ensure that the data and the systems within which critical decisions are taken are all made trustworthy by creating automated cyber defence capabilities and methods to create fundamentally more secure systems.
- Harness biology as technology: This includes programmes to accelerate progress in synthetic biology and master new neuro-technologies.
- Expand the technological frontier: This is the enduring efforts to overcome seemingly insurmountable physics and engineering barriers. Once these problems have been proven tractable, those new capabilities are applied directly to national security needs.

5.2 National Science Foundation

The National Science Foundation (NSF) is an independent federal agency created by congress in 1950 “to promote the progress of science; to advance the national health, prosperity and welfare; to secure the national defence”. NSF is vital because it supports “discovery” research and people to create knowledge. This type of support:

- is a primary driver of the US economy
- enhances the nation’s security
- advances knowledge to sustain global leadership.

With an annual budget of $8.1 billion (FY 2019), they are the funding source for approximately 27 per cent of the total federal budget for research conducted at US colleges and universities. In many fields such as mathematics, computer science and the social sciences, NSF is the major source of federal backing[81].

The NSF issues limited-term grants - currently about 12,000 new awards per year, with an average duration of three years,

[81] https://www.nsf.gov/about/glance.jsp

to fund specific research proposals that have been judged the most promising by a rigorous and objective merit-review system. Most of these awards go to individuals or small groups of investigators. Others provide funding for research centres, instruments and facilities that allow scientists, engineers and students to work at the outermost frontiers of knowledge. The NSF's goals are:

- discovery
- learning
- research infrastructure and stewardship
- provide an integrated strategy to advance the frontiers of knowledge
- cultivate a world-class, broadly inclusive science and engineering workforce and expand the scientific literacy of all citizens
- build the nation's research capability through investments in advanced instrumentation and facilities
- support excellence in science and engineering research and education through a capable and responsive organisation.

Another essential element in NSF's mission is support for science and engineering education, from pre-school through graduate school and beyond. The research that is funded is integrated with education to help ensure that there will always be plenty of skilled people available to work in new and emerging scientific, engineering and technological fields and plenty of capable teachers to educate the next generation.

5.2.1 Cybersecurity Funding

The NSF supports cybersecurity research, and its investments in basic research in this area have resulted in innovative ways to secure information and ensure privacy on the internet. They have led to algorithms that form the basis of e-commerce, software security, spam filtering, amongst other inventions.

This commitment has resulted in the awarding of research grants to the value of $74.5 million (2015) through the NSF Secure and Trustworthy Cyberspace[82] (SaTC program). Projects in this programme aim to enhance security practices and technologies, bolster education and training in cybersecurity, establish a science of cybersecurity and transition promising research into practice in the real world.

The SaTC programme investment includes a portfolio of 257 new projects to researchers, in 37 states across the US. The projects support early-career investigators and early-concept grants as well as collaborative multi-institute broader scope work.

[82] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709

6. Considerations for UK-US Collaborations

The table below outlines the key opportunities identified during the mission for UK-US collaboration in cybersecurity:

Opportunities for Collaboration
• R&D partnerships and collaborations between cyber start-ups are challenging because as young companies they are still vulnerable with divergent strategies and different investor pressures.
• In the US people are confident and less risk averse in comparison to the UK. This is demonstrated by the success of Silicon Valley and the clusters around New York and Boston, where some of the most innovative technologies and world leading companies have come from. Also, due to the size of the market, the US is less likely to depend on other countries for technological development and to generate economic wealth. This means that any collaboration would probably be much harder to successfully initiate except where the UK might have some very niche expertise to offer which would aid the development of technologies in the US.
• The UK is naturally more collaborative with over 90 per cent of its national R&D funding programmes requiring collaboration. Collaboration comes with risks and it is critical that any joint programme understands those risks and takes them into account. Companies have different strategic agendas, investor pressures, technology roadmaps and business plans. Whilst collaborative innovation can prove profitable, it is important to consider how the inherent risks can be mitigated.
• The US cybersecurity sector is well-financed, and start-ups do not struggle to raise finance from private investors. This means that collaboration and the need to access this type of public funding is not a high priority.
• Cybersecurity companies in the US are primarily focused on sales and expanding their routes to new markets. As such it means that collaboration on innovation is not at the forefront of their strategic agendas. Furthermore, the size of the domestic market has the potential to make them more inward looking.
• The US government has been placing increasing pressure on businesses located outside the US to comply with US export and re-export laws such as ITAR. Controlled articles extend to physical goods as well as technical data, software and any associated services.
• Some market opportunities or channels are more difficult than others for UK companies to enter - cybersecurity is a highly-competitive environment in the US especially when trying to sell into financial services and healthcare.

Annex 1

List of UK Participants

Assentian

BT

Darktrace

Department for Digital, Creative, Media and Sports (DCMS)

Digital Catapult

Innovate UK

Knowledge Transfer Network

National Cybersecurity Centre (NCSC)

List of US Participants

Defence Advanced Research Projects Agency (DARPA)

DreamPort

Internet Security Alliance (ISA)

John Hopkins University

Maryland Department of Commerce

National Institute for Standards and Technology (NIST)

National Science Foundation (NSF)

Northrop Grumman

ReFirm Labs

TEDCO

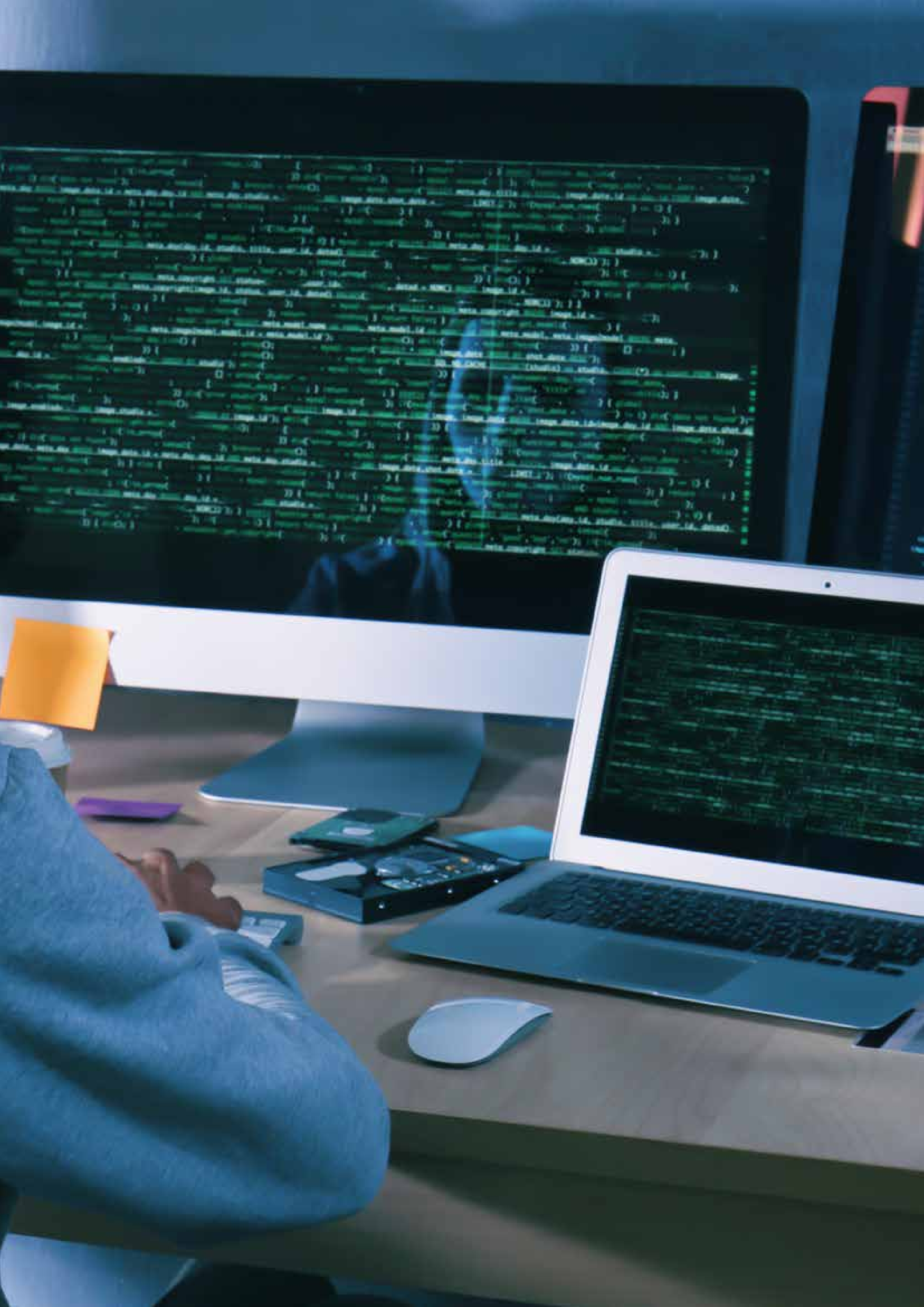
Tenable

The Cybersecurity Association of Maryland

The White House Office of Science and Technology (OSTP)

University of Maryland and Baltimore County

United States Cyber Command



ktn