Alexander Briscall Bowker
17015787
MSIN0032
20th January 2020

Which third-party Computer Vision application(s) should dstl partner with to benefit UK domestic counter-terror?

Part I:

Understanding the current System and scoping the issue

Word Count: 4997

1. CLIENT OVERVIEW

This report is for the attention of:
Dave Walker (Deputy Programme Manager of Autonomy, dstl), and
Paul Kealey (Head of Cyber and Information Systems, dstl)

Dave Walker operates within Paul Kealey's department. Dave is the primary client of this research, based on his current role and previous experience. Dave has led the dstl Cyber Capability Integration program and the Cyber International Collaboration program; whereby his remit was to identify and pursue collaborative opportunities between the UK Ministry of Defence (MOD) and US Department of Defence (DOD). In his current role, Dave is focused on identifying the most suited application areas of Artificial Intelligence[1] technologies for dstl use cases and developing implementation strategies to ensure real value is created for UK defence purposes[2].

2. COMPANY OVERVIEW

The Defence Science and Technology Laboratory (dstl) is an executive subsidiary of the UK MOD. Its goal is to provide advanced Science & Technology (S&T) research for the benefit of UK Defence and Security. For more general information on dstl as an organisation, refer to Appendix 2. Specific to the issues of UK counter-terror, dstl aims to provide specialist technical advice on topics such as how to implement available technology, as well as conduct rigorous analysis and testing of potential S&T resources that can benefit UK counter-terror related organisations[3] – detailed below:

- National Counter Terrorism Security Office (NaCTSO); a police unit that provides advice to the Home Office on counter-terror strategies.
- British Transport Police; a special police force that polices rail networks.
- Departments of the Secret Intelligence Service (SIS); the foreign intelligence service of the UK.
- Departments of the domestic Security Service (MI5).

All of these organisations unite under the common goal of utilising information to help neutralise terrorist activity and promote public safety, as outlined in the UK Government's 2018 agenda 'CONTEST: The United Kingdom's Strategy for Countering Terror'[4].

[1] *Supplementary technological terms defined in Appendix 1*
[2] *Walker via LinkedIn, 2019*
[3] *dstl annual report 2018/19*
[4] *UK MOD, 2019*

3. INTRODUCTION TO THE ISSUE

A significant threat to public safety and security is terrorism; defined as "the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims"[1]. Since 2001, there have been over 100 deaths in the UK resulting from terrorism, with most having taken place in major cities, predominantly Manchester and London[2].

Today more than ever, with massive influxes of people in and around large urban areas, it is becoming increasingly difficult to monitor for potential risks to public safety. London has a current population of over 9 million[3]. With masses of people concentrated in dense public areas, it is increasingly difficult for UK defence and counter-terror organisations to monitor every possible high-risk situation on a real-time basis. It is reported by the UK's most senior counter-terrorism police officer Neil Basu, that in the past two years the number of major terrorist plots foiled has totalled 22[4]. However, this prevention rate is still not perfect, as within that time there have been two major terrorist attacks (Finsbury Park Attack, 2017 and London Bridge Attack, 2019).

Furthermore, the UK is seeing a worrying trend in smaller-scale attacks from lone actors. Because of their low tech and unpredictable nature, these attacks are more difficult to detect and interrupt[5]. The lone actor can launch the attack at their own will, eliminating the need for advanced planning, reducing opportunities for interception and adding spontaneity, which is what makes these attacks so dangerous[6].

Therefore, UK counter-terror organisations, supported by dstl, need to continue to implement more accurate automated techniques to not only flag emergency situations as quickly as possible but also to predict and notify of potential situations before they even occur.

This report aims to present potential applications related to the aforementioned issue and provide a comparative analysis to help dstl become one step closer to understanding the scope of possibility with regard to potential organisations it can partner with to improve its S&T offering for UK counter-terror organisations. However, in order to ensure the relevancy of any applications analysed, this report must first synthesise all factors related to this broad issue (sections 6-9), to define the scope into a more focused problem statement (outlined formally in section 10).

[1]*Oxford Dictionary, 2019*
[2]*Home Office, 2019*
[3]*ONS, 2019*
[4]*Grierson, 2019*
[5]*Laqueur, 2019*
[6]*Cronin, 2019*

4. INTRODUCTION TO THE TECHNOLOGY

There are numerous technological applications that could help support the above issue. One area of technology that has seen promising growth and development is the group of technologies categorised as Computer Vision (CV).

Computer Vision technologies are a sub-domain of Artificial Intelligence (AI) technologies, as illustrated by the hierarchical diagram of Figure 1 below. CV can be defined as enabling computers to gain high-level understanding from digital images or videos. In simple terms, CV is an automated technology that can discern objects or actions present within the visual data that is fed into the system; a visual example is given below in Figure 2. Despite this core functionality, there are many varieties of CV technologies, demonstrated later within this report and furthermore during Part II. For a supplementary glossary of terms technologically related to CV, please refer to Appendix 1.

Based on proprietary research on the Quid® Intelligence Platform, CV technologies in the last five years appear to have received 68% of total funding (as a subset of worldwide technological applications related to counter-terror) and make up 40% of total companies established in this space globally[1]. Furthermore, independent research also points to the future potential of CV technologies. For example, the Hague Centre for Strategic Studies, a think tank for Security Policy for the United Nations, states in its 2018 Artificial Intelligence report that 'Computer Vision & Image Recognition' is one of the three key areas for Governments' future defence strategies[2].

Based on partnering information synthesised from relevant reports with independent Quid analysis, the subdomains of CV that appear to be most relevant to surveillance monitoring and predicting terrorist activity are 'event detection', 'video tracking' and 'object recognition'[3]; this breakdown is illustrated within Figure 3 below.

[1]Quid, 2019 – For the relevant Quid outputs refer to Appendix 3
[2]The Hague Centre for Strategic Studies, 2018
[3]Le, 2018 – For definitions, refer to Appendix 1 and for Quid-related evidence, refer to Appendix 3

Figure 1: *The Hague Centre for Strategic Studies, 2018: An Overview of AI subdomains*

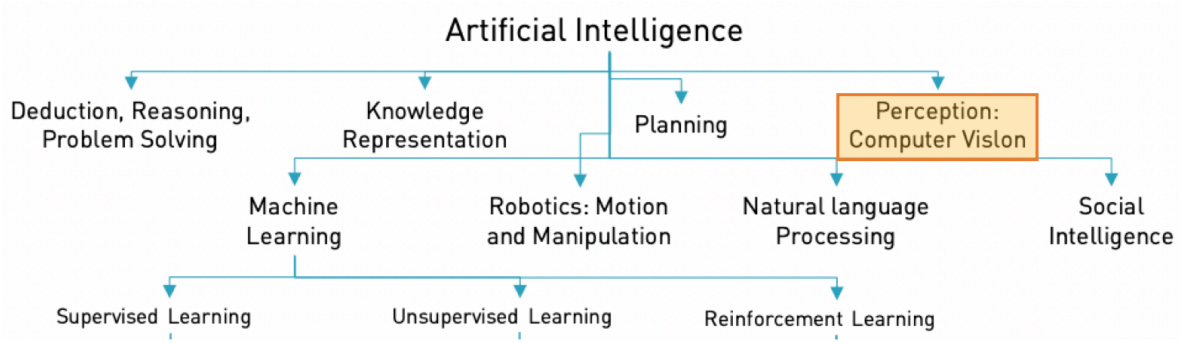
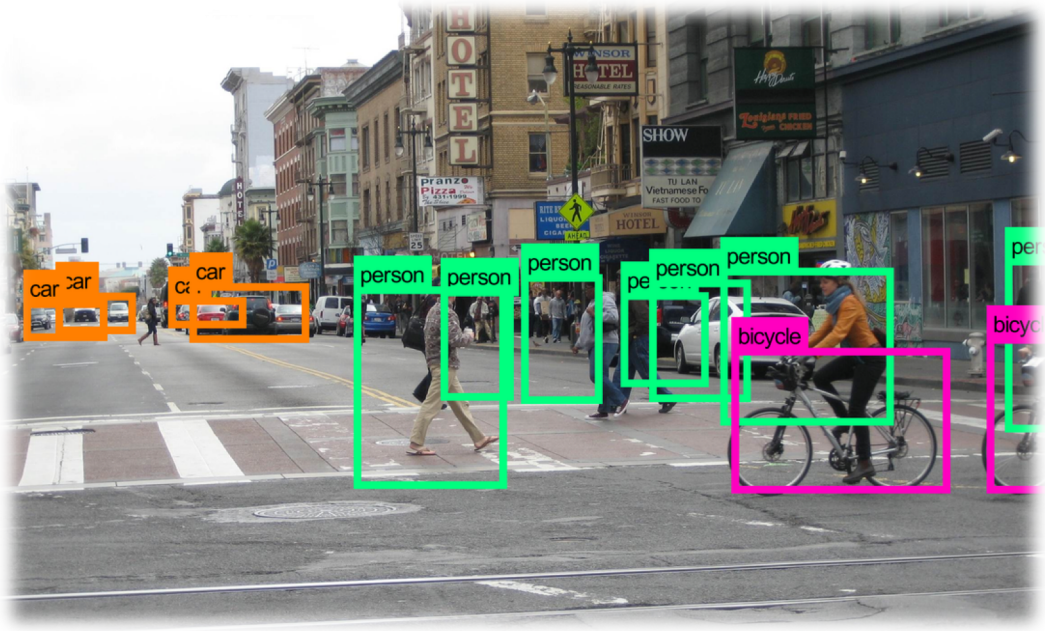
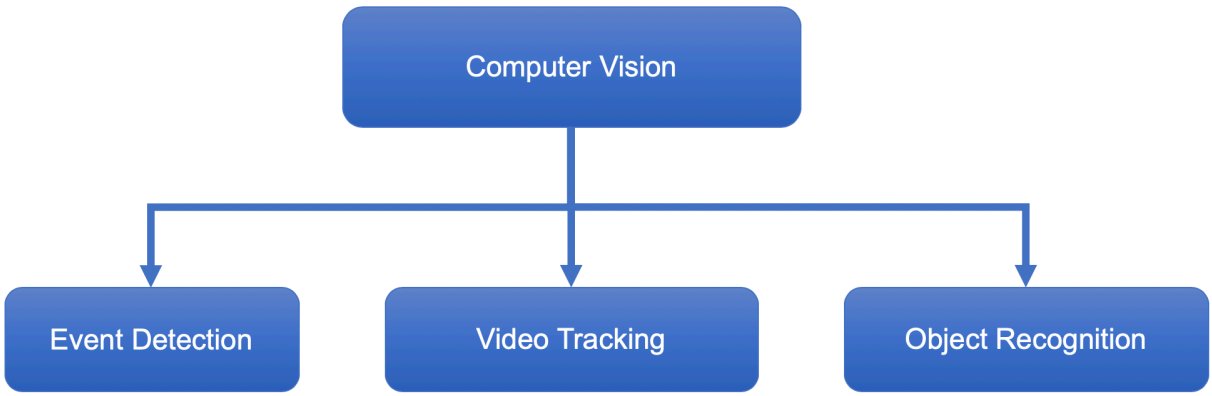


Figure 2: *Visual Demonstration of the Object Recognition Capabilities of CV in Action*



Source: https://www.cvdeveloper.com/projects/machine-learning-technique-for-objects-detection

Figure 3: *Proprietary Diagram Visualising the relevant subdomains of CV*



5. HOW THIS TECHNOLOGY RELATES TO DSTL

The area of capability relevant to CV technologies within dstl's remit, as defined within dstl's 2018/19 annual report, is:

- 'C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)'; delivering S&T for networks, sensors and intelligence integration[1].

dstl is a company that is bound by constraints; such as budget, human capital and time. It utilises technologies and research from third parties, such as organisations working with the current state-of-the-art in a particular technology, to help supplement its own S&T research[2]. Sometimes these third parties can become directly integrated into dstl's S&T supply chain and can help in providing the end value for the organisations dstl serves[3].

Specific to the issue of countering terrorism, dstl currently has no disclosed CV applications it is employing, directly or through partnership. Of course, there may be classified projects in development, yet this report must deduce insights into current dstl activities from publicly available information.

Nevertheless, there is an extensive list of organisations across the world that are developing applications that are directly relevant to dstl within the scope of CV surveillance for countering terror. For example, Anduril Industries is a US-based company that develops a proprietary full-suite surveillance platform that can integrate and autonomously analyse video data from a host of surveillance camera systems. Additionally, TracesAI, another US-based company, develops algorithms that can analyse 2000 parameters of any given person as a more robust alternative to facial recognition[4]. An underlying assumption of this report is that dstl has a greater awareness of organisations operating within the UK; this will be assessed when the current system for partnerships is analysed in section 9. If this assumption holds true, then it is important to incorporate applications from across the globe, that are not country-specific and that can scale to the UK, into this report. This will enable dstl to become more comprehensively aware of the potential application opportunities that are directly relevant to tackling this issue within the UK.

To understand which applications are directly relevant to dstl, we must first understand the organisation's goals and objectives, as described in the following section.

[1]dstl, 2019
[2]Ibid
[3]Aitkenhead, 2019
[4]For further information and more examples, refer to Appendix 11

6. DSTL's CURRENT STRATEGIC GOALS

A prerequisite to any joint venture or partnership with dstl is that the third-party solution is directly in line with the strategic goals laid out by dstl. Therefore, it is necessary that we examine these goals to help us narrow the scope of focus of potential applications so that they are indeed in line with dstl's current strategic focus.

Outlined in dstl's 2018-19 Annual Report, is the 'strategic imperative' of "collaborating more effectively with partners, as well as aiming to increase the number of partners to help deliver S&T capabilities"[1]. This goal directly relates to the capability assessment that dstl also undertook in its annual report. Whereby the nine areas of capability under the remit of dstl[2] are assessed by dstl's internal auditing team for current effectiveness, categorising them as either Green (good health), Amber (needs further, manageable, investment) or Red (poor health and performance).

The relevant capability area, C4ISR (as described in section 5), is in fact classed as Amber for current effectiveness. Inferring that the strategic imperative of increasing the level of investment and partnership for this particular area of capability is necessary.

Therefore, any applications that deliver results for the capability of predictive surveillance fall in line with the current strategic goals of dstl. Though it must be the case that the applications can easily be integrated within the UK's current infrastructure as well as meet the current requirements for partnerships as laid out by dstl, both of which will be examined in the following sections.

[1] *dstl, 2019 – refer to Appendix 4.2 for detail*
[2] *Refer to Appendix 4.3 for detail*

7. THE CURRENT STATE OF INFRASTRUCTURE

With regard to the issue of counter-terror, the main tool currently utilised for preventative surveillance is video surveillance cameras such as CCTV. NaCTSO's 'Protecting Crowded Places' report highlights the importance of CCTV cameras for the purposes of counter-terror surveillance, stating it is a crucial component for the overall protective security measures plan implemented by the UK Government[1].

The use of video surveillance cameras in the UK is common, with approximately 6 million CCTV cameras operational[2]. It is estimated that there are 500,000 of these CCTV cameras within central London and a total of 14,000 operational within the London Underground public transport system[3]. Central London and the Underground system are areas of distinct interest for the analysis of this report, due to the population density of the city as well as the scale of the current infrastructure; it is estimated that an individual within central London is caught on a surveillance camera up to 300 times per day[4].

Despite the extensive coverage of surveillance cameras within the UK, specifically within major cities, there are still current limitations. For example, legal provisions exist that control and restrict the collection, aggregation and retention of information within Government databases. Such that local Governments, intelligence services and police forces that wish to utilise footage from this large network of surveillance cameras must comply with the Surveillance Camera Code of Practice. With the code limiting the retention and storage of the data collected from video streams[5]. Therefore, any application that this report covers should enable real-time monitoring and result in the passive analysis of video footage to avoid any conflicts with the Code, as storing and aggregating the data is not permissible.

Additionally, research suggests that there is a definite need to improve current, traditional CCTV performance. Cumbria Constabulary published their 2017 statistics of CCTV usage over a year, detailing that a total of 4,070 incidents were tagged by CCTV, of which, only 185 incidences were utilised for intelligence purposes and had to be manually identified and submitted by human operators[6]. Highlighting the room for improvement whereby any applications that enable autonomous monitoring and automated flagging of potential situations, objects or individuals of interest could result in substantial improvements.

[1]NaCTSO 'Protecting Crowded Places', 2012 – refer to Appendix 5 for more detail
[2]British Security Industry Association (BSIA), 2017
[3]Transport for London, 2019
[4]BSIA, 2017
[5]UK Government Surveillance Camera Code of Practice, 2013 – refer to Appendix 6
[6]Cumbria Constabulary, 2017

8. DSTL's CURRENT SYSTEM FOR PARTNERSHIPS

The systems outlined and analysed in this section are derived from publicly available sources. It is likely that dstl utilises other channels for acquiring partnerships, that are secretive in nature to ensure their success. This report has collated all the necessary information to ensure that the conclusions drawn here are still insightful, regardless of any secret activities omitted from this report.

In early 2019, dstl announced an investment-partnership fund worth £45 million for small and medium enterprises (SMEs) in the science and technology sectors[1]. The current process for dstl to identify potential organisations is through an event named Venturefest, whereby dstl invites potential SME partners from its compiled list of companies of interest and at the event dstl representatives will be available to meet potential SME partners[2].

Apart from the Venturefest event, the standard procedure for dstl to establish and secure potential partnerships is through the Serapis framework; a framework agreed between the UK MOD and dstl. The framework is intended to enable dstl to access defence technology suppliers that are perhaps overlooked, such as SMEs[3]. According to dstl, there are currently six capability areas, known as 'Lots', that organisations are able to bid on to provide their services through the Serapis framework. The Lot relevant to this report is Lot 1, titled 'Collect': this lot will cover the development and integration of new and emerging ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance)[4].

In the formal online documentation regarding the framework agreement, dstl outlines the current standard practices for suppliers to become potential partners[5]. It should be noted that this framework is ultimately a passive strategy for acquiring partnerships. Meaning that dstl relies on organisation(s) (as the applications can come from single firms or consortiums) approaching the UK MOD or dstl through the Serapis program in order for dstl to become aware of the services the organisation(s) offer and the relevance it may have to dstl's value proposition. Furthermore, the Venturefest initiative appears to fall under a more proactive style strategy, whereby dstl invites partners from a compiled list of interest, yet establishing the list of companies is still dependent on firms becoming aware of the opportunity and then presenting themselves to dstl[6]. Despite dstl accepting partnerships from global organisations[7], both of these current strategies are tailored toward dstl acquiring UK-based organisations – non-UK-based organisations are less likely to be aware of such schemes.

Therefore, if this report can aim to provide a synthesised comparative analysis of the current state-of-the-art in relevant applications of CV technologies across the globe, then this will enable dstl to take a more proactive stance on understanding relevant applications and potential partnerships.

[1]*Cordwell, 2019*
[2]*Ibid*
[3]*dstl Serapis Framework, 2018*
[4]*Ibid*
[5]*This framework is outlined in Appendix 7*
[6]*Cordwell, 2019*
[7]*dstl, 2019*

9. CURRENT TECHNOLOGICAL APPLICATIONS ACCESSIBLE TO DSTL

Due to the secretive nature of in-development projects within dstl, it is hard to clarify exactly what dstl is currently working on. Yet we can look to organisations within the wider UK Government, that dstl has partnered with in the past, to understand what potential applications and capabilities dstl currently has access to. Specifically, we can look to The Alan Turing Institute (ATI) – the UK's data science and AI research centre – to gain a signal of the current state-of-the-art research that dstl has access to. Dstl utilises research from ATI, revealing in a paper that dstl has worked on a joint project for the use of machine learning technology to support cyber security[1].

Currently listed on ATI are 12 ongoing research projects under the technology scope of "Computer Vision". These are listed in Appendix 8.1, yet the two that are potentially relevant to the issue of this report are:

- Detecting hazardous physical activity; the accurate classification of human movement from automated CCTV monitoring to provide early warning for hazards.
- Human action recognition; developing a generalised framework for interpreting human actions[2].

These two projects are explained in more detail in Appendix 8.2.

These two projects are in no way tailored to the issue of counter-terror, with current contextual use cases being factories and street crossings[3]. Yet if the research proves successful and the performance of the models developed surpasses a minimum satisfactory threshold, then the models are flexible enough to be extended to other applications related to surveillance analysis[4].

However, there are reported challenges that are underpinning these projects. Such as the need for an efficient method for representing the streamed surveillance footage to ensure that the application is time-effective and can be performed with realistic computational power[5]. Therefore, if applications that this report aims to cover have demonstrated effectiveness in terms of having an efficient real-time model that is already applied to the domain of counter-terror, then this could be assumed to be better than what is currently accessible to dstl through the generalised research projects of ATI, and hence worth analysing through the rest of this report.

[1] *UKAuthority, 2018*
[2] *The Alan Turing Institute, 2019*
[3] *Ibid*
[4] *Ibid*
[5] *Ibid*

10. THEREFORE, THIS REPORT AIMS TO HELP WITH…

The previous sections of this report have introduced the issue of monitoring terrorism within densely populated urban areas of the UK, as well as outlined the current state of the System associated with supporting potential CV applications, with respect to dstl as an organisation.

We will now strictly define the problem, for which this report aims to provide research and advice for dstl. The resulting problem statement for dstl is:

Which organisations, if any, working within the field of Computer Vision technologies, that dstl does not have a current awareness of, should dstl allocate portion(s) of its £45 million partnership budget to by the end of the year 2020. In order to supplement current dstl research relevant to UK domestic counter-terror predictive surveillance, with use cases focused on automating the monitoring of densely populated public environments[1].

DSTL's KEY DECISION TO BE MADE FROM THIS REPORT

The end goal of this report is to provide a shortlist of assessed organisation(s) that are relevant in meeting the above problem statement. This reduces the passive nature of dstl's current system for identifying potential partnerships and results in the key decision for dstl (namely Dave Walker and Paul Kealey, the clients of this report) to be which out of the final shortlist of organisation(s) should dstl actively engage and discuss potential partnership(s) with.

The next section of this report will focus on identifying how to assess and benchmark relevant applications, in order to ensure effective comparative analysis within Part II of this report.

[1]*Refer to Appendix 5 for NaCTSO's definition of densely populated public environments*

11. HOW THIS REPORT DEFINES SUCCESS

Due to dstl not disclosing any activity, and hence any assessment framework, currently related to this application area, this report must formulate its own way to assess any applications discussed. A simple approach would be to align the analysis of this report with the goal of increasing the UK terror plot foil rate to 100%, as it is a tangible and objective measure of success. However, there are downfalls to this approach. Primarily, there are too many factors and variables influencing this measurement for any causation results to be inferred.

To illustrate this point, the relevant factors that are interrelated to the issue of 'International Security' (a hierarchical key issue area, of which UK terrorism is a sub-domain) have been synthesised, based on research from the World Economic Forum's Strategic Intelligence Platform[1], into Figure 4 below:

Figure 4: *Proprietary Diagram Illustrating a Synthesised Summary of the WEF Transformation Map focused on the key issue of 'International Security'*

[1]*For more on the relevancy of the WEF Transformation Maps for this research, refer to Appendix 9*

As visualised above, the key issue of 'International Security' has interrelated topic areas that can have direct implications on metrics within this umbrella issue, one such metric being the UK domestic terror plot foil rate. For example, any change in Geopolitics could have implicit impacts on the UK domestic terror plot foil rate, and hence utilising this as a benchmark for success when evaluating applications is ill-suited due to the lack of significant and perceivable causation in the measurement.

Therefore, we must look towards frameworks utilised by the UK Government and non-government entities to understand best practices when it comes to measuring the success of potential applications of CV technologies.

The UN Office for Counter-Terrorism implements a 5-step framework for effective monitoring and evaluation of its projects. This is detailed in Appendix 10.1. The main takeaway from this framework is that it assesses the overall quality of implementation of applications, through dimensions such as cost-efficiency and disruption to the current system, rather than against a singular high-level objective, such as the terror plot foil rate.

Additionally, the Canadian International Council's report 'Measuring Success in Countering Terrorism' states that performance of counter-terror applications should always be measured against implementation goals and not over-simplified objectives[2]. In the report, they go on to state that terrorism is not a threat that can be eradicated, but a risk that can be managed and mitigated. Acknowledging that the UK Government recognises this through its CONTEST framework (the UK Government's counter-terror strategy, summarised in Appendix 10.2). This report, therefore, must build upon this framework to ensure effective and relevant implementation goals are laid out.

Furthermore, The UK Health Foundation's 2013 report 'The Measurement and Monitoring of Safety' outlines several industries whereby the goal is also to avoid high-risk situations and the respective frameworks that are implemented. For example, the report outlines the safety practices of the Aviation Industry[4]. Concluding that leading indicators, such as safety management system audits, whereby the quality of the input system is assessed and not an overly ambitious metric[5], result in a more rigorous and effective assessment of safety applications[6].

[2]Gomis, 2018
[3]UK CONTEST Framework report, 2018
[4]The Health Foundation, 2013
[5]Ibid
[6]Ibid

Therefore, a proprietary assessment framework, that builds upon all of the aforementioned frameworks has been developed. This framework will be used whilst evaluating relevant applications. The assessment framework is as follows:

1. Does the application effectively monitor for potential terror-related incidences and does it correctly predict or notify when actual terror-related activity is taking place?

2. Does the application and its effectiveness fall in line with the current counter-terror strategic goals of dstl and the wider UK Government?

3. Does the application supplement current tools and comply with infrastructure guidelines utilised by UK counter-terror related organisations?

4. Is the application available to be utilised by dstl, based on the current scope of the Serapis framework for partnerships?

5. Does the application produce efficiencies with respect to current counter-terror surveillance monitoring that can be translated as cost savings?

The rest of Part I of this report will introduce the issues of objections and alternatives to potential CV applications, to gain a preliminary understanding of what the applications analysed in Part II will need to provide in order to overcome any of these criticisms.

12. DEALING WITH OBJECTIONS TO POTENTIAL APPLICATIONS

There have been public objections to video surveillance applications in the past. For example, the Government Communications Headquarters (GCHQ) – the UK's intelligence organisation responsible for providing signals intelligence – conducted operation 'Optic Nerve' to large public outcry. Optic Nerve was a mass surveillance programme with help from the US National Security Agency (NSA)[1]. The programme collected images from over 1.8 million Yahoo! user accounts, used for experiments in facial recognition and to monitor for known targets[2]. The programme, when reported through whistle-blower leaks, led to large media coverage. The public upset and distrust stemmed from the fact that surveillance had been undertaken without any prior permission. However, this scandal occurred in 2014 and is in contrast with the current Surveillance Camera Code of Practice[3]. Whereby it is stated that all public surveillance cameras must be easily identifiable to potential subjects of a video. Therefore, applications that abide by this code of practice could potentially mitigate this issue of public distrust.

Additionally, the concern of safety versus imprisonment is one that arises consistently when the debate of increasing surveillance techniques is brought up. For example, it was made the key focus during a test run of increased facial recognition surveillance within Romford by local authorities earlier this year. The test resulted in an arrest of a man who was avoiding the newly installed cameras, and this led to civil rights activists to claim that explicit consent must be a fundamental feature of utilising large-scale automated surveillance applications on the UK public[4]. However, there are numerous organisations in the preliminary sample set of relevant applications that attempt to overcome this issue by providing surveillance techniques that do not require intrusive and personalised data collection such as facial recognition[5]. This is simply one example of how state-of-the-art applications can overcome potential objections to implementing such technologies, others will be discussed as they arise during the comparative analysis sections in Part II.

Despite the recent cases of public distrust when it comes to Government Surveillance techniques, it appears that on aggregate the public perception of video surveillance techniques within the UK is now one of positive sentiment; with an overall 60% positive sentiment score from Quid proprietary research[6]. This is an encouraging sign of a potential paradigm shift in public opinion, that may make for any acceptance of potential applications much more plausible. This will be further addressed once a shortlist of application(s) has been developed and analysed in detail during Part II of this report.

[1] *Ackerman, 2014*
[2] *Perlroth, 2014*
[3] *Refer to section 6*
[4] *Murgia, 2019*
[5] *Refer to Appendix 11*
[6] *Refer to Quid output in Appendix 3.5*

13. ALTERNATIVE APPLICATION AREAS

There are indeed alternative application areas for counter-terrorism surveillance within the UK. It is important that the most relevant and credible of these applications are discussed, in order to validate the importance of the applications that will be analysed in this report.

To accrue honour and praise for carrying out a lone wolf attack, perpetrators oftentimes post their intentions on social media before attacking[1]. This provides the opportunity for intelligence agencies to cooperate with social media outlets and monitor information to flag potential perpetrators before attacks occur.

The advancement of Machine Learning[2] has resulted in promising progress for automated models to detect terrorist-related activity on online social platforms, yet there are still considerable limitations. For example, even the most advanced Machine Learning methods lack consideration of visual and social contexts as well as lack automated methods for parsing and cleaning through the massive volumes of output data from social media platforms[3]. Therefore, it is too limiting for counter-terror related organisations to rely solely on such techniques to detect and predict terror-related activities. Real-time surveillance techniques based on visual data must be used in conjunction to help provide a more comprehensive solution.

Of course, this report is not claiming that CV applications can become the single solution to help mitigate terrorist activity within the UK. This section is simply highlighting that a multitude of technologies must be adopted to help supplement the weak points of alternate applications. However, an underlying hypothesis of this research is that the scope of CV technologies defined in the problem statement is the most beneficial and relevant for dstl, and this will be assessed in Part II of this report as individual applications are analysed in detail.

[1]Ganor, 2017
[2]Refer to terminology in Appendix 2
[3]Ahmad, et al., 2019

14. CONCLUSION AND EXPECTATIONS FOR PART II

The research of this report thus far has painted a detailed picture of the current state of the System; the problem domain and related issue components relevant to dstl as an organisation. The most beneficial and relevant application areas will be assessed during Part II of this report as we begin to compare and understand the potential applications relevant to tackling this problem. From preliminary analysis in this part of the report, the application area that appears to be most relevant is the one defined in the problem statement, which is:

Applications that provide passive real-time surveillance analysis utilising equipment that can be positioned in highly populated urban environments to detect or predict terror-related activities.

From proprietary Quid research, 31 organisations were discovered operating within the domain of CV for public safety surveillance[1]. Refining this output and combining with individual research, this report has identified an initial total of 24 organisations that are providing applications that fall in line with the tightly defined scope above. The 24 organisations are tabulated in Appendix 11, with descriptions and supplementary information also included.

The resulting research that is currently planned for Part II of this report is as follows:

1. Examining each of the applications in detail, synthesising the results to provide a shortlist of recommended organisations.
2. Comparing these organisations to alternate application areas, to evaluate whether the application scope defined in section 10 is indeed the most relevant.
3. If the previous results indicate that the shortlist of potential applications is best suited, then implementation plans will be discussed as well as quantification of potential benefits.

This will leave the final decision in the hands of the clients of this report, namely Dave Walker and Paul Kealey, for deciding based on the information provided which of the shortlisted applications (if any) will dstl proactively engage with to discuss potential future partnerships.

[1]*Refer to Quid output in Appendix 3.4*

APPENDICES

APPENDIX 1: SUPPLEMENTARY TERMINOLOGY

Artificial Intelligence – Theories and techniques developed to allow systems to perform tasks normally requiring human or biological intelligence[1].

Cloud Computing – The practice of using a network of remote servers hosted on the internet to store, manage and process data, rather than on a local server or a personal computer[2].

Data Integration Software – Programs that utilise a combination of processes to combine data from disparate sources into meaningful and valuable information[3].

Event Detection – A subset of Computer Vision that is focused on getting machines to provide outputs, given a visual input of an event, in which a perceived level of understanding of what is occurring in the event is shown[4].

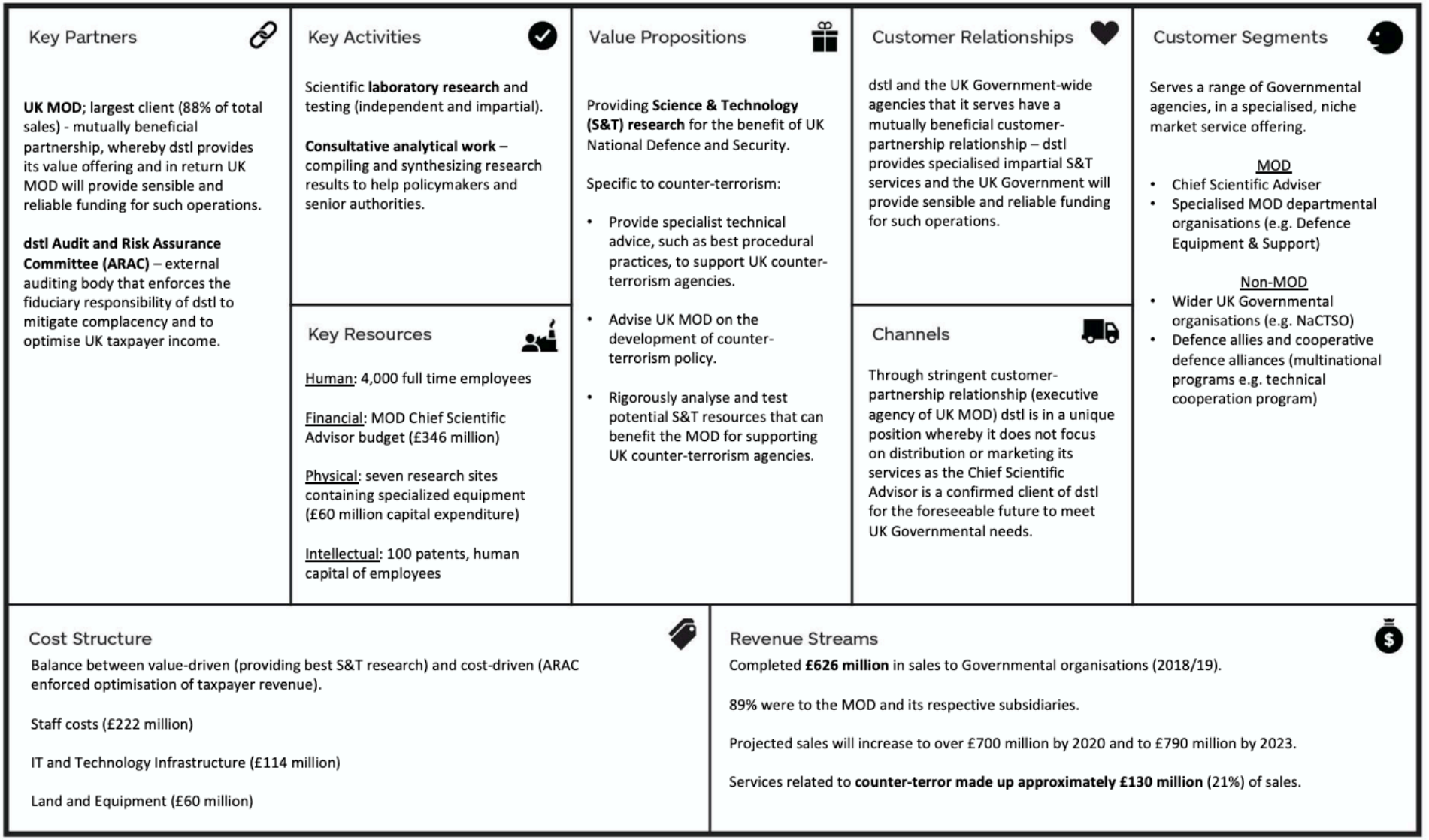
Machine Learning – A field that aims to provide computer systems with the ability to learn and improve automatically without having to be explicitly programmed[5].

Object Recognition – A subset of Computer Vision that is focused on getting machines to provide outputs, given a visual input, that isolate particular subjects and provide classification for these subjects such as though a perceived level of understanding of the subject is shown[6].

Video Tracking – A subset of Computer Vision that is focused on getting machines to isolate particular subjects within a video and follow these subjects throughout the duration of their time being displayed[7].

[1] *dstl "The dstl Biscuit Book" 20193*
[2] *Oxford Dictionary*
[3] *IBM, 2019*
[4] *Morris, 2004*
[5] *dstl "The dstl Biscuit Book" 2019*
[6] *Ibid*
[7] *Ibid*

APPENDIX 2: DSTL's BUSINESS MODEL



Value Proposition

dstl aims to provide advanced Science & Technology (S&T) research for the benefit of UK National Defence and Security. Specific to the issues of UK counter-terrorism, dstl aims to achieve this goal through the below service and product offerings:

- Provide specialist technical advice, on topics such as best procedural practices, and how to implement available technology, to support UK counter-terrorism agencies.
- Advise UK MOD on the development of counter-terrorism policy and on improving the effectiveness of MOD's initiatives through recommended S&T implementation.
- Rigorously analyse and test potential S&T resources that can benefit the MOD with regard to supporting UK counter-terrorism.

Even though dstl is an executive agency of the UK MOD, it aims to act as an impartial and specialist advisor on topics related to science, technology, research and development to help the UK Government meet its needs of providing an effective defence against terrorism threats and helping to ensure public safety.

Key Activities

In order for dstl to execute its value proposition, it needs to perform research and testing to the highest quality, rigorously and independently. This entails scientific laboratory work as well as consultative analytical research on subject matters relevant to meeting the needs of the MOD. Compiling and synthesising the results of the research that dstl produces in order for it to be easily understood and utilised by policymakers and senior authorities within UK Government, MOD and other UK defence organisations is also a key activity for dstl.

Key Resources

Human: dstl has approximately 4,000 full-time employees, with approximately 70% of staff focused on research and technology, and the remaining revolving around business development and operations (*percentages extrapolated from LinkedIn research).

Financial: The MOD Chief Scientific Advisor provides a significant proportion (62%) of dstl funding, totalling £346 million in 2018/19, enabling dstl to carry out its functionalities.

Physical: dstl has over seven devoted sites for research and operations located around the UK. Their headquarters are located at Porton Down, Wilshire – a secluded and highly secretive location where they conduct proprietary research, testing and analysis. Within these areas, dstl owns specialised capital equipment that it requires to perform such analysis and testing, this is highly specialised scientific equipment and laboratories, and each year costs dstl approximately £60 million through capital expenditure.

Intellectual: dstl has recorded over 100 patents over its lifespan (with 39 recorded just in the year 2018/19). This enables dstl to have protection over its proprietary scientific techniques and developments. Additionally, the human capital (skills) of employees at dstl is a key resource for ensuring the best research is conducted.

Partner Network

The UK MOD makes up the largest client that dstl offers its products and services to (88% of total sales provided). This is not a one-way seller-buyer relationship though. The MOD and wider UK Governmental organisations have a mutually beneficial partnership with dstl, through the agreement that dstl provides specialised impartial services and products in line with its value proposition, and the UK Government will in return provide sensible and reliable funding for such operations. Of course, as a subsidiary of a UK Governmental body, there are stringent rules when it comes to this partnership, as optimising the UK taxpayer's money as well as mitigating complacency must be upheld – this is done through external auditing bodies, such as the dstl Audit and Risk Assurance Committee (ARAC).

Customer Segments

dstl serves a range of Governmental agencies, in a specialised, niche market service offering, dependent on specific issues that arise. The main customer of dstl is the MOD Chief Scientific Adviser. dstl's key top-level customer segments are set out below:

MOD
- Chief Scientific Adviser
- Specialised MOD departmental organisations (e.g. Defence Equipment & Support)

Non-MOD
- Wider UK Governmental organisations (e.g. NaCTSO)
- Defence allies and cooperative defence alliances (e.g. multinational programs)

Channels

Through the mutually beneficial customer-partnership relationship that dstl has, it is in a unique position whereby it does not need to focus on how to distribute and market its services to its clients. dstl is positioned as the go-to support for UK Defence related issues for Governmental agencies with regard to Science and Technology research, whereby it conducts its analysis and research at and on its own accord.

Customer Relationships

As previously mentioned, dstl and the UK Government-wide agencies that it serves have a mutually beneficial customer-partnership relationship. Whereby dstl provides specialised impartial services and products in line with its value proposition, and the UK Government will in return provide sensible and reliable funding for such operations.

Cost Structure

As finances are derived from Governmental taxation revenues, dstl needs to find the balance between being value-driven (by providing the best possible research and analysis feasible) and cost-driven (ensuring that expenditure is sensible and reasonable, enforced by such organisations as the dstl Audit and Risk Assurance Committee (ARAC).) Find below a breakdown of the most important monetary costs for dstl in financial year 2018/19:

- Staff Costs (£222 million)
- IT and Technology Infrastructure (£114 million)
- Land and Equipment (£60 million)

Revenue Streams

dstl completed £626 million in sales to the Governmental organisations it serves in 2018/19. 89% of these sales were to the MOD and its respective subsidiaries. Whilst stringent rules are applied by the dstl Audit and Risk Assurance Committee (ARAC) to ensure that taxpayer money is provided to dstl in a smart and efficient way, it is projected that sales will increase to over £700 million by 2020 and to £790 million by 2023. dstl services related to counter-terrorism made up approximately £130 million (21%) of the 2018/19 financial years revenue streams.

(Data Sourced from dstl Annual Report 2018/19)
(Business Model Canvas Structure Interpreted from Osterwalder, A. 2010's Book)

APPENDIX 3: QUID® RESEARCH OUTPUTS

Below are the key outputs from the application scoping analysis, conducted on the Quid® Intelligence platform. A total of 20 distinct searches were conducted, on all three of Quid's databases; Patents, News & Articles, as well as Companies.

APPENDIX 3.1: LIST OF KEY SEARCHES

This first table illustrates searches focused on the News & Articles database, in order to gain an understanding of the current documentation on topics related to counter-terror and automated surveillance.

Search Iteration Number	Database	Boolean Search	Goal of Search	Result
1	News & Articles	("counter terror" OR "terror*") AND "computer vision"	To provide an initial benchmark of the information accessible to my broad key terms.	244 stories, 26% unique
2	News & Articles	("counter terror" * OR "terror" *) AND ("computer vision" OR ("artificial intelligence" AND "surveillance"))	To test whether more focused inclusion of relevant technologies helped improve relevancy.	1.5k stories, 36% unique
3	News & Articles	("counter terror" * OR "terror" *) AND ("computer vision" OR ("artificial intelligence" AND "surveillance")) AND ("united kingdom")	To test the scope and relevancy of the current systems in place, specific to the target country of the UK.	140 stories, 45% unique
4	News & Articles	("computer vision" OR "artificial intelligence" OR "object recognition" OR "event detection") AND ("predictive anal" * OR "surveillance" OR "video anal" *) AND ("counter terror" * OR "terror")	To refine the Quid analysis to incorporate the key sub domains of the technology for which I plan to focus.	558 stories, 32% unique
5	News & Articles	(("artificial intelligence video" ~ 20) OR ("computer vision video" ~ 20) OR "video analysis" OR ("video detect" ~ 10)) AND ("counter terror" * OR "terror")	Realising clustering and defining is better suited to the post search phase, the specificity of the keywords now relates to the problem, rather than the technical features.	891 stories, 16% unique

This second table documents research focused on the Patents database, to gain an understanding of the current state-of-the-art in technological capability.

Search Iteration Number	Database	Boolean Search	Goal of Search	Result
1	Patents	counter terror	To initially scope how many patents were labelled relevant to the broad domain of interest.	8 Patents
2	Patents	video analysis AND detection	To provide a sense of how many patents were identified relevant to the broad sense of the disruptive technology of choice.	1227 Patents
3	Patents	video AND analysis AND surveillance	To iterate on the above search, to ensure the relevancy of the patents returned by the search is increased.	699 Patents
4	Patents	video AND analysis AND surveillance AND detection AND software	To iterate on the above search, to ensure that the patents returned are related to the domain of software for this particular focus point.	9 Patents
5	Patents	camera AND analysis AND surveillance	To 'zoom out' of the previous searches and to test whether a broader term of "camera" is more suitable than "video" for this context.	603 Patents

The third table documents the research conducted on the Companies database, aimed to gain an understanding of companies operating within the relevant scope of the report.

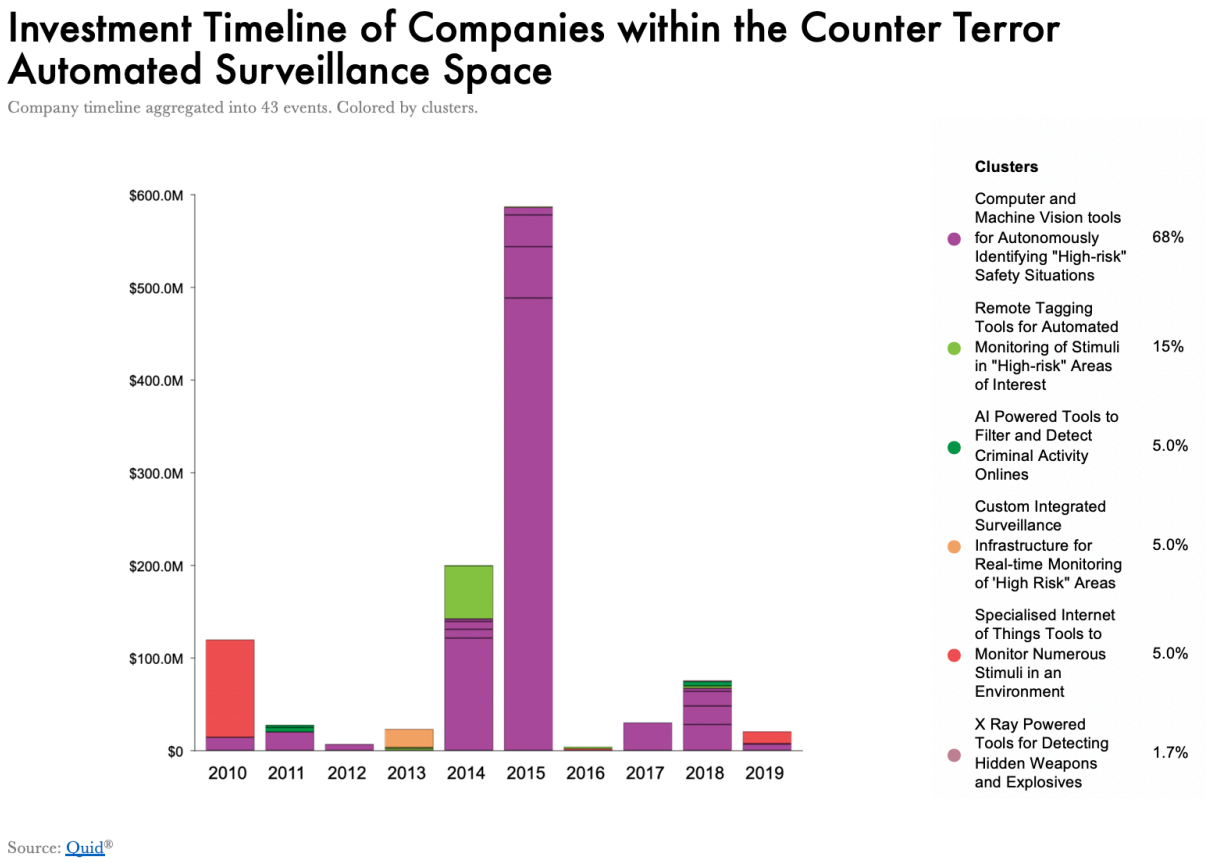
Search Iteration Number	Database	Boolean Search	Goal of Search	Result
1	Companies	counter terror	To gain an understanding of the companies explicitly labelled under the field of "counter terror"	10 Companies
2	Companies	counter terror AND video analytics	To test how many of this initial, very small subset, was in the relevant technological scope. To understand if searching without counter terror as a parameter is more effective.	1 Company
3	Companies	acquirer:("technology laboratory dstl")	To see if within Quid's company database, there were many references to previous ventures undertaken by dstl.	1 Company
4	Companies	video analytics software ~ 10 AND detection	To understand the total number of relevant companies working within the relevant broad domain of technology.	42 Companies
5	Companies	("counter terror" OR ("public" AND "safe" *) OR ("crime" AND "prevent" *)) AND ("detection" OR "prediction" OR "surveillance" OR "prevention") AND tech *	An attempt to enhance above searches. The broad terms such as "public safety" have been broken up to ensure that more companies meet this subset of a generalised search.	81 Companies

The final table illustrates searches on a combination of the different databases, with a focus on understanding potential applications specific to the scoped problem statement that the report develops.

Search Iteration Number	Database	Boolean Search	Goal of Search	Result
1	Companies	("counter terror" * OR "safety") AND ("detection" OR "surveillance" OR "prevention") AND tech *	To provide a benchmark framework for companies operating in the generalised realm of counter terror prevention utilising technology.	252 Companies
2	News & Articles	("counter terror" ~ 5 OR "public safety" ~ 5) AND ("detection" OR "surveillance" OR "prevention" OR "prediction") AND tech *	To provide an understanding of news coverage, relevant to the generalised field of technology for prediction and prevention purposes, with regard to counter terror	3.7K stories, 32% unique
3	News & Articles	("counter terror" ~ 5) AND ("tech" *) AND ("advance" *) AND ("detection" OR "surveillance" OR "prevention" OR "prediction")	To focus in on the news coverage of technological advancements within the large scope of counter terror prediction and detection.	218 stories, 43% unique
4	Companies	("counter terror" OR "public safety" OR "crime prevention") AND ("detection" OR "surveillance" OR "prevention") AND tech *	An attempt to enhance above searches yet include a test to see whether the output of broad linked topic issues such as "public safety" and "crime prevention" are of relevance.	35 Companies
5	Companies	("counter terror" OR ("public" AND "safe" *) OR ("crime" AND "prevent" *)) AND ("detection" OR "prediction" OR "surveillance" OR "prevention") AND tech *	An attempt to enhance above searches. The broad terms such as "public safety" have been broken up to ensure that more companies meet this subset of a generalised search.	81 Companies

APPENDIX 3.2: ANALYSING INVESTMENT IN RELEVANT COMPANIES

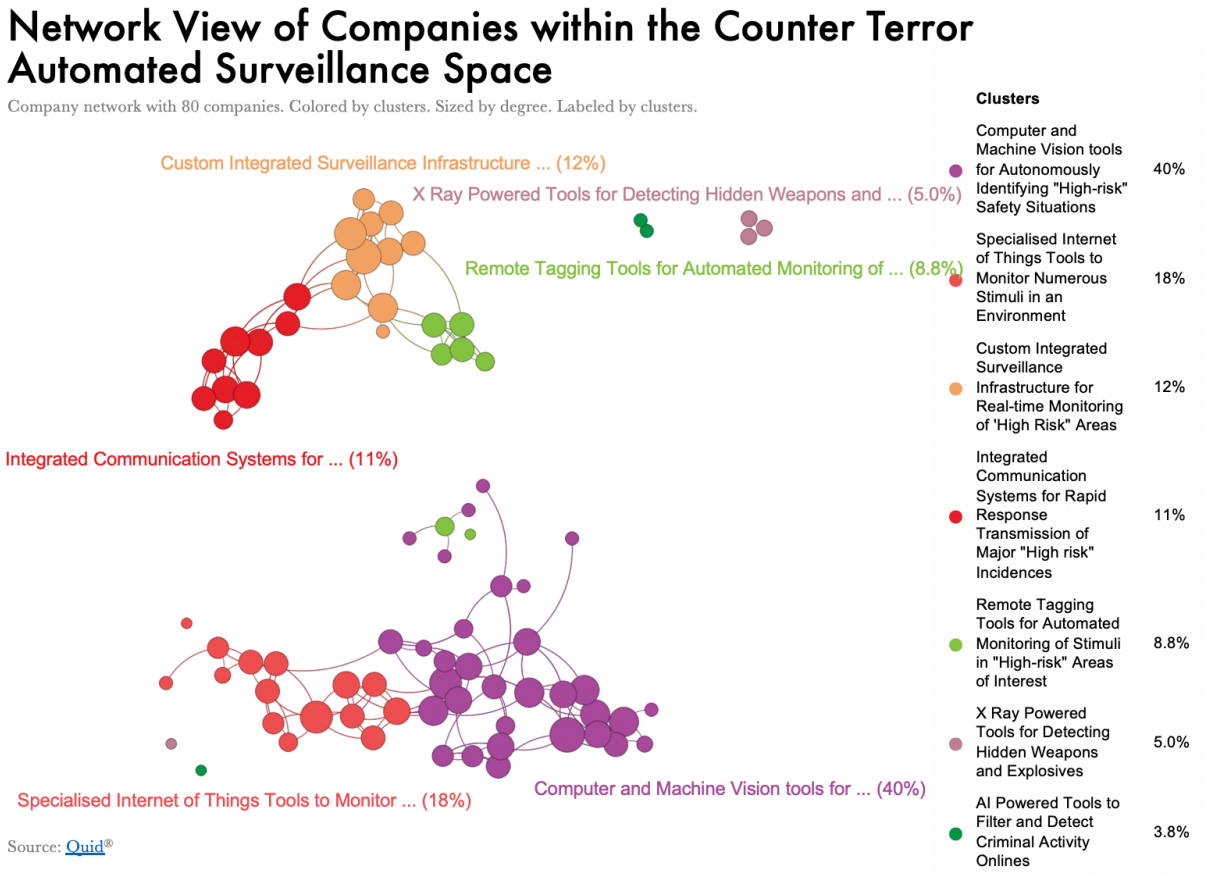
The below Quid graph illustrates total invested amounts in the relevant applications, refined according to the finalised problem statement. The investments are broken down chronologically and categorised by application cluster.



Source: Quid®

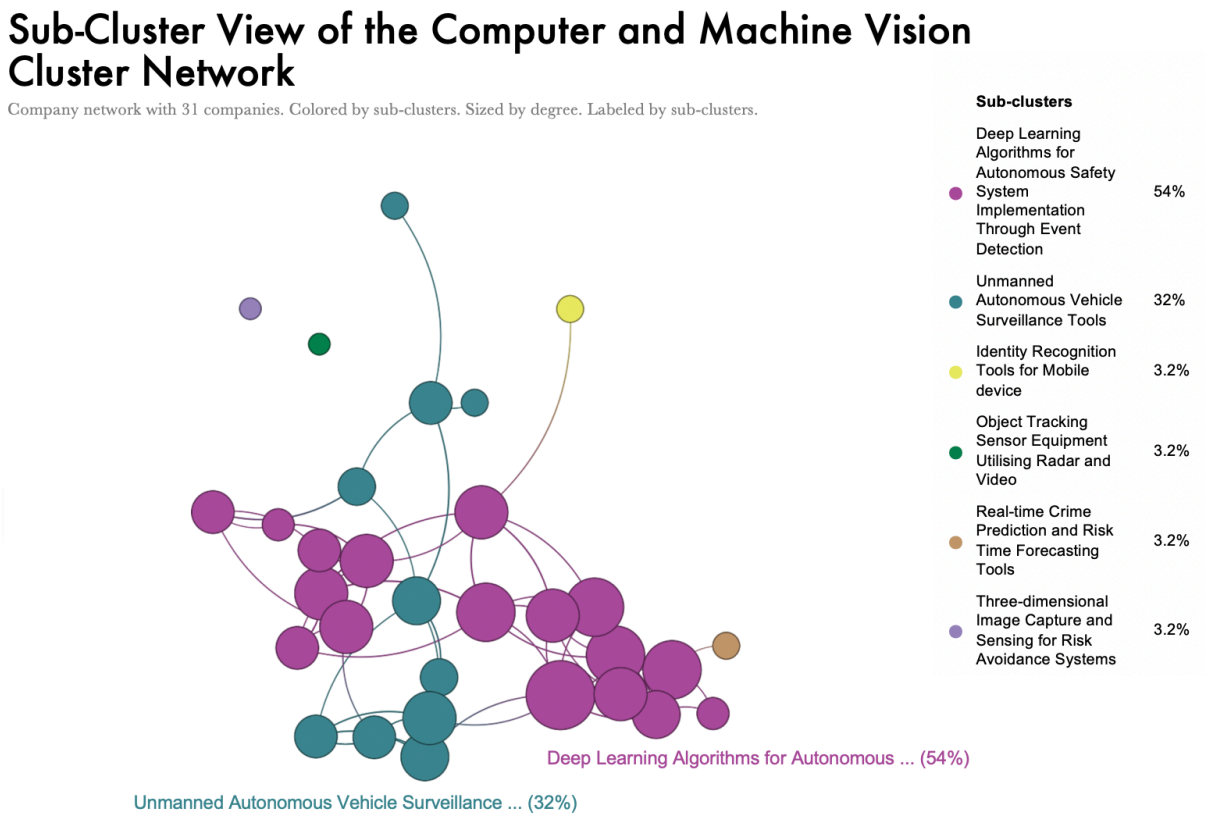
APPENDIX 3.3: UNDERSTANDING THE POTENTIAL APPLICATION SPACE

The below Quid output is a cluster view representing potential applications areas relevant to the issue of this report, defined and categorised by technological application. This output helped contextualise the application area related to Computer Vision and compare it to alternate application areas.



APPENDIX 3.4: UNDERSTANDING THE SPECIFIC APPLICATION SPACE

The below Quid output is a cluster view representing potentially relevant applications. After the problem statement was wholly defined, I refined this output to provide solely relevant applications. This output contributed to the list of 24 relevant application organisations finally identified.



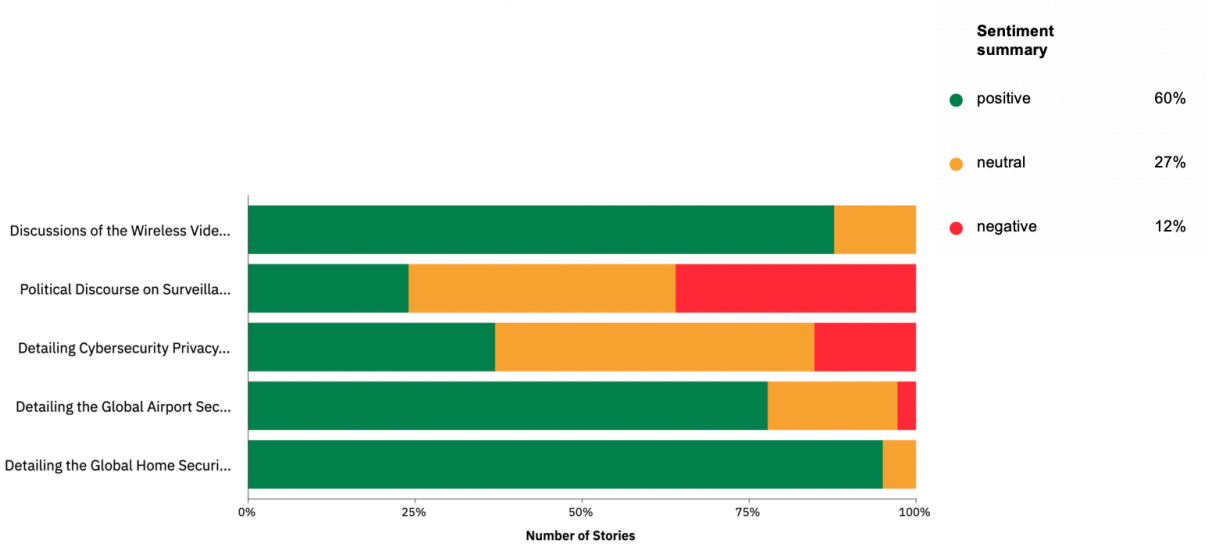
Source: Quid®

APPENDIX 3.5: UNDERSTANDING PUBLIC PERCEPTION OF SURVEILLANCE

The below Quid output provides sentiment analysis based on a focused News & Articles search relevant to automated video surveillance techniques within the UK. The stories are categorised into distinct topic areas, and aggregated sentiment analysis is detailed.

Sentiment Analysis of Articles Detailing Video Surveillance Systems with the UK

News article bar chart with 209 stories. Colored by sentiment summary.



Source: Quid®

APPENDIX 4: UK GOVERNMENT AND DSTL STRATEGIC GOALS

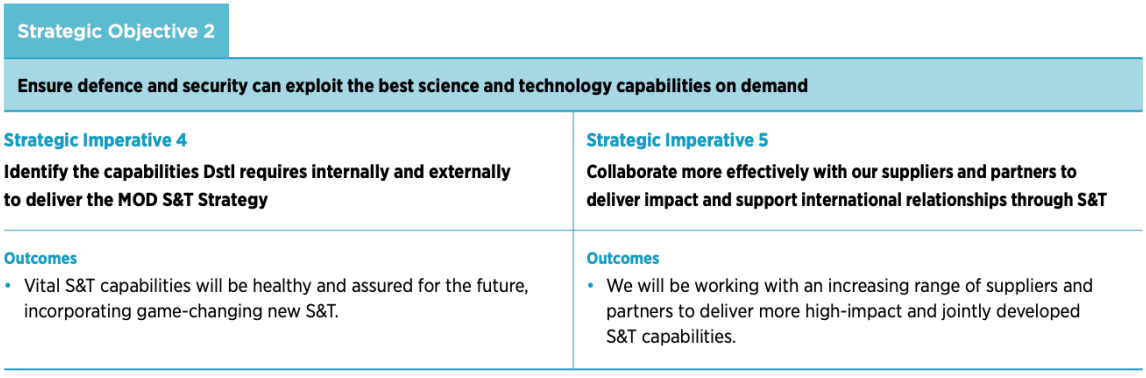
APPENDIX 4.1: UK "GLOBAL" STRATEGIC TRENDS REPORT

Below is a summarisation of the relevant components of the 2018 UK Government's report on Global Strategic Trends that are evaluated to be critical to be accommodated into modern policy and future decision making. The two relevant categories with regard to UK counter-terror are 'Surveillance' and 'Urban Conflict'. These are summarised as follows:

- Surveillance: Technology will play a growing role in surveillance and policing. Facial recognition technology is showing prospect to be capable of monitoring a suspect's every move in public, and the use of algorithms may predict some kinds of criminal activity before they occur. The UK Government must proactively engage to understand all plausible applications and potential benefits for future surveillance technology.
- Urban Conflict: As more people live in cities, urban areas are likely to become more central to conflict. The dense, multidimensional nature of urban environments, with constraints on infrastructure capability and exhaustive surveillance monitoring, means that military and police tactics are likely to require modifications over the coming decades. As techniques look to become more automated and predictive in approach compared to traditional reactive human intervention.

APPENDIX 4.2: DSTL ANNUAL REPORT STRATEGIC OBJECTIVES

Below is an excerpt from dstl's 2018-19 annual report, detailing one of their top prioritised strategic objectives. The objective relates the goal of partnership and collaboration. With a focus on ensuring dstl aims to collaborate more effectively with current and potential partners to deliver on its core value proposition.



Strategic Objective 2

Ensure defence and security can exploit the best science and technology capabilities on demand

Strategic Imperative 4	Strategic Imperative 5
Identify the capabilities Dstl requires internally and externally to deliver the MOD S&T Strategy	**Collaborate more effectively with our suppliers and partners to deliver impact and support international relationships through S&T**
Outcomes • Vital S&T capabilities will be healthy and assured for the future, incorporating game-changing new S&T.	**Outcomes** • We will be working with an increasing range of suppliers and partners to deliver more high-impact and jointly developed S&T capabilities.

APPENDIX 4.3: DSTL CURRENT CAPABILITY ASSESSMENT

Below is another excerpt from dstl's 2018-19 annual report, whereby the nine key capability areas relevant to dstl's core value proposition are defined (left) and on the right is the outcome of the 2018-19 capability assessment. The assessment evaluates current effectiveness and categorises by either Green (good health), Amber (needs further, manageable, investment) or Red (poor health and performance).

Our work focuses on nine key capability areas:

Analysis. We use science and technology to solve complex policy, planning and operational problems.

C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). We develop S&T for networks, sensors and intelligence integration.

CBR (Chemical, Biological and Radiological). We provide authoritative S&T advice on CBR materials, and develop CBR countermeasures.

Counter-terrorism and Security. We deliver S&T to respond to a diverse range of current and future defence and security threats.

Cyber. We find ways to defend against cyber attacks and to outsmart our adversaries in the digital age.

Human Capability. We develop S&T to benefit and enhance the contribution that humans themselves make to defence and security.

Integrated Survivability. We use systems engineering to achieve the best chances of survival for our service personnel and for the successful completion of affordable missions.

Platform Systems. We enable the integration of technologies across the land, sea and air military platforms.

Weapons. We assess and advise on conventional and new weapons technologies and systems.

APPENDIX 5: NaCTSO 'PROTECTING CROWDED PLACES' REPORT

Below is an excerpt from the NaCTSO 2012 report on 'Protecting Crowded Places' – an analysis report providing prescriptive actions for best practices for enhancing public safety on such issues as UK domestic terrorism.

Counter-terrorism design principles	Examples of measures
Better blast resistance	• external barriers or a strengthened perimeter to prevent a penetrative (ramming) or close proximity (parked or encroachment) attack; • use of building materials which reduce the risk of fragmentation including blast resistant glazing and structural design which reduces the risk of building collapse; and • install doors and locks which are better able to withstand entry from armed intruders and provide robust ground floor facade material, which together will help to provide cover for people caught up in a firearms attack.
Better building management facilities	• entrance arrangements which resist hostile entry; • the separation of general heating, ventilation and air conditioning systems for entrance areas, delivery areas and mailrooms from those occupying the main occupied spaces; • air intakes that are in a secure area and above first floor level; • hazardous material stores that are at a safe distance from the building; and • communications systems (eg public address systems) installed to pass on advice to those caught up in a firearms attack.
Better traffic management and hostile vehicle mitigation measures	• structural measures that prevent access to, or close proximity of, unscreened vehicles to the building or space; and • measures that reduce the speed of vehicles approaching the site or its defences, like bends or chicanes.
Better oversight	• clear lines of sight around a building; • absence of recesses on the façade or elevations of a building; • uncluttered street furniture; • well maintained and managed litter-free building surrounds that reduce the opportunity for suspicious hidden items and suspect activity to go unnoticed; • CCTV and security guarding to provide formal oversight; • orientating the building so that it overlooks public space and neighbouring buildings to support informal oversight by those who use and visit the location; and • well-managed access points and reception facilities that offer less opportunity for intruders to go undetected and may deter them from taking further action.

Within the better oversight design principle category, the category most associated with surveillance applications discussed in this report, there is the inclusion of CCTV and safety guarding. Additional measures for this design principle include more external infrastructure and design components of the surveillance techniques, such as the positioning of any cameras and the design layout of any high-risk public locations – these are all important secondary design components that must also be considered when evaluating any relevant applications.

Densely Populated Public Environments Definition: "a location or environment to which members of the public have access that may be considered potentially liable to terrorist attack by virtue of its crowded density".

APPENDIX 6: CAMERA SURVEILLANCE CODE OF CONDUCT

Below is an excerpt from the UK Government's Surveillance Camera Code of Practice, detailing a selection of some of the 12 guiding principles for which all operators of camera surveillance equipment must oblige. Specific to this report are points 6 and 7, whereby there are clearly defined constraints placed on the storage and retention of any data captured by surveillance camera systems.

Guiding Principles

2.6 System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

APPENDIX 7: GOVERNMENT SERAPIS FRAMEWORK

Below is a synthesised summary of the different components of the UK Government and dstl's Serapis framework; the current framework utilised for identifying and acquiring any potential partnerships with third-party technology providers. It is important to mention that the capability areas of dstl are categorised into 'Lots' for the third-party organisations to place their bids. The Lot relevant to this report is Lot 1; **Collect**: the development and integration of new and emerging ISTAR (Intelligence, Surveillance, Target Acquisition, and Reconnaissance).

Bids: The bids for acquiring any potential partnerships are open to any organisation, and could be a single company or a consortium, or an academic organisation.

Funding: The funding is sourced and allocated predominantly from the MOD Chief Scientific Advisor budget (totalling £346 million for 2018/19), as of current the split of funding per lot is still under review.

Review: Once relevant suppliers have been collected, collated and the organisation with the capabilities to potentially best suit the current need of the 'Lots' key issues, dstl will produce a business case for approval.

Approval: Approval is required from the relevant key stakeholders within Governmental Organisations, with the predominant case being the MOD Chief Scientific Advisor.

Collaboration: Regarding the level of collaboration that this framework allows, dstl is still fine-tuning the detailed structure of the framework, yet dstl states that it is 'committed to establishing a framework which fundamentally encourages innovation, collaboration and partnering.'

APPENDIX 8: THE ALAN TURING INSTITUTE RESEARCH INSIGHTS

APPENDIX 8.1: LIST OF ONGOING RESEARCH PROJECTS

Below is a list of all 12 ongoing research projects defined under the technology scope of "Computer Vision" being conducted at The Alan Turing Institute. The bolded two projects are the ones that are implicitly relevant to applications of counter-terror predictive surveillance:

- Solar Nowcasting with machine vision
- Deep learning in electron cryo-microscopy
- Digital twins in aeronautics
- Intuitive human-robot interaction in work environments
- Digital fingerprinting of material microstructure
- AI and inclusion (digital disability accessibility)
- Topological hierarchies in complex image data
- Design change in digital twins
- **Detecting hazardous physical activity**
- **Human action recognition**
- Capturing complex data streams
- Adversarial machine learning (testing with manipulated data)

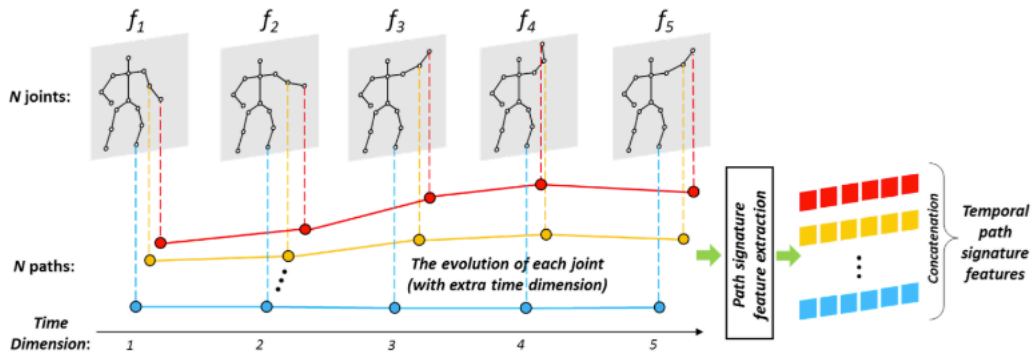
APPENDIX 8.2: DETAILED EXPLANATION OF RELEVANT PROJECTS

Below is further detail on the two projects that are closely aligned to the potential applications analysed in this report.

Detecting hazardous physical activity: The accurate classification of human movement from automated CCTV monitoring of customers in retail environments and of workers performing strenuous tasks. This has the potential to provide early warning for hazards and increase their protection. Cutting-edge deep learning technologies in combination with the technique known as 'path signatures', will allow for the development of domain-specific classifications of different action patterns to improve the safety of these particular contexts.

Human action recognition: The detection and recognition of human actions from real-time CCTV video data streams. This is a popular challenge, with the potential to aid in video surveillance and anomaly detection of, for example, potentially hazardous scenarios in factories. This project aims to efficiently and effectively address this challenge by developing a generalised framework for interpreting human actions, combining cutting-edge deep learning technologies with 'path signatures'. The expected outcome is a high-performance, real-time human action recognition and detection system.

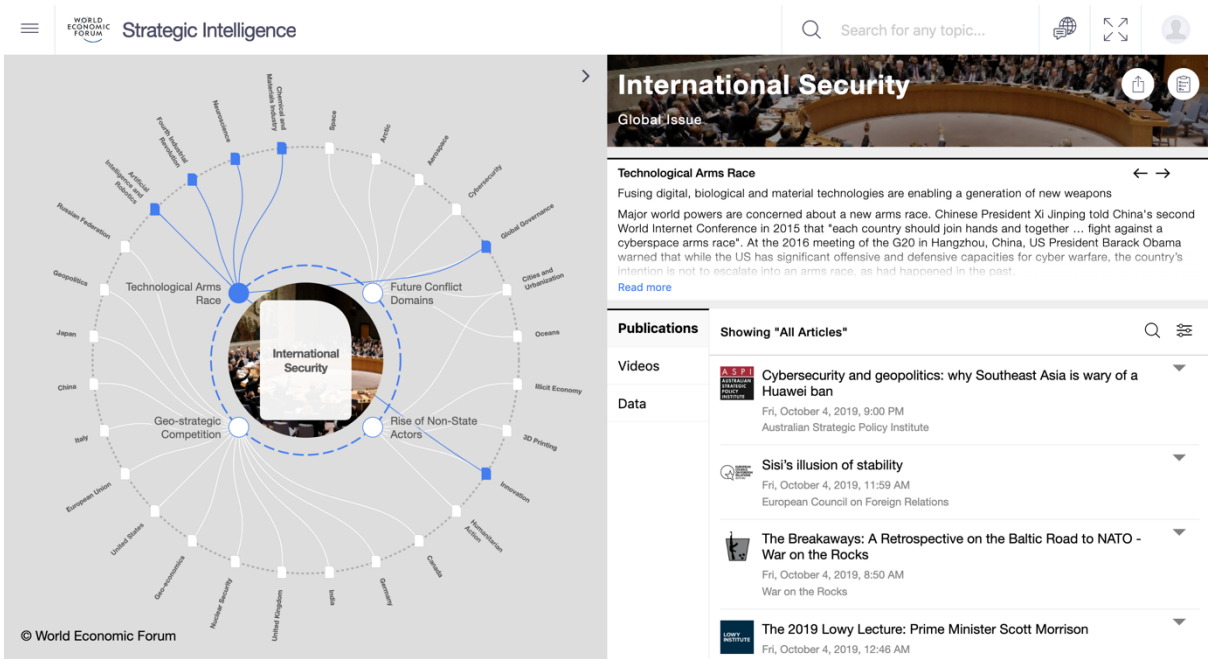
Below is a diagram illustrating the theoretical proposition of the capability of these two projects. Illustrating the deep learning technologies known as Path Signatures; a way to extract features from visual data in a way that is similar to human perception of different objects within particular footage (therefore, this technology is similar to the Object Recognition categorisation of applications defined in this report):



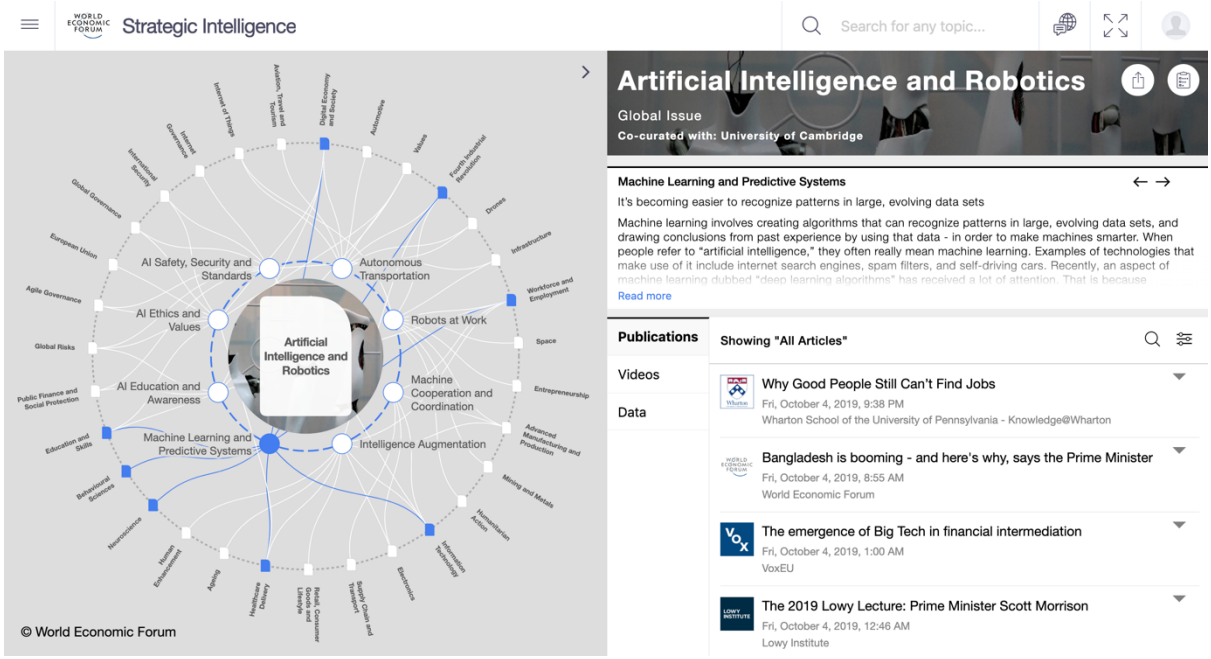
The Alan Turing Institute states that the ultimate goal of this project is to develop a generalised framework by incorporating 'path signatures' and deep learning to interpret complex multi-dimensional streamed data of human actions. This of course with time and results that show satisfactory performance could be translated to applications outside of traditional safety within manual industries and perhaps towards UK public safety applications such as UK domestic counter-terror. However, it is stated that there are current limitations for this technology, as discussed in the main body of the report.

APPENDIX 9: UTILISING WEF TRANSFORMATION MAPS

Utilising the World Economic Forums' Transformation Maps on their proprietary Strategic Intelligence Platform®, interrelated topics were identified relevant to Defence and Artificial Intelligence advancements. Research on the platform started out with exploratory analysis, viewing the core topic 'International Security':



For focused relevancy, the branch of 'Technological Arms Race' was isolated within this search. This helped identify another core topic, resulting in the exploration of 'Artificial Intelligence and Robotics', with specific focus on the branch of 'Machine Learning and Predictive Systems':



Below is an outline of the key takeaways from analysing the WEF Transformation Maps. The insights come from identifying the interrelated topic areas that must also be factored into my analysis, in order to make for an exhaustive report that accommodates all presently known issues into a coherent solution. The key issues are the major themes that I explored through the Transformation Maps, with relevant (and interrelated) topic areas flagged. Additional, no less relevant, areas are also included – illustrating areas of exploration that may have potentially been overlooked from my analysis.

Key Relevant Topics and Interrelated Issues

1. International Security
    a. Issue - Geopolitics
    b. Issue – Urbanization
    c. Issue – Technological Arms Race (Key Topic Area 2)

2. Technological Arms Race
    a. Issue – Machine Learning and Predictive Systems (Key Topic Area 3)
    b. Issue - Global Governance
    c. Issue - Fourth Industrial Revolution

3. Machine Learning and Predictive Systems
    a. Issue - Behavioural Sciences
    b. Issue - Information Technology

APPENDIX 10: CURRENT FRAMEWORKS FOR DEFINING SUCCESS

APPENDIX 10.1: UN OFFICE FOR COUNTER-TERRORISM SUCCESS FRAMEWORK

The UN Office for Counter-Terrorism implements a result-based framework for effective monitoring and evaluation of any ongoing and newly commissioned programs and applications. The UN emphasises this is a framework that assesses the overall quality of implementation and the holistic performance of the application in question rather than against a singular high-level objective. The 5-step evaluation criteria are laid out below, adapted and synthesised into brief statements relevant to this report:

1. Relevance: The extent to which the application is suited to the policies and objectives of the implementing group.
2. Effectiveness: A measure of the extent the application attains its specialised objectives, with an evaluation of the factors influencing the performance.
3. Efficiency: Measures the intended outputs in relation to the amount of input and resource allocation required, major focus on cost-efficiency and timeliness.
4. Impact: Assessing the changes brought about, directly or indirectly, to the current system for the application being implemented. A major focus is placed on the amount of disruption and the alteration to the activity of individuals.
5. Sustainability: Measuring the expected lifetime benefit in regard to the required input resources once implementation funding is complete.

APPENDIX 10.2: UK CONTEST FRAMEWORK

CONTEST is the UK Government's counter-terror strategy, developed and enforced from the highest level of Governance and overseen by the Home Secretary and Executives of the MOD. The four pillars of CONTEST, representing four key phases of countering terror, are Pursue, Prevent, Protect, and Prepare. A synthesised brief description of the four pillars is detailed below:

1. Pursue: To proactively engage with identified leads and suspected threats to ensure that all risks are mitigated through coverage by law enforcement, intelligence, and justice authorities.
2. Prevent: To stop people becoming terrorists or supporting terrorism, which is primarily done through proactive pursuit by intelligence and law enforcement, but with focused analysis on vulnerable individuals and communication networks of interest.
3. Protect: To strengthen UK protection and defence against a terrorist attack, which includes both physical and online components of infrastructure, ensuring that there is sufficient resiliency in the current system.
4. Prepare: To mitigate the impact of a terrorist attack, through ensuring response and protective systems are sufficient. Whereby first responders and critical infrastructure providers need to be at a high standard with strong procedural practices in place.

APPENDIX 11: PRELIMINARY RESEARCH OF SUITABLE APPLICATIONS

Below are the tabulated results of my preliminary research in identifying suitable applications that meet my refined problem scope. They are categorised by technology sub-clusters, of which there is Event Detection, Object Recognition or Video Tracking.

Name	Technology Sub Cluster Category	Short Description	Link to website
Deep Sentinel	Event Detection	Utilises Computer Vision technology to flag suspicious behaviour detected from their proprietary cameras positioned outside properties, and pairs this with human security officers to intervene if necessary.	https://www.deepsentinel.com/
iCetana	Event Detection	Real-time autonomous monitoring of video feeds to flag critical events for human inspection. They serve a wide range of industries, yet defence is a key feature of all product offerings.	https://icetana.com/
IntelliView	Event Detection	Real-time passive monitoring of security footage to notify of any potential safety risks that occur. They specialise in oil industry safety surveillance yet have features that can be incorporated into general security and defence use cases.	https://intelliviewtech.com/
Prophesee	Event Detection	Autonomous real-time monitoring of video content, in order to detect criminal activity and crowd-management. The USP is the effective speed and quality of the vision capture systems Prophesee develops.	https://www.prophesee.ai/
Shield AI	Event Detection	Computer Vision technology that aims to create situational awareness, the software has been implemented into proprietary drone technology thus far.	https://www.shield.ai/
Signal Innovations (BAE Systems)	Event Detection	Incorporates CV tools with its Big Data predictive capabilities to integrate a holistic predictive platform to monitor for events related to public security.	https://www.baesystems.com/en/article/bae-systems-completes-acquisition-of-signal-innovations-group
Stanley Security Systems	Event Detection	Real-time autonomous monitoring of video feeds to alarm of any critical events, they offer a full suite of security services and specialise in tailoring integrated security products.	https://www.stanleysecuritysolutions.com/
Umbo	Event Detection	Autonomous detection and identification of human behaviour, classifying and flagging any behaviours related to security such as loitering and tailgating.	https://umbocv.ai/
VideoIQ	Event Detection	Pre-integrated surveillance platform that filters through video feeds to flag any relevant event footage to be monitored and analysed through their proprietary platform, that also aims to incorporated Machine Learning powered predictive intelligence.	http://www.videoiq.com/
Vii Sights	Event Detection	Autonomous real-time monitoring of video content from widespread surveillance, providing alerts for a variety of actions and events of interest.	https://www.viisights.com/
Yitu	Event Detection	Full suite platform as a service offering, providing city-wide scale of surveillance management and event detection, integrating features that help to quickly identify and manage situations whilst they occur.	https://www.yitutech.com/en/business/intelligent-city

Name	Technology Sub Cluster Category	Short Description	Link to website
Athena Security	Object Recognition	AI tool trained to spot violence related objects such as weapons and to autonomously monitor areas of interest to flag for any sign of these types of objects.	https://www.builtinaustin.com/company/athena-security
Cortexica	Object Recognition	Computer Vision applications for businesses, providing image recognition services for use in relevant safety industries.	https://www.cortexica.com/
D-ID	Object Recognition	Protects identities from facial recognition by providing software to anonymise individuals yet still monitor and validate for security purposes.	https://www.deidentification.co/
Evolv	Object Recognition	Screening device that can passively scan up to 800 persons per hour to detect any high-risk items on their persons. It aims to help support security checks at public locations such as airports.	https://evolvtechnology.com/
Lumineye	Object Recognition	Wall-penetrating radar to help first responders and emergency service staff survey through objects (e.g. walls).	https://www.lumineye.com/
Traces AI	Object Recognition	Advanced individual search that can isolate targets from non-facial sources used advanced computer vision models	https://www.traces.ai/
Video Intellect	Object Recognition	Software suite that provides analysis of streamed video and can be instructed to detect certain situations in real-time.	http://intellect.video/

Name	Technology Sub Cluster Category	Short Description	Link to website
AgentVi	Video Tracking	Full suite platform as a service offering to provide real-time monitoring of city surveillance footage, centralising security analysis and provides automated flagging of potential security breaches for human inspection.	https://agentvi.com/
Anduril	Video Tracking	Full suite platform as a service offering, incorporating proprietary software to aggregate sensor video surveillance to increase the total data sourced and utilised from surveying an area of interest.	https://www.anduril.com/
Digital Barriers	Video Tracking	Real-time surveillance monitoring for large public areas, with metrics reported such as number of individuals and monitoring of congregated public areas - incorporating proprietary IoT devices with edge computing capabilities.	https://www.digitalbarriers.com/
Hauwei Safe City Program	Video Tracking	Full suite platform as a service offering, providing full time autonomous monitoring and tracking of potential high-risk events through the use of proprietary surveillance cameras (partnership with HikVision).	https://e.huawei.com/uk/solutions/industries/public-safety
Magal Security Systems	Video Tracking	Full suite platform as a service offering, providing integrated security monitoring and centralised analysis of video footage, a key feature if the scalability of the sensor systems that can be incorporated into the platform.	https://magalsecurity.com/
SDI Presence	Video Tracking	End-to-end video surveillance integrated system, from the sensors and video camera equipment installed to the platform that automatically monitors the video footage in real-time to provide aggregated analysis.	http://www.sdipresence.com/

Below is an aggregated list of all of the 24 applications where supplementary information regarding operating location(s) and funding amount to date has been provided.

Name	Technology Sub Cluster Category	Operating Location(s)	Funding Total
Deep Sentinel	Event Detection	USA	$7.4M
iCetana	Event Detection	Global (Inc UK)	$9.5M
IntelliView	Event Detection	Canada	$2.5M
Prophesee	Event Detection	France	$68M
Shield AI	Event Detection	USA	$48M
Signal Innovations (BAE Systems)	Event Detection	Global (Inc UK)	N/A
Stanley Security Systems	Event Detection	USA	N/A
Umbo	Event Detection	Global (Inc UK)	$18M
VideoIQ	Event Detection	USA	$37M
Vii Sights	Event Detection	Israel	$3.7M
Yitu	Event Detection	China	$382M
Athena Security	Object Recognition	USA	$5.6M
Cortexica	Object Recognition	UK	$9.2M
D-ID	Object Recognition	Israel	$9.4M
Evolv	Object Recognition	USA	$54M
Lumineye	Object Recognition	USA	$150K
Traces AI	Object Recognition	USA	$150K
Video Intellect	Object Recognition	Russia	$4.1M
AgentVi	Video Tracking	Global (Inc UK)	$20M
Anduril	Video Tracking	Global (Inc UK)	$41M
Digital Barriers	Video Tracking	Global (Inc UK)	N/A
Hauwei Safe City Program	Video Tracking	Global (Inc UK)	$1.5B
Magal Security Systems	Video Tracking	Global (Inc UK)	N/A
SDI Presence	Video Tracking	USA	N/A

Below are additional diagrams illustrating key summarising statistics.

Figure 1: *Diagram indicating funding statistics of these organisations, number and size represent count of distinct organisations*

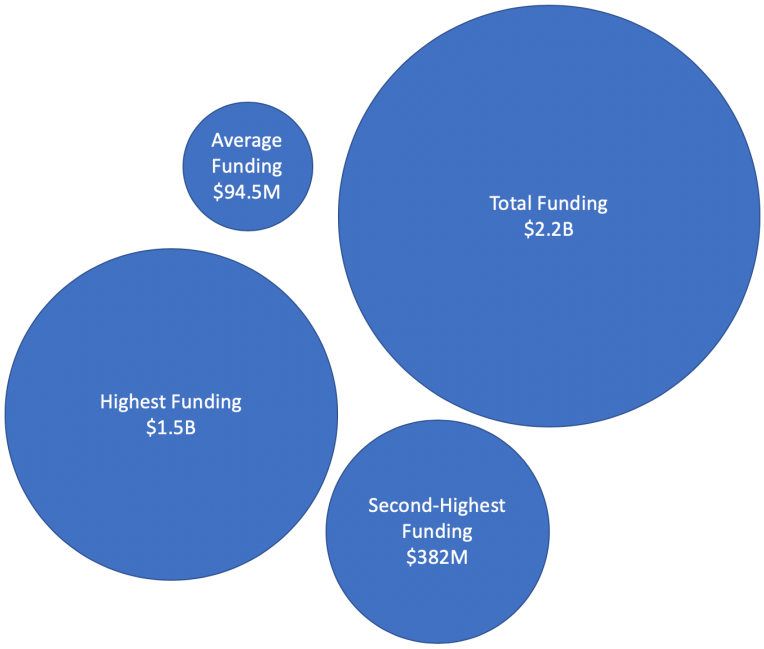


Figure 2: *Diagram indicating the categorisation of the applications identified, number and size represent count of distinct organisations*

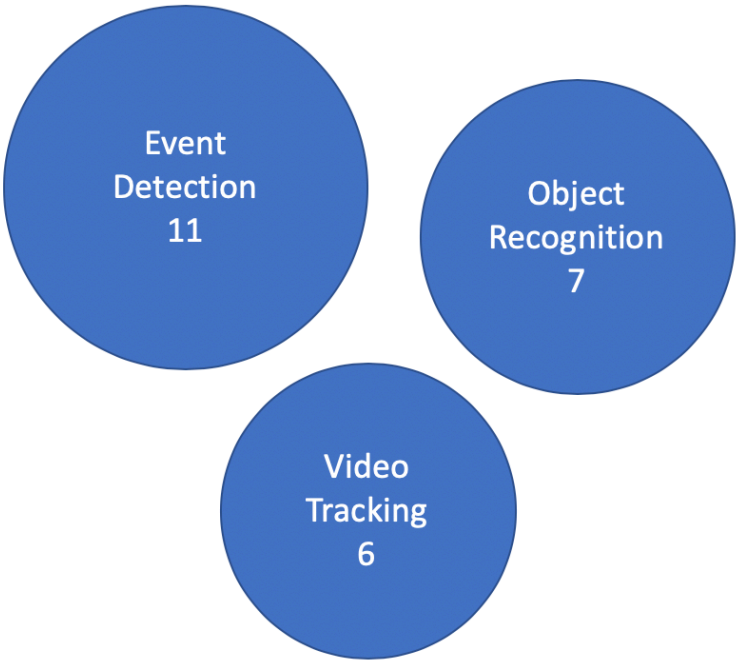
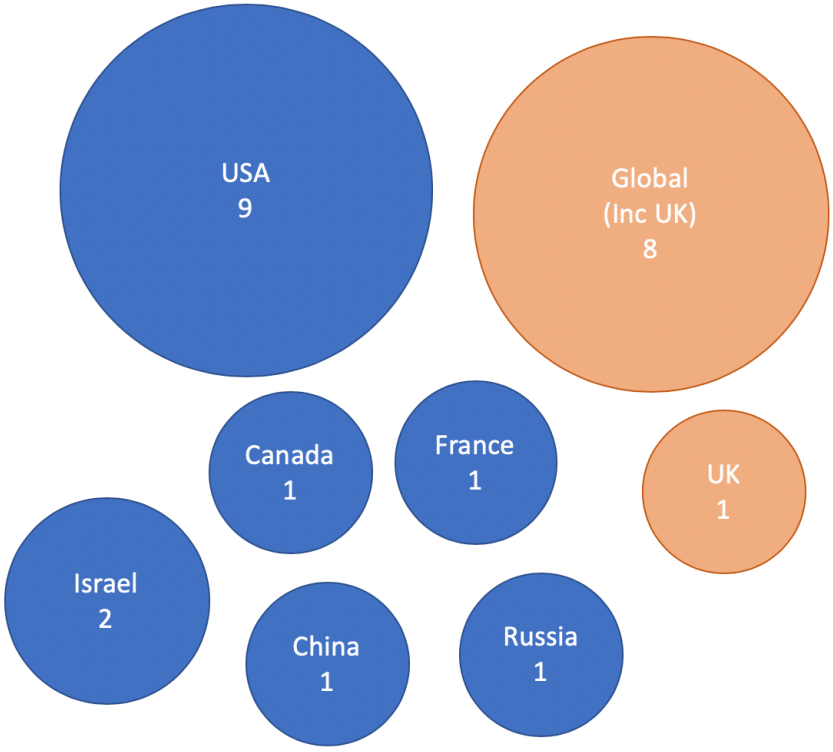


Figure 3: *Diagram indicating the current operating location(s) of each organisation, number and size represent count of distinct organisations*



MSIN0032 SUPPLEMENTARY APPENDICES

APPENDIX 1: INSIGHTS FROM WORKSHOP 1

Below is a summary of my insights developed during the Dissertation Workshops. The information provided here was simply my best estimates, based on the information I had at that time, for the answers to the following activities. This is not wholly representative of my final report, as numerous iterations have been undertaken – this is just a reflection of my preliminary understanding.

Description (Individual Activity 1):
My project aims to provide exploratory analysis and partnership/s recommendations for the Defence Science & Technology Laboratory (dstl, a subsidiary of the UK Ministry of Defence) with regard to the 'state-of-the-art' in Computer Vision technologies. Part I will involve scoping out the current technological landscape and provide sensible analysis and conclusive recommendations on relevant companies of interest for which dstl could partner with. Part II will further this analysis and also include analysis on how this new technology will integrate within the current systems utilised by dstl.

Data that will be utilised and generated will include model comparisons of traditional analytics (e.g. regression models to predict high-risk terrorism locations) with more advanced disruptive techniques (e.g. Anduril Industries Lattice AI and IBM PowerAI vision models).

Underlying Assumptions (Individual Activity 2):
Currently, I am assuming that mitigating terrorism risks and enhancing public safety is a top priority issue for dstl – I need to uncover concrete evidence to confirm this and understand the current focus areas and interest of dstl and confirm that scope of such a project is directly applicable to dstl (through report based analysis).

Plan of Action (for Part I): Firstly, I will present the significant problem which is mitigating UK terrorism risks and enhancing public safety, I will introduce dstl as the scoped client and the relevancy of their current work. I will then introduce the technology 'Computer Vision' – outlining how it meets dstl's scope and detailing the current 'state-of-the-art'. I will then analyse current application opportunities, current limitations and propose a suitable strategy for potential partnerships with relevant technological firms in the Computer Vision industry for dstl.

Plan of Action (for Part II): I will continue by refining down my choice of proposed partnerships and the advised implementation strategy for dstl – updating my analysis based on new information. I will then discuss the potential barriers still faced by the technology, outlining how these may be resolved in the future with specific relevancy to dstl, and then outlining and quantifying potential benefits through demonstrative examples.

APPENDIX 2: INSIGHTS FROM WORKSHOP 2

Decisions, Impact and Value:

From the three peer activities, I realised that I had to refine my key decisions and the problem I aimed to address in order to make the report more specific and scoped relevant to what an analyst can realistically achieve in 300 hours. The key question changed from 'how should dstl implement computer vision technologies to better serve their clients?' to 'which third party computer vision related companies should dstl look to partner with to help support its current goals in serving its clients?'. This moves the focus area to the key decision of partnerships and joint collaboration, whereby I need to uncover the current features of the decisions that go into establishing partnerships and what information is necessary for the key decision maker to make an informed decision. I believe that the key decision maker will be Paul Kealey, and I will treat him as my client. Aiming to provide value and impact through providing a synthesised list of relevant companies in the space of computer vision and performing a comparative analysis to provide partnership and strategy recommendations.

Problem Statement (first iteration):

Which organisations, if any, working within the field of Computer Vision technologies, should dstl allocate portions of its $40 million partnership budget by the end of year 2020, in order to benefit the current science and technology research relevant to the field of counter-terror.

It was noted that Counter-terror is term too broad for a finalised problem statement, therefore the scope should be based on refinement through understanding such information as which partnerships have already been established by dstl.
For example: UK domestic counter-terror predictive surveillance in public environments

Initial Hypotheses:

- Computer Vision is one of the most prevalent and potentially impactful technologies, relevant to the field of counter-terror.
- Current organisations working within the field of computer vision technologies, such as Anduril Industries and Traces AI, have illustrated significant advances from the state-of-the-art that dstl currently is working with, that is in fact worthwhile for partnerships to be established.

Alternative Hypothesis:

- The constraints and objections to Computer Vision are too strong, and it appears better suited to develop applications from within. Therefore, I would recommend that dstl should focus on proprietary research and development of tools, and look the create bespoke, suitable legacy integrated applications that are optimised for the relevant use cases.

APPENDIX 3: INSIGHTS FROM 1-1 WITH STEPHEN TODD

Below is a synthesised summary of the key takeaways from my one on one discussion with my Program Director, Stephen Todd. Stephen helped structure my thinking and together we formed an implicit strategy for directing my research in order for me to suitably scope my problem statement.

- I need to find the SPECIFIC employee (operating under Paul Kealey's Org) who will be the direct focus of my report.

- I need to first understand the exact purpose for particular aspects of the partnership fund – and what is the process for selecting and spending that money (e.g. sandbox consortium (or individual) pitching or relevant prototyping etc.)

- I need to confirm or understand if partnerships are a key issue and decision or NOT.

- Value may come from scoping out the relevancy of potential applications – to give standardised vocabulary of complex terminology and a base layer understanding for all key decision makers. I need to UNDERSTAND THE STARTING POINT OF RESOURCES AVAILABLE TO DSTL – I may need to create an exhaustive ontology of things, e.g. categories of applications and their relevancy of impact. For example, it may be of value to provide basic CV technology landscaping to find out who is not even on the dstl's radar with regard to partnerships and strategy.

- Dstl might not even know how to structure their funding for optimising impact (what even is a sensible impact to expect?). They may require explicit statements of what is a sensible spending structure (here it is alright to make assumptions and assertions).

- There could be a potential problem after the initial call to action for funding that needs addressing. For example, dstl may need guidance on how to structure their decisions and refine their potential options e.g. the structure of the technology and the impact.

- Value needs to be defined (e.g. JTBD of solutions, need to DISCUSS THE EXISTING SYSTEM and how potential technologies will impact this system). I need to ensure that I do not focus on technicalities, but the metrics based on the changes in outcomes.

- Value creation: avoidance of rare events (find other metric systems that focus on this particularly difficult to quantify metric and structure value creation e.g. aircraft safety systems and chemical plant control features)

- Design thinking is a key skill of this project; structuring thoughts and filling in the gap for any necessary problem structuring and being able to focus on what matters and providing relevant value for the key decision makers.

APPENDIX 4: RECORD OF UTILISING MY SUPERVISOR

Below is a table documenting the times that I utilised my Dissertation Supervisor. Included in the log is the initial agenda which was sent to the Supervisor prior to the meeting being held. Additionally, there are both the meeting minutes and key takeaways recorded, painting a picture of how I incorporated my Supervisor's advice and feedback into my report.

I would like to thank Dr Rouba Ibrahim, my Supervisor, for being such a thoughtful and careful help during my dissertation. She provided lots of beneficial insights and advice to help me structure my thinking and direct my research.

Date	Goal of Meeting	Initial Agenda	Meeting Minutes	Key Takeaways
24/10/19	To confirm the POA for conducting my Analysis	**The preliminary goal of my report** - I want to run by you the potential plan of action I have for how I want to direct my research and analysis, as well as to check whether you agree with the outcomes of the meeting I have had with Stephen with regard to my project (attached is my current preliminary outline of the problem as well as the notes from my meeting with Stephen, we can discuss this in the meeting). **The approach for scoping my report and the result expected by January -** I want to just run by you the way I plan to conduct my analysis (such as Quid industry analysis as well as analysis on relevant sub-domains of my technology of focus). I want to clarify that we are on the same page concerning what is feasible and expected for January.	• The goal of part I is to formally define and present logical questions related to the problem at hand– e.g. what are the main challenges currently faced by dstl? • There needs to be a logical flow introducing the problem that is the focus of this dissertation, such as highlighting the gap in current information available to dstl. • There does not need to be any 'individual analysis touch' for part I – just ensure that the current problem and system is clearly defined. • Regarding testing, model development could be an adequate form of demonstrating hypothesis and analysis within part II.	I need to ensure that my introduction directly engages the reader and provides a 'soft intro' into discussing and exploring the problem and the related system. Also, with regard to what I aim to complete by the first deadline, I have refined my expectations and placed greater importance on the initial exploratory analysis of understanding the system, therefore leaving discussing application areas until part II.
14/11/19	To review the introduction and overview sections of my project	**Is the flow of these sections of the repost cohesive** - I want to ensure that the audience are captivated and well informed immediately from reading my report, I want to understand if the way the client and company are introduced first then the introduction of the issue and technology is the appropriate way to frame these opening sections. (additionally, outlining how late my final problem statement will be detailed in the report is something I would like to discuss). **Are these sections detailed and exhaustive enough to ensure that all relevant background information is supplied** - I want to be able to briefly outline what the sections contain in order to gain confirmation (or not) if the level of detail provided is sufficient.	• The current structure makes sense and the contents does, from a quick scan, look to be exhaustive - yet the flow of information and the soft introduction of the formal problem statement needs to be cohesive to ensure that the reader does not feel left unclear until section 10 (need to assess the writing content). • The plan for softly introducing any analysis that I have conducted appears to be a strong plan, just introduce my initial scoping findings and then support my final hypothesis that will be tested in part II.	I will finalise my completed draft within the coming weeks, incorporating the second point related to finishing sections 11-14 to ensure that the analysis for section II is introduced in an enticing way without too much information included. Additionally, once complete I must assess whether the structure of the report is effective in engaging and informing the reader, specifically I need to assess whether the formal problem statement is better to be included earlier within the report.
03/12/19	To review my finalised completed draft	**Review the content of the report** - I want to ensure that all necessary content has been included for the purposed for this preliminary part of my total project. Specifically, I want to ensure that I have not excluded any key sections and that I have addressed all questions and concerns that come to the mind of the reader throughout reading the report. **Review the structure of the report** - I want to ensure that the literacy flow and overall discursive format of my report is coherent and addresses all key questions that the reader develops as soon as possible and introduces all sections in a relevant and convenient manner.	• If I include comparisons to other countries other than the UK, make sure that I incorporate this comparison into all analysis metrics (e.g. explicitly state the subset for Quid analysis as well as for applications currently accessible to dstl). • Some features (e.g. terminology glossary) can be included in the Appendix - on that point, it may be beneficial to give an outline of what is contained within the Appendix. • Make sure that all supplementary information, such as figures and diagrams are explicitly referred to within the text and are placed for additional value. • Include further discussions on dstl's current frameworks, the current technology they implement as well as perhaps give a stronger outline on Computer Vision technologies.	Some key comments refer to providing more exhaustive summaries of current descriptions and ensuring that all basis for analysis and discussion have been accommodated for and have been explicitly mentioned within the report. Furthering this, there needs to be some iteration on the structure, perhaps including a priori to outline the different sections as well as connect sections more explicitly. Additionally, give more explicit connection from the main body of the report to the Appendix. If I do this, as well as incorporate more information related to CV as well as what dstl is currently employing, this will go a long way to strengthening my report.

REFERENCES

Ackerman, S. (2014) *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ.* Available at: https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (Accessed: 04 November 2019).

Ahmad, S. et al. (2019) *Detection and classification of social media-based extremist affiliations using sentiment analysis techniques.* Available at: https://link.springer.com/article/10.1186/s13673-019-0185-6#citeas (Accessed: 02 November 2019).

AITechnologies. (2019) *Computer Vision technologies.* Available at: https://www.aitechnologies.com/computer-vision/ (Accessed: 29 August 2019).

Alan Turing Institute. (2019) *Detecting hazardous physical activity.* Available at: https://www.turing.ac.uk/research/research-projects/detecting-hazardous-physical-activity (Accessed: 14 November 2019).

Alan Turing Institute. (2019) *Human action recognition.* Available at: https://www.turing.ac.uk/research/research-projects/human-action-recognition (Accessed: 14 November 2019).

Alan Turing Institute. (2019) *Research projects.* Available at: https://www.turing.ac.uk/research/research-projects (Accessed: 14 November 2019).

Bidwell, C. (2018) *Emerging disruptive technologies and their potential threat to strategic stability and national security.* Available at: https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf (Accessed: 04 November 2019).

Cordwell, J. (2019) *dstl plans £40m opportunities for SMEs.* Available at: https://www.governmentcomputing.com/central-government/news/dstl-plans-40m-research-and-partnership-opportunities-for-smes (Accessed: 08 October 2019).

Cronin, M. (2019) *How technology can improve counter terrorism.* Available at: https://www.defenceiq.com/defence-technology/articles/proactive-vs-reactive-security-how-can-we-best-mitigate-the-terrorist-threat (Accessed: 30 October 2019).

Cummings, M. (2017) *Artificial intelligence and the future of warfare.* Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf (Accessed: 14 November 2019).

Dowdy, J. (2017) *McKinsey Report: Agility in US National Security.* Available at: https://www.mckinsey.com/industries/public-sector/our-insights/agility-in-us-national-security (Accessed: 30 October 2019).

Dstl (2019) *About dstl.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/362518/About_Dstl.pdf (Accessed: 04 October 2019).

Dstl (2019) *Annual report and accounts 2018/19.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818308/20190708-Dstl_ARA_2018-19_FINAL_v1_1-O_WEB-OPTIMISED.pdf (Accessed: 29 August 2019).

Dstl. (2019) *Serapis framework documentation.* Available at: https://www.gov.uk/government/publications/dstls-serapis-framework (Accessed: 04 October 2019).

Dstl. (2017) *Framework for conducting operations.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605511/20170331-Dstl_Framework_Document-FINAL.pdf (Accessed: 04 October 2019).

Ganor, B. (2017) *Lone wolf: passing fad or terror threat of the future?* Available at: https://www.washingtoninstitute.org/policy-analysis/view/lone-wolf-passing-fad-or-terror-threat-of-the-future (Accessed: 14 October 2019).

Gomis, B. (2018) *How 'success' should be defined in countering terror.* Montreal: Canadian International Council.

Government Computing. (2019) *dstl announces partners to deliver Serapis framework agreement.* Available at: https://www.governmentcomputing.com/central-government/news/dstl-serapis-framework-agreement (Accessed: 10 October 2019).

Grierson, J. (2019) *Foiled terrorist attacks risen to 22 says top officer.* Available at: https://www.theguardian.com/uk-news/2019/sep/09/foiled-terrorist-attacks-on-uk-soil-have-risen-to-22-says-top-officer (Accessed: 08 October 2019).

Hague Centre for Strategic Studies. (2018) *Artificial intelligence and the future of defence.* Available at: https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf (Accessed: 28 September 2019).

Health Foundation. (2013) *The measurement and monitoring of safety.* Available at: https://www.health.org.uk/sites/default/files/TheMeasurementAndMonitoringOfSafety_fullversion.pdf (Accessed: 04 October 2019).

Hoffman, B. (2019) *The return of violent far-right terrorism in the age of lone wolves.* Available at: https://warontherocks.com/2019/04/back-to-the-future-the-return-of-violent-far-right-terrorism-in-the-age-of-lone-wolves/ (Accessed: 14 October 2019).

Home Office. (2019) *List of terrorist groups and attacks.* Available at: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2 (Accessed: 06 October 2019).

IBM. (2019) *Data Integration Software Definition.* Available at: https://www.ibm.com/uk-en/analytics/data-integration (Accessed: 04 October 2019).

Jeffery, K. (2019) *How could applying Artificial Intelligence to CCTV help emergency service's control rooms?* Available at: https://www.apdcomms.com/news/2019/6/25/how-could-applying-artificial-intelligence-to-cctv-help-emergency-services-control-rooms (Accessed: 01 November 2019).

Karlin, M. (2018) *The implications of artificial intelligence for national security strategy.* Available at: https://www.brookings.edu/research/the-implications-of-artificial-intelligence-for-national-security-strategy/ (Accessed: 04 November 2019).

Kirk, A. (2017) *How many people killed in terrorist attacks in the UK?* Available at: https://www.telegraph.co.uk/news/0/many-people-killed-terrorist-attacks-uk/ (Accessed: 04 October 2019).

Laqueur, W. (2019) *The future of terrorism.* Available at: https://www.ft.com/content/114ccd5a-0459-11e9-99df-6183d3002ee1 (Accessed: 04 October 2019).

Le, J. (2018) *The 5 computer vision techniques that will change how you see the world.* Available at: https://heartbeat.fritz.ai/the-5-computer-vision-techniques-that-will-change-how-you-see-the-world-1ee19334354b (Accessed: 29 August 2019).

McKendrick, K. (2019) *Artificial intelligence prediction and counterterrorism.* Available at: https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf (Accessed: 04 November 2019).

Morris, T. (2004) *Computer Vision and Image Processing*. London: Palgrave Macmillan.

Murgia, M. (2019) *How London became a test case for using facial recognition in democracies.* Available at: https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959 (Accessed: 30 October 2019).

NaCTSO. (2012) *Protecting crowded places: design and technical issues.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97992/design-tech-issues.pdf (Accessed: 04 November 2019).

ONS. (2019) *Population Estimates for the UK.* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland (Accessed: 30 September 2019).

Osterwalder, A. (2005) *What is a business model?* Available at: b*usinessmodelalchemist.com* (Accessed: 06 August 2019).

Perlroth, N. (2014) *British spies said to intercept Yahoo webcam images.* Available at: https://www.nytimes.com/2014/02/28/technology/british-spies-said-to-have-intercepted-yahoo-webcam-images.html?hpw&rref=technology&_r=1 (Accessed: 04 November 2019).

Robertson, D. (2019) *Three steps the UK MOD can take to ensure it makes the most of artificial intelligence and automation.* Available at: https://www.paconsulting.com/insights/making-the-most-of-artificial-intelligence-and-automation/ (Accessed: 02 November 2019).

Schutskaya, V. (2018) *Trends of Computer Vision Applications.* Available at: https://www.kdnuggets.com/2018/11/trends-computer-vision-technology-applications.html (Accessed: 30 September 2019).

Sonka, M. (2008) *Image Processing, Analysis, and Machine Vision*. Stanford: Thomson.

Transport for London. (2019) *CCTV cameras across the London Underground network.* Available at: https://tfl.gov.uk/corporate/transparency/freedom-of-information/foi-request-detail?referenceId=FOI-0077-1718#targetText=London%20Underground%20have%2013%2C596%20station,the%20length%20of%20the%20train. (Accessed: 20 October 2019).

UKAuthority. (2018) *dstl explores machine learning for cyber security.* Available at: https://www.ukauthority.com/articles/dstl-explores-machine-learning-for-cyber-security/ (Accessed: 14 October 2019).

UK Government. (2019) *The dstl biscuit book.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819879/The_Dstl_Biscuit_Book_WEB.pdf (Accessed: 08 October 2019).

UK Government. (2018) *CONTEST: UK's strategy for countering terror.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/716907/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf (Accessed: 08 October 2019).

UK Government. (2018) *Terrorism in Great Britain: the statistics.* Available at: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7613 (Accessed: 14 October 2019).

UK MOD. (2018) *Global strategic trends.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/771309/Global_Strategic_Trends_-_The_Future_Starts_Today.pdf (Accessed: 08 October 2019).

UK MOD. (2012) *Technology, equipment, and support for UK defence and security.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf (Accessed: 04 October 2019).

UN. (2019) *Information and Communications Technologies Strategy.* Available at: https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/ (Accessed: 10 October 2019).

UN. (2019) *United Nations office of counter-terrorism framework for measuring impact.* Available at: https://www.un.org/counterterrorism/ctitf/en/uncct/measuring-impact (Accessed: 04 November 2019).

US DOD. (2018) *Summary of Department of Defence AI Strategy.* Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF (Accessed: 14 October 2019).

Vuorisalo, V. (2019) *Accenture report: Defence in the era of AI.* Available at: https://www.accenture.com/gb-en/services/public-service/defence-era-ai (Accessed: 02 October 2019).