Alexander Briscall Bowker
17015787
MSIN0032
4th May 2020

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

Part II:

Comparative analysis in order to provide recommended partnership(s)

Word Count: 6,989

1. INTRODUCTION TO PART II OF THE REPORT

The research and analysis of this report is a direct continuation from Part I. Whereby the relevant scope of Computer Vision (CV)[1] applications that could benefit UK counter-terror, from the perspective of the UK's Defence Science and Technology Laboratory (dstl)[2], has been established. For direct reference, the tightly defined problem statement that was formulated in Part I is as follows:

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.

Part I of this report concluded with the identification of 24 directly relevant applications. Part II of this report will analyse each of these applications in detail, in order to identify the most beneficial and relevant application for dstl, from the perspective of establishing potential partnership agreements. The applications will be assessed in two stages; firstly, by utilising the proprietary assessment framework developed in Part I, and secondly by utilising case studies and associated technical documentation.

Due to limitations placed on access to certain data, the analysis conducted was further scoped down to central London, with primary focus on the Transport for London (TfL) underground rail network. The fact that London is the most densely populated area of the UK, as well as being the city facing the greatest challenges when it comes to countering UK terrorism[3], means that the analysis is still of significant relevance.

The results of this analysis are summarised within the executive summary below and you can find detailed explanatory analysis within section 3 of this report. After this shortlisting process, the most relevant and beneficial application will be subject to economic assessment (section 5), followed by a discussion of prospective implementation plans (section 6) as well as recommendations for overcoming any potential limitations (section 7).

This will leave the final decision in the hands of the clients of this report, namely Dave Walker (Deputy Programme Manager of Autonomy, dstl) and Paul Kealey (Head of Cyber and Information Systems, dstl)[4]. The resulting key decision being: based on the information provided, should dstl proactively engage with the shortlisted application to discuss potential future partnerships.

[1] *For further explanation of CV and related terminology, refer to Appendix 1*
[2] *For further information on dstl as an organisation, refer to Appendix 2 of Part I*
[3] *Home Office, 2019*
[4] *For further detail regarding the clients of this report, refer to section 1 of Part I*

2. EXECUTIVE SUMMARY OF RESULTS

From the 24 applications that had been identified by the end of Part I, 8 made it through the first stage of shortlisting analysis; whereby the proprietary assessment framework developed during Part I was utilised. These 8 applications were reduced to a single application during the second stage of analysis; whereby case studies and technical documentation were utilised. You can find the key reasons for omitting applications during each stage of the shortlisting process within section 3 of this report.

The single application that made it through this shortlisting process is a software solution developed by an Australian organisation known as iCetana. The shortlisting analysis identified this application to be the most relevant and beneficial to dstl, for the purpose of the defined problem statement. The iCetana application is described in detail within section 4 of this report. For further information on the results and process of shortlisting the applications, please refer to both section 3 of this report and Appendices 4-5.

The shortlisted application, iCetana, was then evaluated based on an economic cost-benefit analysis of applying the application to the London underground rail network. The results are as follows; efficiency gains between £3.25-£6.57 million annually, given initial investment of £23,000-£73,000 per annum. You can find more detail regarding this analysis in section 5.

3. SUMMARY OF SHORTLISTING PROCESS

The shortlisting process, to identify the most relevant application for dstl, has been split into two components. The first utilises the proprietary framework developed within Part I. The second utilises case studies and technical documentation to further test relevancy and efficacy. Key insights and summaries of each stage are provided in turn below.

STAGE 1: UTILISING THE PROPRIETARY ASSESSMENT FRAMEWORK

For direct reference, the five-step proprietary assessment framework developed in Part I is repeated below:

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?

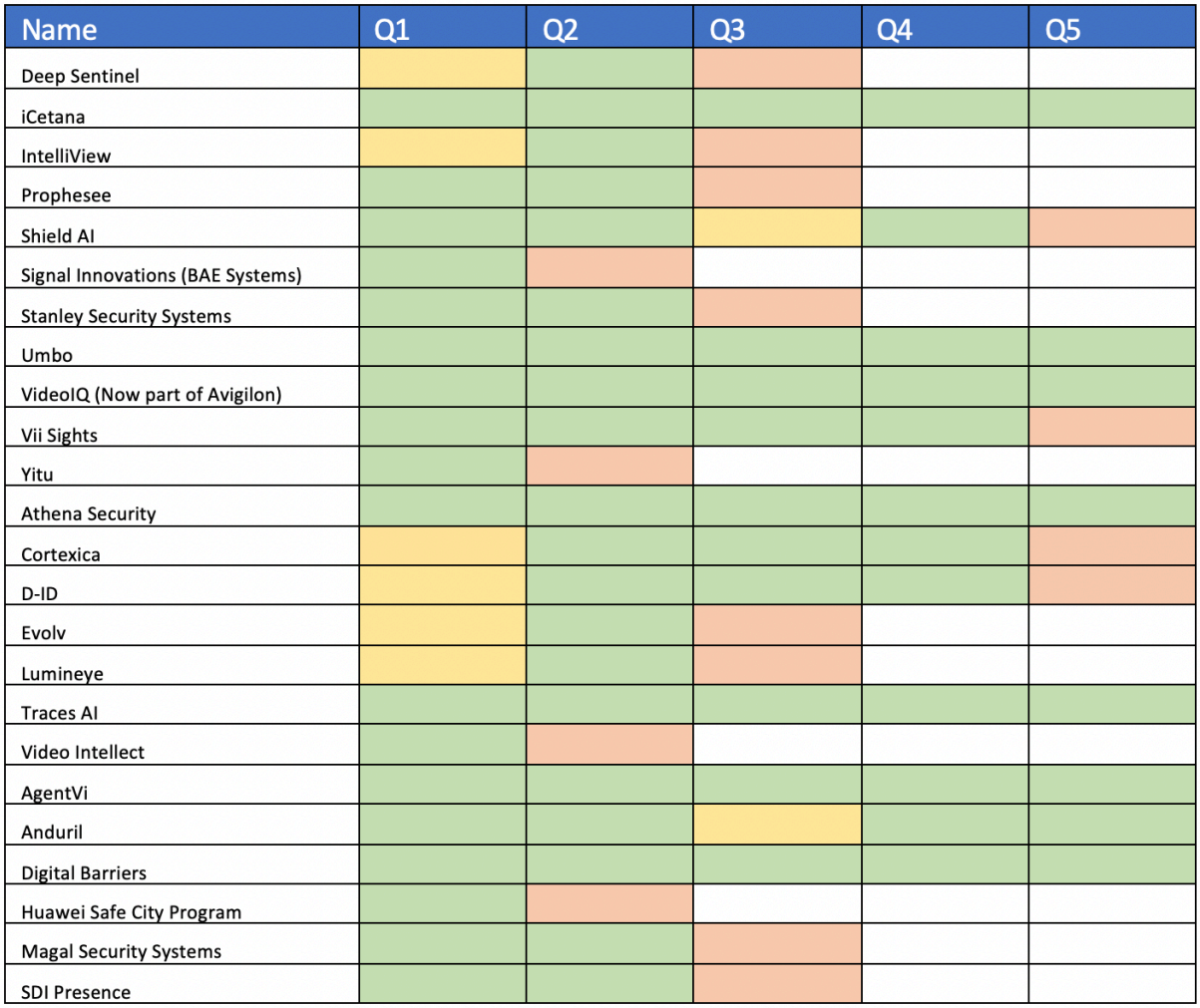
4. Is the application available to be utilised by dstl, based on the current scope of the Serapis framework for partnerships?

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

Each of the five points of the assessment framework are necessary but not sufficient criteria. Meaning that if one of the applications fails to meet one of the points, regardless of its performance relative to the other criteria, it will have to be excluded from my recommended shortlist of most suitable applications. Therefore, when conducting the analysis, the most efficient protocol was to systematically progress through the criteria (from Q1 to Q5) and disregard an application as soon as it failed to meet one of the criteria. Of course, features and insights learnt from studying all of these applications should still be included within the holistic analysis of this report and hence each application was still looked at in detail.

Figure 1 is a tabulated summary of the results from assessing each application against each respective assessment criteria. Each green box denotes an application surpassing the threshold for effectiveness for any given criteria. Each red box denotes an application failing to meet the criteria, and hence being disregarded for shortlisting (resulting in the non-coloured cells within figure 1). Each amber box denotes that an application adequately meets the criteria, yet there are nuances that need to be accommodated for. You can find a fully detailed version of the below summary in Appendix 4.

Figure 1: *Visual Summary of Stage 1 of the Shortlisting Process*



One of the primary reasons that applications failed to meet the criteria of the assessment framework was due to incompatibility with the UK and dstl's strategic objectives (related to assessment framework Q2). This shortcoming was most common with organisations that were either headquartered or state-run in countries where it would be highly improbable for the UK Government to rely on their services, based on the current state of geopolitics and global relations. For example, the Huawei Safe City Program has recently come under scrutiny due to its direct ties to the Chinese Government - the Centre for Strategic & International Studies claims that the safe city product fuels China "exporting authoritarianism"[1]. Therefore, it is reasonable to disregard such organisations as being suitable for such a sensitive and potentially secretive component of the UK's defence strategy. An exception to this trend is Signal Innovations, which has been acquired by BAE systems Intelligence & Security Inc., a subsidiary of the British Company that is a US-focused defence contractor that works solely with the US Department of Defence (DOD)[2]. Of course, there have been resource-sharing partnerships between the UK and US before, such as the sharing of R&D research (to avoid duplication of results) through the Technical Cooperation Program (TTCP)[3]. However, the specificity of Signal Innovation's scope makes it an unlikely candidate for being directly applicable and malleable to the desires and goals of dstl and the wider UK government.

Another reason applications failed to meet the criteria of the assessment framework was due to incompatibility with the UK's infrastructure (related to assessment criteria Q3). This trend was more apparent as a problem for hardware-focused applications, compared to entirely software-focused applications. For example, Evolv Technology develops a static screening device for passive object detection and surveillance that could be positioned, for example, at the entrances to the TfL underground rail network[4]. It can be argued that this proprietary device would be impossible to position at all points of interest in order to provide exhaustive coverage, and it could be the case that these screening points would become new areas of terrorist focus and targeting. However, being a hardware-focused organisation does not necessarily mean that the application is incompatible with the UK's current infrastructure. As long as the application itself is scalable and adaptable to common hardware components, it made it through this stage of the assessment framework. For example, Digital Barriers provides an application that benefits from specialised camera modules in order to utilise Internet of Things (IoT) capabilities, yet the underlying software is highly scalable and adaptive (it does not require the hardware in order to function entirely)[5]. As this application was already highly tailored to this reports problem domain, Digital Barriers made it through this stage of the assessment framework despite the fact it claims to be a hardware-focused organisation.

The final reason that applications failed to meet the criteria of the assessment framework was due to a lack of alignment between the applications core functionality and the desired key functionality defined within the problem statement. Of course, all 24 of the preliminary applications performed to some extent within the desired scope – that is why no application failed the first criteria (Q1). However, there were 6 applications whereby the desired functionality was simply a supplementary result of the core intended functionality of the application. In other words, the jobs to be done (JTBD)[6] of the application were only implicitly aligned with the desired job of the defined problem scope. For example, D-ID has developed a highly scalable software solution that aims to utilise non-personal identifiers of an individual as opposed to facial recognition[7]. The software solution does include the capability of analysing and assessing the activity of the monitored individuals; such a use case could indeed be for autonomous surveillance for domestic counter-terror. However, any investment required to implement such an application could not be justified in an economic sense, because the core functionality of the application was not as desired. Meaning that the functionality relevant to the defined problem scope was less optimised and less sophisticated compared to the eight applications that subsequently made it through to the end of this shortlisting process. Therefore, when it came to the last assessment criteria (Q5), applications such as D-ID were disregarded, if they hadn't been already.

[1]CSIS, 2019
[2]BAE Systems, 2020
[3]DST Defence, 2020
[4]Evolv Inc., 2020
[5]Digital Barriers, 2020
[6]Refer to terminology, Appendix 1
[7]D-ID Technologies, 2020

STAGE 2: DEEPER ANALYSIS UTILISING CASE STUDIES AND TECHNICAL SPECIFICATIONS

To examine the eight remaining applications in further detail, reported case studies and technical specification documentation were analysed. This helped give a greater sense of which application was most suited to dstl and the tightly defined problem domain. For specific notes on the analysis conducted on each of the respective applications, please refer to Appendix 5. Below is a summary of the key themes from this stage of the shortlisting process.

To truly understand the specificity of an application's ability to be integrated into existing UK infrastructure, the current surveillance equipment and vendors being utilised within the UK needed to be identified. A good place to gain this understanding was to examine the contracts in place between Transport for London and surveillance camera equipment companies. In line with the 2015 Transparency Code, TfL publishes details of contracts it holds with a value of over £5,000. This database of current contracts was examined for the purposes of identifying any CCTV equipment vendors that are currently in operation with TfL for supplying CCTV for London infrastructure. From analysing this database, the two CCTV vendors identified were Delatim Limited and Telent Technology Services. The output from analysing this dataset is displayed in Appendix 6. Of course, it is possible that other CCTV vendors could be utilised by TfL in the future, yet we can assume this is improbable due to the legacy nature of the infrastructure system; to replace these vendors could be costly as current CCTV systems may need to be overhauled[1]. Furthermore, assuming that potential applications will continue to increase their list of compatible vendors is not a proactive stance – it is important dstl takes swift immediate action and not wait passively for hypothetical improvements. Based on this insight, it was possible to omit both Traces AI and AgentVI, as both applications produce software that is only compatible with a defined subset of hardware technology partners, of which the subset lists did not include Delatim or Telent.

Secondly, to ensure there could be swift and effective integration, the scope of each application's current use cases needed to be analysed. If a certain application has only had exposure to a very narrow scope of situations, for which their models have been able to be trained, then this raises concern for how quickly that particular application could be tailored to the tightly defined problem statement and the context of urban environments within central London. For example, Athena Security's solution has only been utilised within the context of US high schools, utilising object recognition algorithms that so far have only been optimised to detect wielded firearms[2]. It takes vast data (as well as time and money) to train object recognition models; as a base recommendation, 10^4 distinct data points are expected in order to adequately train a CV model[3]. The UK is known for enforcing stricter gun control than the US and as a result terrorists, especially lone wolf attackers, have most often resorted to weaponry that is more subtle – for example, November's London Bridge attacker was armed with a kitchen knife[4]. In comparison to other applications, such as those that made it through this stage of shortlisting, there is concern that Athena's solution is too focused and would require too much initial investment in terms of time and capital in order to repurpose the software for this particular defined scope. The two other applications that were omitted based on similar reasoning were VideoIQ and Anduril. For information related to these particular applications, please refer to Appendix 5.2.

Finally, there were three applications left until this stage in the shortlisting process: Umbo, Digital Barriers and iCetana. These appeared to be the most promising applications, with the greatest benefits and the least disruptive implementation ability. You can find detailed descriptions of both Umbo and Digital Barriers in Appendix 5.3. The difference between iCetana and both Umbo and Digital Barriers is that iCetana is a completely software-focused application, whereas the impressive statistics related to the high performance of the autonomous surveillance of both Umbo and Digital Barriers is preconditioned on the implementation of their complementary proprietary wireless hardware camera modules[5]. What makes Umbo and Digital Barriers different to other hardware-focused applications is that their software can run effectively without the hardware they develop; in both cases their software can operate and integrate into existing CCTV surveillance systems[6]. However, the included integration of their hardware modules, both being wireless surveillance camera sensors, enables both companies to perform with greater efficiency and accuracy. It is with the included hardware that the performance of such applications is on par with the performance of iCetana's software-only approach. Hence, if both Umbo and Digital Barriers require considerably more investment, both in terms of capital and time, to be implemented and perform as well as iCetana, then it can be concluded that iCetana is the preferable application of choice.

Therefore, the entire shortlisting process resulted in the identification of a single, most relevant and beneficial application: iCetana. This application appears to overcome or mitigate all of the issues discussed above, that were the resulting drawbacks of other respective applications.

It is interesting to point out that this shortlisting analysis has disproven a preliminary hypothesis that was formed during Part I of this report; that the application(s) potentially most beneficial to dstl would be one that does not currently operate within the UK (refer to section 8 of Part I to understand the formation of this hypothesis). iCetana has the potential to be already on dstl's list of companies of interest – iCetana is a company that already operates within the UK[7] and in fact was an attendee at the UK 2017 security expo whereby the Robotics Technical Lead, Mark Emerton, from dstl attended[8]. Through the analysis conducted during this shortlisting process, it has become evident that organisations already with deep practical experience in the specific problem domain within the UK had significant advantages compared to their peers with regard to relevancy and potential implementation opportunities. The most capable and promising of these highly relevant applications was identified as iCetana. The rest of this report will assume that there is no current partnership established between dstl and iCetana (currently, there are no publicly published details of such a partnership anyway). Henceforth, the capabilities and features of the iCetana application are discussed in detail in the following section.

[1]Smart, 2020
[2]Athena Security Inc., 2020
[3]Mitsa, 2019
[4]Edwards, 2019
[5]Umbo Computer Vision Inc., 2020 and Digital Barriers, 2020
[6]Ibid
[7]iCetana, 2020
[8]dstl, 2018

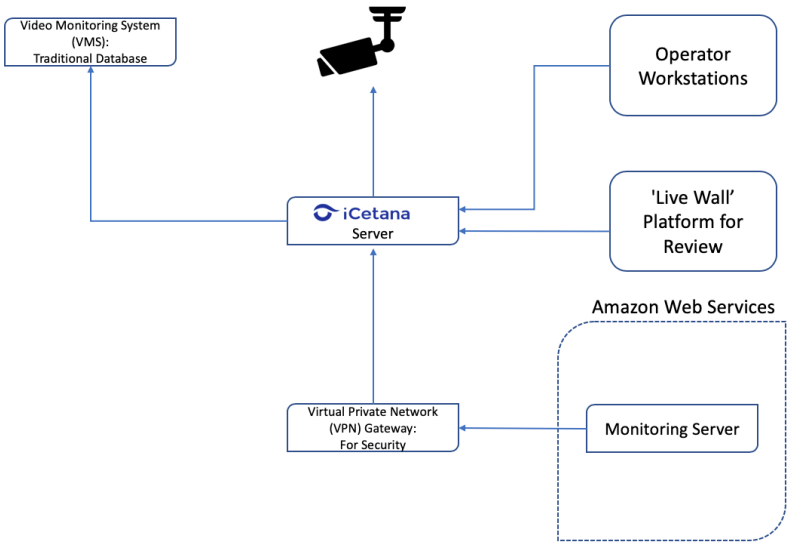
4. DESCRIPTION OF THE SHORTLISTED APPLICATION

For comprehensive understanding, it is useful to include a technical explanation of iCetana, the application that successfully made it through my shortlisting analysis. Technological features, as well as notable performance indicators, have been included to provide an overall sense of the capabilities of the application.

An Australian-based organisation that already operates within the UK, iCetana is a software company that produces autonomous video surveillance that aims to identify suspicious activity and precursor events, filtering solely relevant incidences for human operator intervention. iCetana's software requires two weeks of training – passively monitoring the new environment to learn to identify unusual activity - when it is integrated into a new surveillance system[1]. After this period, iCetana's software aims to reduce, by screening for potentially relevant threatening events, video overload for human operators by 99%[2]. Resulting in an increase in capability of 60x more cameras monitored per operator as well as the ability to review 24 hours' worth of video footage in 30 minutes[3]. Additionally, the software aims to incorporate predictive analysis by incorporating Machine Learning[4] techniques to identify potential precursors to events. As of current, CCTV surveillance systems have non-existent analysis capabilities or utilise basic rule-based video content analysis (VCA)[5].

Furthermore, iCetana's software integrates with existing video infrastructure, adaptable to any common video monitoring system (VMS). A simple visual demonstration of a standard integrated system utilising iCetana's software platform is illustrated in figure 2. The current domains of expertise, for which iCetana's detection software has been optimised, that are relevant to the problem scope include public places such as shopping malls, educational campuses and public transport[6].

Figure 2: *Visual Demonstration of Integrating iCetana's Software with Current Infrastructure*



[1] *iCetana, 2020*
[2] *Ibid*
[3] *Ibid*
[4] *Refer to terminology glossary, Appendix 1*
[5] *British Security Industry Association, 2016*
[6] *iCetana, 2019*

5. THE ECONOMIC CONSIDERATIONS OF THE SHORTLISTED APPLICATION

It is important to note the economic factors, such as cost and potential efficiency gains, related to the shortlisted application. This helps develop a strong potential business case for the purposes of implementing iCetana; details of which can be found in the following section.

Analysing iCetana's financial statements enabled the derivation of an estimated cost placed on installing iCetana's software on a given CCTV camera. Appendix 7 contains details of analysing iCetana's income statement, whereby aggregated cost of goods sold (COGS) was extrapolated in order to derive a cost range of approximately £108-£216 per camera for utilising iCetana – assuming a range between 50,000-100,000 cameras for iCetana installations in 2019[1]. If this value can be expected as the cost for implementing iCetana's software within such a place as London's underground rail network, for which this report continues to focus on, then this per-camera cost can soon become a substantial sum; there are a total of 15,000 cameras within London's underground rail network[2].

However, simply establishing a net cost that the UK Government would potentially incur as a result of utilising iCetana is an unsophisticated approach. Instead, the cost of incorporating the software should be annualised over the expected useful lifetime of the CCTV equipment. Despite equipment expenditure being independent to the cost of installing iCetana, it can be argued that iCetana's setup costs will only be applicable up until the camera equipment needs to be changed, after which iCetana's application will be required to be integrated again. Therefore, this practice will help paint a more accurate picture of the cost that the UK Government would incur, on an annual basis, from utilising iCetana. In order to annualise this cost, we need to assume an average useful life of CCTV camera equipment of 5 years[3] and a discount rate of 3.5% (the standard rate applied to project appraisals in UK Government[4]). Furthermore, we will utilise the following formula for annualising this cost:

$$Equivalent\ Annual\ Cost = \frac{Net\ Present\ Cost\ x\ discount\ rate}{1-(1+discount\ rate)^{-number\ of\ useful\ years}}$$

To accommodate for uncertainty in both the estimates for the cost per unit of iCetana's software as well as the scale of integration within the entire TfL infrastructure, a range of annualised costs are provided in the below matrix – assuming in a 'low uptake' scenario only 60% of cameras have the application installed compared to 100% in a 'high uptake'. You can find details of this calculation, as well as assumptions to form the ranges, within Appendix 8.1.

Figure 3: *Matrix Demonstrating the Range of Possible Annual Costs for Implementing iCetana.*

(Cols) iCetana's COGS (Rows) TfL's Integration	'Low' Scenario	'High' Scenario
Low Uptake	£22,000	£44,000
High Uptake	£37,000	£73,000

There are increased cost pressures being put in place at a Governmental level; the entire global spend by the UK Government on surveillance equipment has decreased 46% to £56 million per annum within the last ten years[5]. Therefore, it is increasingly important that applications such as iCetana can be proven to be cost-effective. For this use case, the benefits drastically appear to outweigh the costs. It is estimated a terrorist act costs the UK approximately £600 million due to the resulting decrease in investment and fall in GDP[6]. Therefore, even stopping one act is enough to make iCetana economically feasible. Although, it is perhaps an inconsiderate thing to place economic value on saving lives, as well as there being innate issues with basing success on such a high-level objective - this was discussed in detail in section 11 of Part I.

Instead, it is perhaps useful to gain a comparative understanding of the capabilities and resulting efficiency gains that would come about by utilising iCetana's software. The reported benefits from utilising iCetana's autonomous surveillance application have already been discussed within the previous section, yet calculating implicit economic impacts from such metrics, for the purposes of helping dstl develop a justifiable business case, may be of use. Of course, it is important to be wary of utilising these metrics as the basis of forming our economic assessment; they are self-reported claims from iCetana itself. However, these statements have been corroborated with evidence from independent client testimonials within Appendix 8.2.

From extrapolating current costs, as reported within the British Transport Police's annual report, it appears iCetana could result in efficiency gains per annum of approximately:

Figure 4: *Table Demonstrating Potential Efficiency Gains as a Result of Implementing iCetana.*

Efficiency gains as a result of	'Low' Scenario	'High' Scenario
More efficient CCTV monitoring	£56,000	£168,000
More efficient Police emergency response	£3.2 million	£6.4 million

Explanations of the derivation of these estimated ranges are provided within Appendix 8.2. If we compare these figures to the cost estimations also conducted, it is clear that iCetana is worth pursuing and will result in surplus efficiency gains and cost savings – with a demonstrated return on investment of between 44- and 284-times cost. We will now go on to discuss best practices with regard to implementing iCetana's solution.

[1]*You can find the derivation of this range within Appendix 8.1*
[2]*Transport for London, 2020*
[3]*Silva, 2014*
[4]*HM Treasury, 2018*
[5]*Surveillance Camera Commissioner, 2018*
[6]*Morrison, 2018*

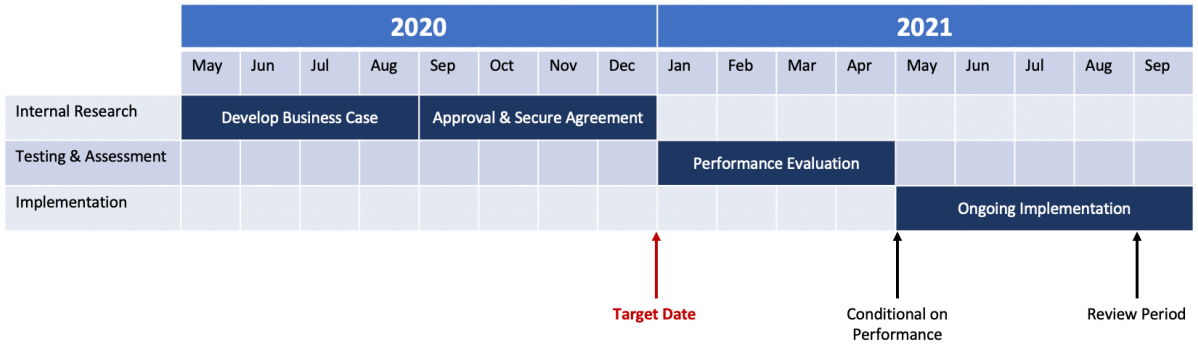
6. POTENTIAL IMPLEMENTATION ROADMAP OF THE SHORTLISTED APPLICATION

The intention of this section is to provide an understanding and set expectations with regard to the potential implementation strategy that could be employed in order for dstl and iCetana to partner effectively. Of course, more comprehensive implementation plans will be laid out if dstl approves of such a partnership and continues in developing a strategic plan of action. However, it is of potential benefit to include preliminary discussions within this report in order to help supplement dstl's work if such circumstances come into fruition.

dstl currently follows the Serapis framework when it comes to implementing and developing any potential partnerships with third-party technology providers. This framework has been analysed and discussed within Part I of this report. Within this framework, it states that the preliminary steps for establishing a successful partnership require dstl to produce a business case for approval by the MOD Chief Scientific Advisor[1]. Fortunately, it so happens that iCetana has substantial experience in developing such businesses cases; being a well-established and successful organisation has enabled iCetana to expend the resources to have in place expert staff to help develop the necessary reporting in order to build a successful business case such as the one required for the Serapis framework[2]. This is yet another key benefit of iCetana in comparison to other applications that were analysed throughout the shortlisting process. If it is such that iCetana can help dstl develop a business case quickly, then it will help kickstart the implementation process in an efficient manner.

For the purpose of setting expectations, please refer to figure 5 below in order to understand the potential timeline for implementing iCetana's solution, with the start date being the date of publishing this report (4th May 2020).

Figure 5: *Visual Representation of the Potential Implementation Roadmap for dstl and iCetana*



As visualised above, the prospective implementation strategy involves three stages:

1. Internal research and assessment conducted by relevant stakeholders within dstl.
2. Cooperative assessment of the performance of the application in the given operating environment.
3. Direct implementation of the application into the operating environment.

The time periods illustrated above have been extrapolated from iCetana's white papers and their documented case studies with similar infrastructure systems, such as college campuses[3]. These are not hard deadlines, nor have they been confirmed by dstl as achievable, yet they provide a baseline for a sensible time period for implementing such tasks. It should be noted that the first stage, the development of the business case and a partnership contract, is set to be completed by year-end 2020. This can be extended, if required, due to the global situation regarding COVID-19, yet most of this stage can be undertaken remotely. This deadline would be in line with the objective laid out within Part I of this report; whereby if dstl can successfully establish a partnership agreement with iCetana and confirm the amount (if any) to be allocated out of the partnership budget, then the problem statement objective has been completed. Of course, the partnership agreement is subject to approval by the MOD Chief Scientific Advisor[4]. If the partnership is agreed upon, then the second stage can be commenced. Whereby both iCetana and dstl should work in tandem to test the capabilities and assess the performance of iCetana's application within the specific environment for which it will be launched. This report continues its focus on the London Underground rail network and recommends initially testing the application within certain underground stations with high footfall, such as those situated upon the Circle line[5]. Again, advancing to the third stage is conditional on the performance of iCetana's application surpassing a satisfactory threshold during the performance evaluation stage. Although, it should be noted that this report would not have identified iCetana as the shortlisted application if research did not point to iCetana being able to confidently pass this threshold. The third stage, launching the application, is to be conducted on an ongoing basis, extending the iCetana application to more CCTV surveillance systems within the TfL public transport network before extending the application nationwide. This report recommends that during the next three years (by June 2023), iCetana's software should become operational within all major public surveillance infrastructure systems within the UK. There will, of course, be many obstacles and limitations that this project may potentially face – overcoming the most prominent is discussed in the following section.

[1]dstl, 2019
[2]iCetana, 2020
[3]Ibid
[4]dstl, 2019
[5]Transport for London, 2020

7. OVERCOMING POTENTIAL LIMITATIONS OF THE SHORTLISTED APPLICATION

Of course, no application is perfect and without potential downfalls. It is important that these limitations are discussed, in order for the client of this report to make the most well-informed decision with regard to confirming any potential partnership. Additionally, examining these limitations will help develop a potential strategy that can help mitigate these downfalls.

7.1 DATA PROTECTION

The issue of public distrust and concern with regard to the protection of personal information such as facial recognition data was discussed in section 12 of Part I of this report. In summary, there have been many public scandals within the last 10 years involving surveillance programs and their techniques for gathering intelligence. For example, as discussed in Part I, the Government Communications Headquarters (GCHQ) 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]. These scandals have resulted in large-scale public distaste for utilising personal information without explicit consent (refer to section 12, Part I). Therefore, iCetana must help appease public perception and fall in line with the stringent rules that have now become commonplace with regard to the data collection of the general population.

An advantage that iCetana holds in this regard is that it does not conduct explicit facial recognition[2]. It passively monitors without the need to distinctly identify each person caught within the visual imagery. Partnering this with iCetana's robust security-camera-code-of-practice-compliant storage techniques[3] can help build a strong case for iCetana being able to mitigate any of the concerns regarding data protection. Furthermore, despite the recent cases of public distrust, as discussed in Part I, it appears that on aggregate the public perception of video surveillance techniques within the UK is now one of positive sentiment. With sustained growth in positive public perception over the last five years – perhaps due to the macro increase in technology's presence within our personal lives[4] – resulting in an overall 60% positive sentiment score from Quid proprietary research[5].

However, despite the fact that iCetana not conducting explicit facial recognition is considered an advantage with regard to this issue, it may in fact be a hindrance to the overall effectiveness of the application. For example, cross-referencing any suspicious activity with a known intelligence database of suspected individuals may be crucial in swiftly and efficiently understanding the genuine threat level of a given situation; currently, this cross-referencing is best done through techniques such as facial recognition[6]. If this is proven to be too much of a limitation on iCetana's part, then it is recommended that this application is used in conjunction with other applications that are more specialised in this domain. For example, through the analysis of this report, many applications have been identified that serve as more robust, accurate and secure alternatives to facial recognition. This report recommends the application Traces AI is considered first if it is the case that individual-identification techniques are required as part of the entire automated solution. You can find detailed information related to the Traces AI solution in Appendix 5.

7.2 LACK OF CONTINUITY AND INTEGRATION

This report has identified iCetana as the overall most well-suited application, partly due to its ability to easily integrate with any Video Monitoring System (VMS). Flexibility and adaptability are what became a key differentiating factor in shortlisting iCetana, as compared to alternative applications. However, the extent to which UK infrastructure varies is hard to overstate. For example, the current infrastructure in place throughout the TfL public transport systems varies extensively. London Overground rail networks are operated by a concession holder on behalf of TfL, that is in fact different to the operator of the majority of the London Underground rail network[7]. Any CCTV and VMS systems in or around these rail networks are the responsibility of the concession holder[8] – hence the potential degree of variability in hardware is considerable. iCetana itself claims to overcome this potential downfall by providing a software solution that can be integrated with practically all types of VMS and surveillance infrastructure. This report recommends that, if partnership talks are proactively established by dstl, the first point of clarification between dstl and iCetana to be an exact reconciled list of all compatible surveillance systems with iCetana's software. Whereby this list can then be cross-referenced with the UK Government's list of active surveillance infrastructure, in order to understand which areas can be of direct and immediate implementation and which require potential overhaul of current infrastructure. This report believes that the former should be maximised and the latter should be minimised, as compared to alternative applications, based on the shortlisting analysis conducted.

However, the issue of direct integration with current VMS and CCTV equipment is not the end of this issue. Because of the disparate management and organisation of different infrastructure systems, even within the TfL network, there may be areas whereby iCetana is truly not applicable. For example, some London Underground stations are less covered with surveillance cameras compared to others (Oxford Circus' Bakerloo Line has 309 cameras, whereas the equally busy Piccadilly Circus' Bakerloo Line has only 175[9]). Research must be undertaken to understand if this difference in camera quantity does in fact result in potential blind spots and areas susceptible to greater risk of undetected terrorist activity. This assessment must be undertaken for each new environment for which iCetana will be implemented, such as each distinct London Underground station. If it is the case that there is an apparent safety gap due to the lack of continuous surveillance coverage in any of the given environments, then it should invoke a reassessment of the Security Camera Code of Conduct; whereby the extent of the prescribed surveillance coverage is more strictly defined and enforced. dstl, partnering with the Surveillance Camera Commissioner, may find it useful to outline and document the initial testing & assessment implementation stages (see section 6) as a case study to be included in an updated Surveillance Camera Commissioner report.

7.3 LACK OF DEFINITIVE COVERAGE

Not only will the application need to be implemented cohesively and extensively within a given environment, it will also be necessary to maximise the extent of the different environments for which it is used. For example, if it is the case that the application has been implemented within a single environment; for example, London Underground. Then it is of national interest to not reveal any information related to such implementation publicly. As it may be the case that terrorists will utilise this information and will pursue other areas, that they know are not utilising this sophisticated surveillance application. This is exacerbated when considering the worrying trend of lone wolf attackers within the UK[10], whereby the unpredictable and spontaneous nature can result in attacks in a wide variety of public environments[11].

This concern highlights the point that iCetana cannot be relied upon as a one-stop answer for counter-terrorism surveillance. There are simply too many areas for which the application would need to be implemented, not to mention the areas for which implementation is not feasible. However, this report is not trying to argue that iCetana can be the single resolution for counter-terror surveillance. Instead, this report believes that iCetana is the best application to renew the current video surveillance techniques utilised throughout the UK; whereby reactive monitoring by human operators is employed. iCetana aims to be a more automated and sophisticated alternative to this current practice, and the analysis of this report indicates that iCetana is indeed the most suited application for this purpose. This report recommends that dstl, again in partnership with the Surveillance Camera Commissioner, compile a list of the most well-suited implementation areas – whereby automated passive surveillance will help relieve significant resources from human operators. These locations must enable cohesive and exhaustive surveillance, through current infrastructure. Provided below are what this report believes to be exemplar locations that meet these criteria, with reasoning behind the selection included in Appendix 10. This list can help provide preliminary points of discussion for dstl to utilise if such talks with the Surveillance Camera Commissioner are pursued. The areas include:

- TfL Rail Network
- Shopping Complexes such as Westfield™ and Selfridges™
- Entertainment and Sporting Stadiums such as The O2™

This would leave a number of public places without the implementation of the iCetana application - even previously targeted areas, such as London Bridge. However, it can be argued that relieving resources such as human operators and efficiently dealing with issues through pre-emptive action will enable for more effective and focused protective protocols to be put in place within these other environments. One such protocol is already being put in legal motion – through the development of 'Martyn's' Law[12]. The regulation has been developed since the Manchester Arena bombing and involves a comprehensive 'scheme of best practice' for protecting public environments such as those outside the implementation scope of iCetana's application – for example, Manchester's Market Street[13]. Manchester Council has announced that the Law will be incorporated into future licencing regulation across the region. If iCetana can implicitly help, through efficiency gains and automated procedures, enable a shift in focus to more obscure at-risk areas, then the application can be deemed a success.

[1]*Ackerman, 2014*
[2]*iCetana, 2020*
[3]*Ibid*
[4]*Wardynski, 2019*
[5]*Refer to Appendix 9.2*
[6]*UK CONTEST framework, 2018*
[7]*Transport for London, 2020*
[8]*Transport for London, 2019*
[9]*Transport for London, 2018*
[10]*Lacqueur, 2019*
[11]*Cronin, 2019*
[12]*Blakey, 2020*
[13]*Ibid*

8. CONCLUSION AND ADVICE FOR DSTL

The purpose of this report was to identify any application(s) that may be of significant interest to dstl, with the intention of establishing a collaborative partnership, in order to improve the current solution offering for UK domestic counter-terror. This report has focused specifically on Computer Vision technology, identifying state-of-the-art applications that can enable real-time surveillance monitoring of densely populated public environments. Based on the analysis conducted within this report, a singular application - iCetana's autonomous video surveillance software - was determined to be the most well suited and beneficial out of all available options.

This report has aimed to present all of the necessary information and conduct all preliminary analysis required for dstl to make swift and informed decisions during any partnership talks that it engages in with iCetana. Of course, these talks are conditional on dstl agreeing to engage in such communication – such a decision is to be made by the key clients of this report; namely Dave Walker and Paul Kealey.

For reference purposes, this report has conducted analysis that models the potential cost and performance of the iCetana application within the London underground rail network. The results indicate that dstl can expect the estimated benefits of iCetana to fall within £3.25-£6.57 million in annual efficiency gains, given a monetary investment of between £23,000-£73,000 per annum; a return of 44-284 times the initial investment.

However, it is important to note, as detailed throughout section 7, that UK domestic counter-terror does not have a singular solve-all-solution. This report is not aiming to present iCetana's software application as such. As discussed throughout this report, there is a definitive need to incorporate a wide variety of solutions, legislative as well as technological, to help supplement the wider issue of UK domestic counter-terror. Potential action points that dstl can take include proactively partnering with the Surveillance Camera Commissioner, in order to implement supporting regulation to help ensure the efficacy of the iCetana solution as well as help to support areas for which the application is not best suited. If it is the case that the iCetana application can help relieve resource pressure and improve pre-emptive action, even if it is only within certain public environments, then this can be deemed a success and a benefitting feature of the UK's nationwide counter-terror surveillance practices.

9. NOTES ON LIMITATIONS OF ANALYSIS

It is important to note, due to the secrecy and sensitivity of some of the data surrounding this problem domain, that there have been limitations placed on my research. Information such as exhaustive lists of all current projects dstl is working on and all potential organisations dstl has noted interest in are inaccessible due to their sensitivity regarding national security.

Ideally, for my shortlisting analysis and research, I would have interviewed relevant members of dstl for information related to dstl's take on the assessed applications as well as the defined problem scope. This would have enabled me to confirm my assessment that the applications identified were truly relevant, rather than my actions being based on assumptions and hypotheses derived from secondary information.

I also acknowledge there will be nuanced differences when it comes to extrapolating this research to other areas of the UK. However, I believe the insights derived during this research are a good starting point for understanding potential benefits for any area of the UK in which there are densely populated urban environments.

Furthermore, when analysing the shortlisted application for potential benefits and costs, I had to rely on extrapolated data and strong assumptions in order to arrive at estimated values. Examples of this extrapolation can be found in section 5 and within Appendix 7; whereby I annualise the costs of utilising the application. Even if these figures are simply within the realm of possibility, they are solely intended to give a comparative evaluation of the application in order to give preliminary understanding to the clients of the report. If dstl is to engage in further communication with the iCetana, then more accurate and representative information will be required.

APPENDICES

APPENDIX 1: SUPPLEMENTARY TERMINOLOGY

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

Internet of Things (IoT) - The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data[2].

Jobs to be done (JTBD) – A theory of consumer action, it describes the mechanisms that cause a consumer to adopt a certain product or service to suit a particular need[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 isolates particular subjects and provides a 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" 2019*
[2] *Oxford dictionary, 2020*
[3] *Klement, 2016*
[4] *Morris, 2004*
[5] *dstl "The dstl Biscuit Book" 2019*
[6] *Ibid*
[7] *Ibid*

APPENDIX 2: PRELIMINARY LIST OF SUITABLE APPLICATIONS

Below is an aggregated list of all of the 24 applications that were analysed at the beginning of this report. This detail is included for reference and summarisation purposes, you can find a detailed list of all 24 applications in Appendix 11 of Part I of this report. Supplementary information regarding operating locations and funding amount to date has also 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

APPENDIX 3: NOTES ON SPECIFIC FUNCTIONALITY OF POTENTIAL APPLICATIONS

Below is the list of 24 preliminary relevant applications, each with a brief discussion of the fundamental features of its product offering that make it unique and distinctive. This is important in order to understand and appreciate the similarities and differences between all of the applications. This list was helpful when first conducting the assessment analysis on each of the given applications.

Name	Notes on specific functionality
Deep Sentinel	Proprietary camera sensor unit that connects to smart hub which is reviewed by human operators.
iCetana	Software integrates with existing video infrastructure, providing a smart automated filter to show to human operators only scenes of potential interest.
IntelliView	Proprietary camera systems that produce combined analysis from their joint thermal and visual sensors to provide a more holistic and sophisticated automated detection system.
Prophesee	Patented vision sensor enables for distinctive speed and quality of vision capture.
Shield AI	Drone technology camera system technology that aims to increase the scope of useful visual data captured.
Signal Innovations (BAE Systems)	An automated monitoring platform that incorporates data from numerous sources in order to detect any predetermined events of interest.
Stanley Security Systems	Specialise in integrated video surveillance equipment - bespoke installations of specialised hardware for automated defence monitoring.
Umbo	Proprietary camera sensors that aim to reduce the cost and improve quality of video capture. Additionally, have a software feature (Umbo Light) that focuses on analysing and identifying human activity; usually incorporated into an all-in-one packaged product.
VideoIQ - Now part of Avigilon	Patented software aims to detect solely actions and events of concern, flagging these events to human operators. It additionally aims to learn from these actions to produce predicted monitoring.
Vii Sights	Holistic analysis platform to detect activity. Notably slow performing (could class as only near-real-time) also requires a distinct aerial camera to be optimised.
Yitu	Requires largescale infrastructure deployment (of standardised camera units) to execute its platform suite.
Athena Security	Software developed to screen video analysis from any existing CCTV - with a key detection focus on weaponry as of current.
Cortexica	Proprietary software for distinct object recognition in working environments. They specialise in consultative work that can tailor the needs of the models to meet predetermined requirements.
D-ID	Software utilises parameters of a person to identify and log their activity, flagging any potential threats, whilst maintaining anonymity due to natural blurring and disregard for face and personal information.
Evolv	Static screening device that detects for specific objects, through Computer Vision technology, when individuals pass through, much like traditional X-Ray machines - though has cost and speed advantages.
Lumineye	Hardware module and software component that enables for short-distance object penetration screening. Helping supplement other monitoring and surveillance techniques.
Traces AI	Software that incorporates and utilises over 2000 parameters of any given individual in order to track and monitor for any specific suspicious activity.
Video Intellect	Software suite that aims to flag and predict potential threats, with a focus on integrating all video sources into a single, controllable network platform.
AgentVi	Software that can be tailored for the detection to become specialised and rule-based, with events on the integrated camera network being flagged when the desired activity is detected.
Anduril	Drone technology with proprietary software network architecture that enables for continuous and highly integrated monitoring of events, specialising in passive surveillance of points of interest.
Digital Barriers	Proprietary hardware that enables for real-time surveillance monitoring, utilising Computer Vision and IoT technologies.
Huawei Safe City Program	Largescale infrastructure deployment scheme that enables integrated and automated (and potentially predictive) surveillance on its platform suite.
Magal Security Systems	Full-suite integrated platform that requires proprietary hardware to be installed. Focuses on smaller individual and corporate products as of current.
SDI Presence	Full-suite integrated platform that requires proprietary hardware to be installed. Focuses on smaller individual and corporate products as of current.

APPENDIX 4: NOTES FROM STAGE 1 OF SHORTLISTING APPLICATIONS

Below are the results from assessing each application against the proprietary assessment framework, as summarised in section 4, tabulated with accompanying labels.

Name	Q1	Q2	Q3	Q4	Q5
Deep Sentinel	Yes - but still reliant on human operator review		Proprietary camera units make it difficult to integrate		
iCetana					Subject to further Assessment
IntelliView	Their tool is predominantly a supplement for other tools to utilise for this particular task		Proprietary camera units make it difficult to integrate		
Prophesee			Proprietary camera units make it difficult to integrate		
Shield AI			Software component can be integrated, the drone hardware technology can be seen as a supplement		As of current, the technology is only beneficial within drone surveillance, making it tricky for the UK to truly benefit without significant investment
Signal Innovations (BAE Systems)		Software has been acquired by BAE systems Intelligence & Security Inc., which is solely a US defence contractor			
Stanley Security Systems			Consultative, specialised nature of their camera systems make it difficult to scale to the UKs infrastructure		
Umbo					Subject to further Assessment
VideoIQ (Now part of Avigilon)					Subject to further Assessment
Vii Sights					Notably slow performing (could class as only near-real-time) and requires aerial footage to be optimised
Yitu		Chinese state-run components to this business, which makes for highly difficult regulatory compliance			
Athena Security					Subject to further Assessment
Cortexica	This tool shows promise with capability, yet has not been purpose-built for the issue domain of counter-terror				The current lack of focus means that this would translate to direct and immediate benefits.

D-ID	Their tool is predominantly a supplement for other tools to utilise for this particular task				The benefits are less direct from this tool, and hence does not favour any cost-benefit analysis
Evolv	Perhaps too specific of a object recognition device for any incidents to be detected or predicted		Screening device - hard to position at all points of interest. Then also argue that these would become new areas of terrorist focus		
Lumineye	Their tool is predominantly a supplement for other tools to utilise for this particular task		Despite the hardware component being easily installed, it is hard to scale and generalise to UK infrastructure		
Traces AI					Subject to further Assessment
Video Intellect		Russian focused and headquartered business, which makes for highly difficult regulatory compliance			
AgentVi					Subject to further Assessment
Anduril			Software component can be integrated, the drone hardware technology can be seen as a supplement		Unlike ShieldAi, Anduril has a stand-alone software package (Lattice AI) - Subject to further Assessment
Digital Barriers					Subject to further Assessment
Hauwei Safe City Program		Chinese state-run components to this business, which makes for highly difficult regulatory compliance			
Magal Security Systems			Consultative, specialised nature of their camera systems make it difficult to scale to the UKs infrastructure		
SDI Presence			Consultative, specialised nature of their camera systems make it difficult to scale to the UKs infrastructure		

APPENDIX 5: NOTES FROM STAGE 2 OF SHORTLISTING APPLICATIONS

Below are the notes made during the second stage of the shortlisting process on the five applications that were omitted based on the results of this analysis. Explanations are given for each of the application's omission. These notes formed the basis of the summary of the shortlisting process in the main body of the report, section 3.

AGENTVI

AgentVI is the company in this list with the most experience developing applications for this problem space, operating for close to thirteen years in the field (Agent Video Intelligence Ltd., 2020). Despite their security surveillance capabilities and experience, all of their experience integrating with UK infrastructure has been for enterprise and other purposes unrelated to the problem scope – the two prominent examples within the UK have been for resource management at both Wirsol Solar Farms and the National Exhibition Centre (Agent Video Intelligence Ltd., 2020). Furthermore, AgentVI's software is one that is compatible with a subset of defined technology vendors. The list of vendors capable of integration, based on their online documentation, was cross-referenced to the vendors in current partnership with TfL (Delatim and Telent, as defined in the previous section were applicable). Unfortunately, due to AgentVI's specialism with US-based technology vendors and infrastructure, the two relevant vendors were not on the compiled list of compatibility.

ATHENA SECURITY

Athena's software specialises in object recognition capabilities, specifically with regard to weaponry such as guns and knives – its unique selling point is its efficient and accurate detection of individuals carrying and operating such objects (Athena Security Inc., 2020). The UK is known for enforcing strict gun control and as a result terrorists, especially lone wolf attackers, have most often resorted to weaponry that is more subtle – for example, November's London Bridge attacker was armed with a kitchen knife (Edwards, 2019). Therefore, it may be the case that this software solution is too specific and not generalised to nuances that could potentially be relevant. Additionally, all of Athena's case studies so far have been physical institutions such as High Schools in Southern USA (Athena Security Inc., 2020). This furthers the concern that Athena's solution is perhaps too focused, despite seeming very promising with regard to specific object recognition, and there may applications more suited and exhaustive with their analysis, such as iCetana and Umbo.

TRACESAI

Traces incorporates software that aims to dynamically assess and identify individuals based on a holistic set of features, incorporating 2000 parameters of every given individual. Their performance, with regard to personal identification, conclusively surpassed all known competition in an assessment at NeurIPS Conference – the largest scientific conference in AI (Traces, 2020). However, like Athena, Traces' current application experience is of potential concern for being too specialised and not on an all-round holistic solution such as iCetana. Additionally, for Traces' software to perform on 1,000 or more cameras requires a server appliance in order to manage computational demand (Traces, 2020). This makes Traces appear less suitable and cost-inefficient for large infrastructure wholescale surveillance, not to mention the required server appliance technology is not accommodated by any of the current technology vendors for TfL.

APPENDIX 5.2: NOTES OF ANDURIL AND VIDEOIQ

ANDURIL

Currently, Anduril has established one potential UK partnership; providing technology services for the UK Royal Marines. Anduril has an integrated software solution, known as Lattice AI, that is of most relevance to the tightly defined problem scope of this report. However, all of Anduril's current field-tested experience with Lattice AI has been in a military setting – whereby the scale of infrastructure is not as constrained as in public civilian environments. For example, Anduril's Lattice AI's unique selling point is the integration of numerous camera systems to develop exhaustive pre-emptive analysis of a given surrounding. In public environments, such as within London's underground network, there is a real constraint on the type and extent of equipment that is in place. Therefore, based on the reasoning that Anduril's software performs best in military-based environments, perhaps Anduril's solution is not the most justifiable application.

VIDEOIQ (AVIGILON)

Avigilon, the acquirer of VideoIQ's proprietary software, has already launched three specific projects for automated security surveillance within the UK. These projects are for:

- Lincolnshire County Council; utilising Avigilon's solution to protect £12 million worth of road safety equipment.
- 20 Old Bailey; upgraded their security system to Avigilon's solution to provide tenant security and incorporate direct communication to Metropolitan Police.
- Looe Town Council; utilising Avigilon's solution to ensure safety of both residents and tourists. (Avigilon, 2020).

Despite these seemingly applicable and highly relevant case studies, whereby the clients have indicated their satisfaction with the performance of Avigilon's solution, there are some underlying downfalls with Avigilon's technology that may be of some concern for the purposes of dstl's problem statement. There is a lack of demonstrated predictive capabilities with this solution. Additionally, the software solution appears to be tailored towards the unique selling point of cloud-based processing and management of legacy CCTV surveillance cameras (Avigilon, 2020). This weakens Avigilon's potential of being a strongly recommended application, due to other similar applications being capable of much more sophisticated analysis.

APPENDIX 5.3: NOTES OF DIGITAL BARRIERS AND UMBO

DIGITAL BARRIERS (https://digitalbarriers.com/)

A global organisation that already operates within the UK, Digital Barriers has developed a platform-as-a-service software package for real-time autonomous surveillance monitoring. Digital Barriers' software platform solution can be integrated into existing camera CCTV equipment, regardless of type or supplier (Digital Barriers, 2020). Digital Barriers offers numerous software platform products, the one that is relevant to this problem domain is titled "Safe City". The software product results in autonomous surveillance of densely populated public environments; such as sporting events, transportation hubs and major public roads (Digital Barriers, 2020). Digital Barriers has successfully deployed its product within London's infrastructure; at The O2 entertainment facility.

Additionally, Digital Barriers' integrated software solution, based on wireless connectivity of its modules with pre-existing CCTV equipment, is said to use 60% less computational resources due to the reduction in data transfer required, compared to other similar wireless solutions (Digital Barriers, 2020). However, like Umbo, the performance and extended capabilities of the Digital Barriers platform is constrained by the use of its wireless interconnected proprietary camera systems. This is a significant drawback, which makes a solution such as iCetana that much more desirable.

UMBO (https://umbocv.ai/)

A global organisation that already operates within the UK, Umbo is a company predominantly developing hardware camera sensor modules, with a focus on making cost-effective and cloud-integrated surveillance systems. However, they also have a software package, termed Umbo Light, that focuses on real-time automatic analysis of human activity, monitoring for suspicious activity. Umbo's software solution, Umbo Light, can identify human events utilising algorithms that map human actions. This technique is claimed to be more accurate than other analytics products; in an Umbo experiment, Umbo Light was reportedly 10x more accurate than standard-issue current intelligent surveillance platform (IVS) (Umbo Computer Vision Inc., 2020). However, this performance is constrained by the precondition of utilising Umbo's proprietary hardware, which – despite being relatively cost-effective – is a significant drawback compared to a solution such as iCetana.

Additionally, Umbo Light results in real-time alerts, notifying of potentially threatening activity on a proprietary event dashboard, which is intended to be monitored by human operators (Umbo CV, 2019). However, there is concern that this will result in an issue of an event log pileup, with human operators still bottlenecking the system when it comes to real-time surveillance.

APPENDIX 6: ANALYSING TFL CONTRACTS TO IDENTIFY RELEVANT TECHNOLOGY VENDORS

In Part I of this report, the current infrastructure system within the UK – regarding regulation and coverage of CCTV surveillance - was discussed and analysed in detail. Here in Part II, further analysis was undertaken to more precisely identify which of the applications are of most relevancy and benefit to dstl. Below is the final output from the analysis on the TfL database detailing all current contracts in place with a value over £5,000 with technology vendors. The entries below are the contract agreements relevant to supplying, monitoring and supporting CCTV equipment integration.

Contract Title	Contract Description	Earliest Expiry Date	Value Band	Vendor Name
TfL01230 - 1FM CCTV, Access Control and Security Systems	Maintenance, Upgrade and Replacement of TFL CCTV, Access Control and Security Systems	31/03/2027	£25M - £50M	Telent Technology Services Limited
Manufacture and Supply of Saloon CCTV for Central Line 92TS	Design, Manufacture and Supply of CCTV for Central Line 92TS Improvements. Contract includes two agreements. MSA and SSA - in line 20072	14/06/2024	£1M - £5M	Delatim Limited
Central Line One Person Operation CCTV Improvement Project	Works contract for the testing, selection, installation and handover of replacement CCTV cameras at up to 39 Central Line stations.	25/02/2020	£250K - £500K	Telent Technology Services
Reconfiguration of PAVA and CCTV within Westminster Iceberg Retail Unit	Reconfiguration of PAVA and CCTV within Westminster Iceberg Retail Unit	31/12/2019	£5K - £250K	Telent Technology Services Ltd (vendor no.13000145)

Telent Technology Services Limited ('Telent') is a service provider of communication networks related to UK National infrastructure, with a specific focus on UK public safety. It offers a wide variety of services, from consultancy to operating the solutions directly, with industry sectors including Rail, Traffic and Defence[1].

Similarly, Delatim Limited ('Delatim') is a security & telecoms services contractor. They develop and implement constructions for clients within the Transport and Public sectors, including others[2].

Both companies provide their services to Transport for London, developing and implementing surveillance camera modules within areas of the London underground rail network.

[1] *Telent, 2020*
[2] *Delatim, 2020*

APPENDIX 7: ANALYSING iCETANA'S FINANCIAL STATEMENTS

Below is an excerpt from iCetana's 2019 Financial Income Statement, whereby they detail the aggregated revenue derived from the cost of goods sold (COGS):

iCetana Pty Ltd
Consolidated statement of profit or loss and other comprehensive income
For the year ended 30 June 2019

	Note	2019 $
Revenue		
Sales revenue	3	1,407,405
		1,407,405
Other income		
Grant income		-
Interest income		6,171
Other income		602,061
		608,232

From their reported case studies, documented within their White Papers, it is reasonable to assume that iCetana was installed on approximately 50,000-100,000 (rounded for simplicity) camera modules within the financial period ending 30 June 2019. The range provided is so dramatic to accommodate for the significant uncertainty facing this estimate – providing a range whereby a low-uptake and a high-uptake scenario are adjusted for. From this range, we can assume that based solely on COGS, it would cost the UK Government an estimated $14.07-$28.15 (approximately £11-£22) per camera to integrate iCetana's software.

APPENDIX 8: CALCULATIONS TO INFORM ECONOMIC CONSIDERATIONS

APPENDIX 8.1: ANNUALISING THE COST OF ICETANA

This extrapolated per unit COGS needs to be annualised for the purposes of further understanding the costs involved with utilising iCetana's software. The resulting calculation, using the values defined within the main body of the report, is as follows:

$$Equivalent\ Annual\ Cost = \frac{£10.8\ x\ 3.5\%}{1-(1+3.5\%)^{-5}} \text{ to } \frac{£21.6\ x\ 3.5\%}{1-(1+3.5\%)^{-5}}$$

Therefore:

$$Equivalent\ Annual\ Cost = \sim £2.44 - £4.87$$

If there are approximately 15,000 cameras in operation within London's underground rail network, this would translate to a cost of £36,544.42 - £73,088.85 (assuming that all cameras were replaced and installed within the same time period). However, we should adjust for uncertainty, whereby it is reasonable to assume that not all cameras will implement iCetana directly and immediately – a modest assumption would be to assume that approximately 60% of cameras have an uptake in iCetana's software. Therefore, this range of possible values, based on the possibilities of a low- or high-uptake for both iCetana's global coverage as well as the coverage within TfL's camera system, is displayed in the below matrix. (Answers are rounded to the nearest thousand for simplicity):

(Cols) iCetana's COGS (Rows) TfL's Integration	Low Scenario	High Scenario
Low Uptake	£22,000	£44,000
High Uptake	£37,000	£73,000

APPENDIX 8.2: EXTRAPOLATING PERFORMANCE METRICS

There are many statistics that appear to demonstrate efficiency gains and cost savings regarding the iCetana software, yet most are self-reported. Before we can conduct analysis based on these metrics, it is important to attempt to validate these figures through independent client testimonials. For example, two years ago the Middle Eastern retail giant Majid Al Futtaim (MAL) implemented iCetana for the purposes of security and predictive surveillance[1]. Within the first six months of implementation, MAL observed a 10% reduction in their manned security budget. They also self-reported metrics, such as 15% reduction in operational costs, that appear to validate and confirm the metrics that iCetana claims within its own documentation. Therefore, it is not unreasonable to utilise iCetana's metrics in turn to develop estimations for the benefits that could be yielded by TfL.

If TfL were to experience success when implementing iCetana somewhat similar to MAL, then we can quantify the monetary savings that would result. This assumption is not too far-fetched, as the goal in both environments is predictive autonomous surveillance, whereby one public environment involves public transport and the other involves retail facilities (iCetana is already implemented successfully in a variety of these types of environments). Of course, we should accommodate for uncertainty and variability in our estimates and provide a range of plausible answers to help demonstrate the potential impact. The calculations for these estimates are detailed below:

The British Transport Police (BTP) allocate £56 million per year on underground policing[2]. Recorded within this cost are a lot of different features, not only the monitoring of - and response to – potentially suspicious CCTV activity. 2% of the overground BTP policing budget is allocated to CCTV monitoring – extrapolating this percent to the underground budget gives a value of £1.12 million. If, similar to MAL, 5-15% of this budget can be saved due to the implementation of iCetana, then this will translate into a saving of £56,000-£168,000 per annum. This 2% metric perhaps neglects some of the costs that could be associated with this issue, such as emergency response to potential at-risk situations. However, we can accommodate for this through the costs associated with emergency response within the underground network; this cost is reported to be approximately £32 million[3]. A 15% reduction in this cost due to operational efficiency, such as what MAL experienced, would be highly dramatic. However, as discussed in the main body of the report, iCetana would enable more efficient allocation of BTP police officers, perhaps removing the 'bobbies on the beat' strategy in order to ensure proactive coverage. Therefore, a 10-20% reduction is more than plausible. This would translate to cost savings of approximately £3.2-6.4 million per annum.

[1] *Majid Al Futtaim, 2019*
[2] *British Transport Police Annual Report, 2019*
[3] *Ibid*

APPENDIX 9: QUID® RESEARCH OUTPUTS

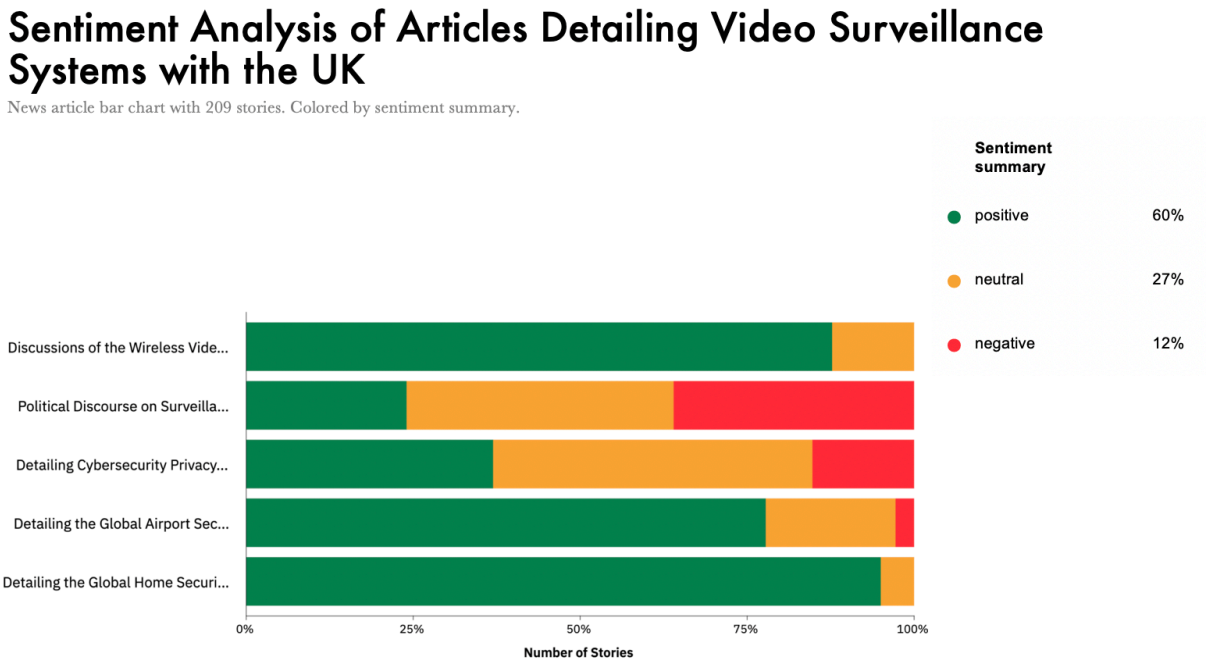
APPENDIX 9.1: LIST OF HIGHLY RELEVANT SEARCHES

Accompanying the 25 distinct searches undertaken for the purposes of the industry scoping analysis for Part I of this report, there were 5 searches that are directly relevant to the formation of the subset of applications analysed in Part II of this report. These searches are tabulated below:

Search Iteration Number	Database	Boolean Search	Goal of Search	Result
1	Companies	("counter terror" * OR "public safety") AND ("real time" OR "autonomous") AND ("surveillance")	To provide a benchmark understanding of all of the possible technological applications that meet the specific scope created.	74 Companies
2	News & Articles	("counter terror" ~ 5 OR "public safety" ~ 5) AND ("video surveillance" ~ 5) AND tech *	To understand the current, highly relevant, state of the art that was being discussed, to see if anything had been missed from preliminary research.	430 stories, 26% unique
3	News & Articles	("counter terror" ~ 5 OR "public safety" ~ 5) AND ("video surveillance" ~ 5) AND tech * AND (predictive OR "real time")	To focus the previous search on the key components of the narrow scope developed; real-time predictive surveillance.	173 stories, 26% unique
4	Companies	("counter terror" * OR "public safety") AND ("real time" OR "autonomous" OR "predictive") AND ("surveillance" OR "video" OR "camera")	An attempt to enhance the first search, and to increase the net of captured companies, by including the component of predictive surveillance for camera hardware into the search.	175 Companies
5	Companies	("counter terror" *) AND ("real time" OR "autonomous" OR "predictive") AND ("surveillance")	Highly specific search, that aims to see which (if any) companies describe themselves as operating within the tightly defined scope of the problem statement.	8 Companies

APPENDIX 9.2: 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. As referred to in the main body of this report, we can see that as a whole, the sentiment regarding the topic of video surveillance is 60% positive.

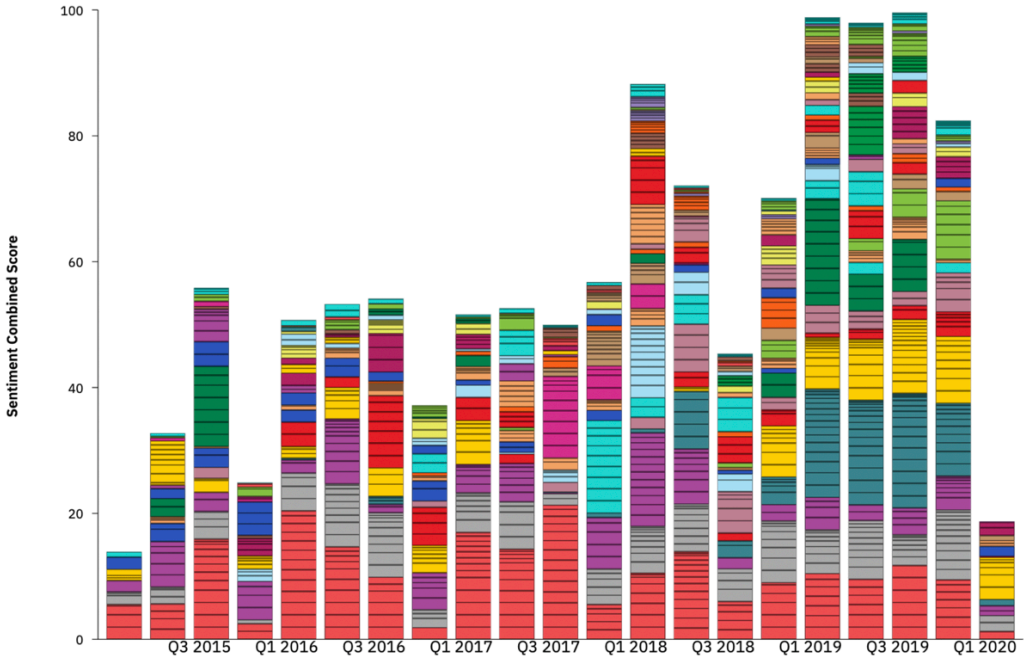


Source: Quid®

Furthermore, a more extensive search has been conducted that compiles articles that go back as far as the 21st January 2015. The purpose of the below Quid® output is to visualise how the overall sentiment of public discourse has progressed over the last five years. As visualised below, there is a clear positive increase in overall public sentiment during this period, further evidencing the trend of increased positive public perception with regard to surveillance analysis techniques.

Quarterly View of Sentiment Progression

News article timeline with 1254 stories. Colored by clusters.



Source: Quid®

APPENDIX 10: FURTHER DISCUSSION OF SUITABLE IMPLEMENTATION LOCATIONS

As discussed within the main body of the report, it is important to identify key preliminary areas of interest, that dstl and the Surveillance Camera Commissioner can focus their attention and analysis on, to help speed up the implementation process. These areas of interest need to meet the remit as defined within the problem statement; they need to be densely populated public environments, that have the infrastructure capabilities to enable effective and comprehensive coverage of iCetana without any significant further investment. Three potential areas of interest are categorised below, with the reasoning for each included:

TFL RAIL NETWORK

The London Underground rail network has been of distinct focus within this report and it has been demonstrated that it is a highly suitable and effective first point of interest for the implementation of iCetana. When compared to other alternative public transport systems, the TfL rail network provides excellent surveillance coverage due to the equipment currently in place; as discussed, there are approximately 15,000 surveillance cameras within the London underground rail network. Additionally, the tightly confined spaces make this an important area of initial interest for two reasons. First, it ensures that all surveillance coverage is optimised, as much as currently possible, due to the narrow lanes of access for individuals whilst navigating the underground rail network – it is impractical to avoid surveillance equipment whilst utilising the network. Second, this tightly confined space is a known area of interest for potential terror attacks – evidenced through past attacks, foiled or otherwise. Therefore, the TfL rail network serves as an ideal area of preliminary interest for implementing the iCetana application.

SHOPPING COMPLEXES SUCH AS WESTFIELD™ AND SELFRIDGES™

Major shopping complexes and department stores, that are based within a single building or site, are another point of initial interest for implementing iCetana. These complexes have large volumes of public foot-traffic each day, which will help iCetana maximise its operational effectiveness. Additionally, these complexes are privately owned, and due to incentives to ensure public safety and to mitigate theft and other criminal activities, their owners install comprehensive surveillance equipment. It should be noted that the coverage is not as domineering as within the London underground rail network, yet there are sufficient cameras installed in any given site for iCetana to be effectively launched. Furthermore, these private complexes are already monitored intensely through human-operated Video Management Systems (VMS) – thereby there is great room for efficiency gains due to the performance and nature of the iCetana software.

ENTERTAINMENT AND SPORTING STADIUMS SUCH AS THE O2™

Much like the reasoning behind selecting large shopping complexes, large stadiums – be it for sporting or entertainment purposes – are another ideal area of initial interest. For example, the O2™ already implements the Digital Barriers surveillance package (see Appendix 5.3). This location, much like many other stadiums, could directly benefit from implementing iCetana's software to help automate and improve the efficacy of the human-monitored VMS platforms.

MSIN0032 SUPPLEMENTARY APPENDICES

APPENDIX 1: IDENTIFYING SKILLS FROM THE PROGRAM UTILISED DURING THE DISSERTATION

Below are short descriptions of the key skills, components and frameworks utilised from each relevant module of the BSc Management Science program that have helped me throughout the development of this dissertation.

Art and Science of Management – The entire premise of my report was derived from a key thread within the Art and Science of Management (ASoM) module. Whereby I first observed and described the current problem (demonstrated throughout the entirety of Part I) and then compare relevant applications in detail (demonstrated throughout section 3 of this report) to eventually understand, in detail, the most suited potential partnership opportunity for dstl. Understanding the key content of ASoM helped structure my thinking, enabling me to analyse this massively complex managerial problem.

Behavioural Science – Section 12 of Part I as well as section 7 of this report both provide commentary and analysis on the difficulty of changing public opinion, as well as evidence the shift in psychological sentiment surrounding surveillance techniques whilst utilising the Quid® intelligence platform. Additionally, the psychology of 'lone wolf' terrorism has been discussed in numerous sections of this report as well as during Part I, such as section 13 of Part I – whereby the potential emotional motivators of a lone wolf terrorist are considered.

Critical Analytical Thinking – Throughout my report I have been required, implicitly as well as explicitly, to implement the skills learnt throughout the Critical Analytical Thinking (CAT) module. From implementing directly tangible skills such as evaluating sources, such a skill is explicitly demonstrated within section 5 of this report whereby I corroborate the evidence provided by iCetana, to more implicit skills such as synthesising a large complex issue such as the current legal structure applicable to this particular problem into insightful and coherent takeaways for the intended client of the report (section 8 of Part I).

Computational Thinking – Entire concepts related to the key technology and the general application of such technology were first introduced within this module. Concepts such as space, memory and time constraints, as well as the practice of training and validating particular algorithmic models were a key component of this module. These principles were most prevalent whilst conducting the shortlisting assessment of each (section 3), as well as in the detailed explanation of the core functionality of the shortlisted application (section 4).

Data Analytics – Similar to the Computational Thinking module, Data Analytics II further distilled the notions of training, validating and testing models involving large data. This knowledge helped me incorporate key discussion points within section 3 and 7 of this report. Furthermore, the practical limitations of algorithmic models as well as the necessity to have high quality and directly relevant data were key topics present within both Data Analytics modules – this topic is directly relevant during the shortlisting analysis undertaken within the section 3 of this report.

Design Thinking – It was useful, for my own understanding and to structure my approach to shortlisting applications, to implement Design Thinking frameworks and frame the problem as a product-market-fit issue. This enabled me to utilise frameworks such as the 'Five Whys' and concepts such as 'Jobs to be Done'. These frameworks and concepts were useful with helping to understand how a particular application served at solving the roost cause issue that was established during this dissertation. Additionally, the concepts of iterative and responsive design are present, even if mildly implicit, throughout the implementation roadmap within section 6.

Mathematical Foundations of Management - The formulae applied to the economic assessment conducted in this part of the report (section 5) were present during Mathematical Foundations of Management (MFoM) I, whereby directly relevant formulas within linear algebra as well as the concept of annuities were introduced.

Intelligent Systems – My Integrated Engineering Program (IEP) minor helped when it came to understanding the fundamental components of Artificial Intelligence and sub-domains such as Computer Vision. During this course, the limitations and constraints, as well as prospective applications of such technology, were explored in detail. This module served as a key inspiration point for this dissertation, whereby the entire space of different application areas that can face innovation and change due to increasingly sophisticated intelligent agents were explored and assessed in detail. Thereby, this course helped during the project proposal and idea formation stages, providing as a key reference point for what intelligent agents are capable of – the combination of this and my interest in UK national defence and security is what led me to explore this particular problem domain. Furthermore, key topics present within this module have been utilised throughout this report, such as during the discussion of limitations (section 7) to iCetana's software application – where practical constraints that we gained an understanding of during this module are applied to this particular context.

Finance – Finance II helped establish a key understanding of the principle of discounting and spreading costs over the given lifetime of a particular asset – this is the guiding principle found during my economic assessment in section 5 of this report. Furthermore, Finance II introduced the key financial statements reported by organisations – this helped when navigating the income statement reported by iCetana, helping me correctly identify the COGS line item for the purposes of my analysis.

APPENDIX 2: RECORD OF UTILISING MY SUPERVISOR

Below is a table documenting the times that I utilised my Dissertation Supervisor within Part II of my report. 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 Part II of 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
22/01/20	To confirm the POA for Part II analysis and outcomes	**The goal of the final output from my research** - I want to run by you the potential plan of action I have for how I want to direct my research and analysis, for the second part of my report. I want to confirm whether you agree with my intentions to direct most of my analysis towards shortlisting the relevant applications, resulting in a discussion on implementation and potential limitations to any shortlisted application(s). **To confirm the intended scope of Part II is sufficient and desirable -** I want to just run by you my preliminary idea that perhaps a singular application will become the main focus of the final stages of my report. I want to sense-check whether you believe this will allow me to demonstrate my ability and skills effectively, even within this tight scope of analysing a singular application.	• It is okay to focus in on a single application, as long as it is thoroughly justified through analysis and evidence. The focus can be more in-depth and insightful this way. • It is okay to use secondary data for extrapolation, yet for any analysis and estimations that contain variability, it is best to accommodate for this utilising an interval of value (this is perhaps best placed in the annualised cost section). • Regarding modelling the performance of the application, it is fine to use abstracted models that are only related to the application in question – just make sure this is stated and the relationship is evidenced. • Providing action points for dstl is a fine way to conclude the report, just make sure that the points are formed cohesively throughout the report and are evidenced sufficiently to be justified.	It is okay to develop conclusions based on indirect and extrapolated data – this skill is necessary not only in research reports but in the real world too. The skill of implicitly identifying the correct information and modelling the data to ensure it is as accurate as possibly can be is key. The end goal of this report is to ensure that dstl are well informed if they so choose to pursue the application of choice. That goal needs to flow through the entirety of this report.
	To provide a preliminary draft check and offer feedback on my current progress	**To understand if the structure of the flow of the report makes sense for the reader** – I want to understand if the current structure and ordering of the systems make logical sense and inform the reader in the most coherent manner. I also want to understand if the report appears exhaustive in nature and to identify if there may be any holes in my coverage and analysis. **To evaluate whether the conclusions provided, and the results provided at the end of the report is informative enough** – I want to confirm that the conclusions stated within the final section of the report make coherent sense based on the arguments formed throughout the report. I also want to assess whether the action points offered to the client at the end of the report are adequate and sensible, based on the content of the entirety of my dissertation.	• The flow and overall structure of the report are fine. The information included as well as the resulting conclusions are rational and well supported. Perhaps a few of the premises can be strengthened through slightly more information being included (even if this is just gathering supporting information from the Appendices and incorporating it into the main body of the report). • Please ensure that you incorporate timeframes into all suggestions and analyse results you discuss. Additionally, please ensure all assumptions related to calculations are (if only briefly) explained in the main body of the report.	Reconcile the minor comments that have been made to a small component of the main body of the report – these include refining explanations, including summarising sentences at the top of sections as well as accommodating for the development of technology over time when discussing objections and analysing suitable applications.

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).

Agent Video Intelligence Ltd. (2020) *Customer Stories.* Available at: https://www.agentvi.com/customer-stories/ (Accessed: 07 January 2020).

Agent Video Intelligence Ltd. (2020) *Product Overview.* Available at: https://www.agentvi.com/ (Accessed: 07 January 2020).

Athena Security Inc. (2020) *Product Overview and Case Studies.* Available at: https://athena-security.com/ (Accessed: 07 January 2020).

Australian Department of Defence. (2020) *The Technical Cooperation Program.* Available at: https://www.dst.defence.gov.au/partnership/technical-cooperation-program (Accessed: 09 January 2020).

Avigilon. (2020) *Case Studies.* Available at: http://avigilon.com/case-studies/ (Accessed: 07 January 2020).

Avigilon. (2020) *Product Overview.* Available at: http://avigilon.com/products/ (Accessed: 07 January 2020).

BAE Systems. (2020) *Intelligence and Security Organisation.* Available at: https://www.baesystems.com/en/our-company/our-businesses/intelligence-and-security/capabilities-and-services/intelligence-surveillance-reconnaissance (Accessed: 09 January 2020).

Blakey, A. (2020) *Government Committed to Martyn's Law.* Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/government-committed-making-martyns-law-17554598 (Accessed: 23 January 2020).

British Transport Police. (2019) *Annual Report 2018-19.* Available at: https://www.btp.police.uk/PDF/BTP_Annual_Report_2018_2019.pdf (Accessed: 12 February 2020).

BSIA. (2016) *An Introduction to Video Content Analysis.* Available at: https://www.bsia.co.uk/Portals/4/Publications/262-introduction-video-content-analysis-industry-guide-02.pdf (Accessed: 14 January 2020).

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: 20 January 2020).

CPNI. (2016) *Storage of recorded CCTV Images.* Available at: https://www.cpni.gov.uk/system/files/documents/c9/87/Storing-of-recorded-CCTV-images.pdf (Accessed: 03 January 2020).

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).

CSIS. (2019) *Analysis of Huawei's Safe Cities.* Available at: https://www.csis.org/analysis/watching-huaweis-safe-cities (Accessed: 09 January 2020).

Digital Barriers. (2020) *Product Overview and Case Studies.* Available at: https://www.digitalbarriers.com/solutions/wireless-safe-cities/ (Accessed: 07 January 2020).

Delatim. (2020) *Security and Telecomms Services.* Available at: http://delatim.co.uk/security/ (Accessed: 03 January 2020).

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: 02 January 2020).

Dstl. (2019) *Serapis framework documentation.* Available at: https://www.gov.uk/government/publications/dstls-serapis-framework (Accessed: 05 February 2020).

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: 14 February 2020).

Edwards, J. (2019) *The London Bridge terror attack shows why really strict gun control is a very, very good idea.* Insider. Available at: https://www.insider.com/london-bridge-attack-and-gun-control-2019-11 (Accessed: 09 January 2020).

Home Office. (2019) *List of terrorist groups and attacks.* Available at: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2 (Accessed: 09 January 2020).

HM Treasury. (2018) *Central Government Guidance on Appraisal and Evaluation.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf (Accessed: 14 January 2020).

iCetana. (2020) *Financial Statements.* Available at: https://icetana.com/presentations-reports/ (Accessed: 14 January 2020).

iCetana. (2020) *Product Overview and Case Studies.* Available at: https://icetana.com/icetana-product-overview/ (Accessed 07 January 2020).

iCetana. (2019) *Technical Data Sheet.* Available at: https://s.icetana.com/wp-content/uploads/2019/02/iCetana-Datasheet-20190121-1.pdf (Accessed: 09 January 2020).

Klement, A. (2016) *What is Jobs to be Done?* Available at: https://jtbd.info/2-what-is-jobs-to-be-done-jtbd-796b82081cca (Accessed: 28 January 2020).

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

Majid Al Futtaim. (2019) *iCetana Case Study.* Available at: https://s.icetana.com/wp-content/uploads/2019/02/iCetana-Retail-case-study-1.pdf (Accessed: 12 February 2020).

Mitsa, T. (2019) *How do you know you have enough training data?* Towards Science. Available at: https://towardsdatascience.com/how-do-you-know-you-have-enough-training-data-ad9b1fd679ee (Accessed: 08 January 2020).

Morrison, C. (2018) *Terrorist Attacks Cost the UK £3 Billion Last Year.* Available at: https://www.independent.co.uk/news/business/news/terror-attacks-uk-economy-cost-manchester-arena-westminster-london-bridge-a8385661.html (Accessed: 14 January 2020).

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: 02 January 2020).

ONS. (2019) *Population Estimates for the UK.* Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland (Accessed: 20 January 2020).

Oxford Dictionary. (2020) *Internet of Things defined.* Available at: https://www.lexico.com/definition/internet_of_things (Accessed: 28 January 2020).

Silva, M. (2014) *The useful life of surveillance equipment.* Available at: https://ipvm.com/forums/video-surveillance/topics/useful-lives-of-surveillance-equipments-versus-depreciation-rates (Accessed: 14 January 2019).

Smart, T. (2020) *How much does a CCTV installation cost?* Available at: https://www.smartaerials.co.uk/blog/how-much-does-a-cctv-installation-cost [Accessed 29 February 2020]

Surveillance Camera Commissioner. (2020) *Annual Report 2017/18.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_d

ata/file/772440/CCS207_CCS1218140748-001_SCC_AR_2017-18_Web_Accessible.pdf (Accessed: 03 January 2020).

Surveillance Camera Commissioner. (2018) *A National Surveillance Camera Strategy for England and Wales.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/608818/NSCS_Strategy_post_consultation.pdf (Accessed: 14 January 2020).

Telent. (2020) *Technology Services.* Available at: https://telent.com/ (Accessed: 03 January 2020).

TracesAI. (2020) *Technology Overview and Detail of Performance.* Available at: https://www.traces.ai/tech.html (Accessed: 07 January 2020).

Transport for London. (2020) *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: 14 January 2020).

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: 02 March 2020).

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: 04 January 2020).

UK Government. (2018) *Terrorism in Great Britain: the statistics.* Available at: https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7613 (Accessed: 09 January 2020).

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 January 2020).

Umbo Computer Vision Inc. (2020) *Product Overview and Case Studies.* Available at: https://umbocv.ai/?gclid=Cj0KCQiA9dDwBRC9ARIsABbedBPenMPqOdgDgT88EtdpY2s3JexKOr-gPKpTHBoeQtbGo6nqK0tiL-oaAlNPEALw_wcB (Accessed: 07 January 2020).

Wardynski, D. (2019) *How Technology Changed Our Lives.* Available at: https://info.brainspire.com/blog/technology-and-society-how-technology-changed-our-lives [Accessed: 01 March 2020].