**Call: SU-FCT02-2018-2019-2020 (Subtopic 3)**

**Technologies to enhance the fight against crime and terrorism**

**Project Name MODEiT:**

**Money Laundering Detection using Enhanced Information Technology**

The University of the West of England (UWE) in the UK, is leading and forming a consortium in response to the above call.  Below is a broad outline providing the background, who we are approaching in this consortium and a draft of how we are responding to the call. We are in the process of forming the Consortium and therefore seeking a quick response of interest (bid submission deadline 27thAugust 2020).

In particular we are seeking collaborative expertise in producing bolt-on track and trace money-flow technology addressing AML/CTF, Dark Web Penetration and Data Provenance. In return this 2-3 year project offers finance to develop leading specialist technology informed by experts (Tech/Law/IP/Crypto/Data Provenance/Dark Web etc) in a living lab environment (end-users Law Enforcement Agencies, bank, LEA training provider) and to inform policy-makers, regulators as well as the academic canon on future requirements.

We are in discussion with EU Law Enforcement Agencies to develop training for this technology as well as piloting the technology in training scenarios and welcome further interest from LEAs, regulators and policy-makers with experience in this area. Our understanding is that whilst advanced intelligence technology exists, it has very limited uptake and we would like to indicate this within our response to the call. We are restricted by the call’s requirements but see this as an important element. So, whilst the project’s focus is the development and testing by LEAs of the technology, we would like to extend our consortium with parties who can enrich, advance and endorse the work of this project.

Below is a link to UWE Bristol Financial Crime Network within which further the project team’s profiles can be viewed. If there is interest, we would like a short synopsis outlining how your support will contribute or advance the project.

[https://www1.uwe.ac.uk/bl/bls/research/globalcrimejusticesecurity/financialcrimenetwork.aspx](https://urldefense.proofpoint.com/v2/url?u=https-3A__www1.uwe.ac.uk_bl_bls_research_globalcrimejusticesecurity_financialcrimenetwork.aspx&d=DwQF-g&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=fexiZNZJOBZ-yA8htumJxuZhCO2W6sAMgsEOutWUyR8&m=R_WTSPkpc5GtymsBdr5uOl3maevrw7gITeFaGIN18mc&s=FjxamLnCC0pwIvSqdmQnmzJkq5COE4xXxgtu3jQDVT4&e=)

|  |
| --- |
| [Financial Crime Network - UWE Bristol: Bristol Law School](https://urldefense.proofpoint.com/v2/url?u=https-3A__eur01.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Furldefense.proofpoint.com-252Fv2-252Furl-253Fu-253Dhttps-2D3A-5F-5Fwww1.uwe.ac.uk-5Fbl-5Fbls-5Fresearch-5Fglobalcrimejusticesecurity-5Ffinancialcrimenetwork.aspx-2526d-253DDwMF-2Dg-2526c-253DeuGZstcaTDllvimEN8b7jXrwqOf-2Dv5A-5FCdpgnVfiiMM-2526r-253DfexiZNZJOBZ-2DyA8htumJxuZhCO2W6sAMgsEOutWUyR8-2526m-253DHjxAS-5Fth4JGSvV0s55O1fRW9Lm3ePjVe6irjduZhHmE-2526s-253D1Ngxow61ikPDYaTYHKs7jTPinPL1t5M901jWMythVLQ-2526e-253D-26data-3D02-257C01-257CCass.Gardiner-2540uwe.ac.uk-257Ca67121590b0541ae880208d828a11166-257C07ef1208413c4b5e9cdd64ef305754f0-257C0-257C0-257C637304019538160426-26sdata-3DUnfX8DFhbp-252FFF4S74GUsjv5Xc2sZTe-252FvE-252FLbMSZh5as-253D-26reserved-3D0&d=DwMF-g&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=fexiZNZJOBZ-yA8htumJxuZhCO2W6sAMgsEOutWUyR8&m=R_WTSPkpc5GtymsBdr5uOl3maevrw7gITeFaGIN18mc&s=8uRgk-wFikHHIyoozfvMf6JcPp8KahH0U7sC8E5avqg&e=)The Financial Crime and Cyber Crime Research Network comprises members of the Global Crime, Justice and Security Research Group, the Computer Science Research Centre at UWE Bristol, and external scholars.. View the profiles of the Network members who lead research into financial and cyber crime.[www1.uwe.ac.uk](https://urldefense.proofpoint.com/v2/url?u=http-3A__www1.uwe.ac.uk&d=DwQF-g&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=fexiZNZJOBZ-yA8htumJxuZhCO2W6sAMgsEOutWUyR8&m=R_WTSPkpc5GtymsBdr5uOl3maevrw7gITeFaGIN18mc&s=QmjS4hDjEMYH5kA73ay8KmaiKLgp0mvcQVO2yddDfRQ&e=) |

Context

Securing the society against disasters is one of the central elements of the functioning of any society. There is barely any societal sector which is not to some extent concerned by disasters and related resilience and security issues.

This Challenge should bring together all security stakeholders: industry - including SMEs, research organisations, universities, as well as public authorities, non-governmental organisations and public and private organisations in the security domain. The active involvement of end-users is of high importance.

The Secure Societies Challenge will contribute to the implementation of the policy goals of the Europe 2020 strategy, the [Security Industrial Policy](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF), the [Internal Security Strategy](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF) and the [Cyber Security Strategy](http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf).

Project Background

Earlier this year UWE Bristol was awarded UK Innovate funding to actively research AML and CTF working with a private sector SME Synalogik Ltd. A summary of the research in action project follows,

The aim of this project is to develop a bespoke Counter-Terrorism Financing (CTF) and Anti-Money Laundering (AML) risk assessment engine which will process multiple meta-data feeds outputting 'live' reports utilising algorithms tailored to an organisations requirements to establish trends and patterns identifying threats to the security of the UK and Europe. The specific aims of the project are:

1. To develop an advanced and unique complex digital platform and CTF/AML operating system with commercial value for the Ministry of Defence (MoD), the Financial Conduct Authority (FCA), the National Crime Agency (NCA), HM Revenue and Customs (HMRC), the UK Security Services (Mi5/Mi6), the regulated sector (financial services sector, financial advisors, legal profession etc), EUROPOL and the Egmont Group of Financial Intelligence Units,

2. To develop risk assessment algorithms specific to Counter-Terrorism Financing and Money Laundering,
3. To perform testing of the prototype operating platform and the algorithms on potential current criminal threats as detected by Somerset & Avon Police, assessing performance and evidencing capability as well as refining functions and 4. To deliver a specialised advanced CTF/AML product and to develop a clear commercialisation pathway.

This business opportunity exists as there is continued pressure on UK Defence organisations to identify and respond to terrorist threats in real time. Key problems facing criminal detection organisations are money laundering and terrorism financing and limited risk assessment systems. Typically, a police officer will spend a minimum of three days tracking criminal activity before being able to respond to a risk.

Synalogik and the University of the West of England propose to address this opportunity by exploiting new digital technology to produce risk assessment outputs in real time; Synalogik's core Platform SCOUT utilises a combination of workflow automation and dynamic risk assessment algorithms to automate the gathering, cleansing and assessment of diverse data, identifying trends and patterns of relevance. The Platform then produces a casefile/report for investigators to act upon. This is already a market-leading approach and has been demonstrated to deliver notable benefits, including the automated processing of 1,400 insurance-based searches in under 6 minutes; opposed to requiring seven people for a month.
If successful this project will deliver a new, simple process for: (1) assessing and collating evidence of terrorist threats in real time (2) determining the level of threat and (3) evidencing an appropriate response. Synalogik's longer term goal is to provide a commercial system for pan-European criminal detection agencies to establish when a threat must be acted on. Synalogik will develop CTF algorithms tailored to the requirements of an organisation, which will be especially attractive to law enforcement agencies, private-public financial crime prevention measures (such as the Joint Money Laundering Intelligence Task Force), HM Government departments and the United Kingdom Security Services because it will permit rapid, simple, coordinated responses to incoming and immediate criminal threats, reducing the risk to lives and reducing insurance costs via damage limitation.
The Risk Assessment Engine SCOUT will be validated to meet legislative requirements. This project addresses three areas of innovation:
(1) innovation associated with the development of a completely new approach to managing Terrorist Threats and Criminal Activity, particularly money laundering;
(2) innovation associated with the design of CTF Algorithms and a Risk Assessment Engine identifying patterns or trends of money laundering and terrorist activity;
(3) innovation associated with Machine Learning and Augmented Intelligence processing multiple feeds of internal and external meta-data in real time.
In this 24 month project, utilising previously obtained research data, the CTF principles will be validated and the prototype engine will be functionalised in accordance with the CTF principles. In parallel with this work novel algorithms will be developed and the associated software created. In the final phases Avon and Somerset Constabulary will be invited to run the proto-type CTF/AML system.

Next Steps

Following on from this success UWE Bristol is coordinating a response to the H2020 Securities Call SU-FCT02-2018-2019-2020.

UWE Bristol will lead a European consortium of collaborators,

Consortium

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Research/University  | Developer/Producer  | End-User/Customer/LL1  | Trainer  | Other |
| UWE UK  | Synalogik UK SME  | Somerset & Avon Constabulary UK LEA  | CEPOL ITALY LEA  | NATO (InterGov Military Alliance) BRUSSELS  |
| Uof CYPRUS  | Nodes & Lines GREECE SME  | Met Police UK LEA  |   | University College Dublin, National University of Ireland Dublin (INSPECTr) |
| Uof GREECE  |   | Dutch Politia LEA  |   |   |
|   |   | Bankia SPAIN Corporate  |   |   |
|   |   |   |   |   |

Fighting crime and terrorism requires new technologies and capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism), including understanding and tackling terrorist ideas and beliefs to also avoid aviation-related threats.

The protection of the European borders requires the development of systems, equipment, tools, processes, and methods for rapid identification. This includes supply chain security in the context of the EU’s customs policy.

On Digital Security, this Challenge focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets & market incentives in Europe, following an end-user driven approach, including for instance law enforcement agencies, first responders, operators of critical infrastructures, ICT service providers, ICT manufacturers, market operators and citizens.

Building on the current CTF/AML project this consortium will expand research into action by developing a series of tools and outcomes;

1. Tracing money flows – traditional money flows are regulated by protocols such as KYC providing providence on the money source. However, AML/CTF are able to circum-navigate current protective mechanisms. Further to this digital currency which is likely to become an accepted currency is exploited by criminal networks. Research will establish significant AML/CTF money flows as well as smaller flows either leaked into the system or the starting point of an illicit money flows such as online gambling, online trades, fraudulent insurance claims. Research will also seek to establish other forms of currency used in criminal activity and establish key points where conversion into a financial resource takes place. The findings of this research will then be converted into IT datasets, a series of decision-making algorithms, an AML/CTF web-data crawler tool, a data providence tool and a network mapping tool tracing money flows identifying suspect transactions within verified transaction. This research will develop and trial with end-users in both the public and private sectors. Outcomes will include a set of web-based IT money-tracing tools identifying money laundering and terrorist financing transactions including entry and exit points, transaction hubs, AML/CTF finance map. Data providence, information weighting and standard deviation assurance filters referring evidence to category alerts will be developed for real-time use and digital forensics.
2. Tracking criminal activities online and establish active protocols protecting personal data – a two-fold approach researching and establishing legislative mathematical decisions trees will categorise criminal activity under legal jurisdiction and category including EU and sub-categories such as national law indicating the legal area of online criminal activity. The second approach will establish a track and trace online criminal activity IT system using data-feeds from multiple-agency databases. The protocol outcomes to be established are likely to result in a series of outcomes including a specialised EU Law Enforcement Agency managing and responding to the Track & Trace IT System, as wells as policy & legislative change to realise new digital protocols for this system and its impact on the Justice System. Protocols protecting personal data developed in line with privacy, ethical and personal liberty guidelines and legislation will be supported by recommendations for policy and legislation changes signalling and identifying at which point and under which legislation personal data can be accessed and used for criminal investigation leading to prosecution.
3. Darknet marketplace analysis and mobility – it is known that the Darknet generally operates off-grid within the confines of the Onion routing, TOR. Research into its early operational purpose, how it functions and if value chains of mobility are possible will be conducted. Darknet marketplace analysis identifying how, where and when markets are formed, the type of activity and trade, whether they are pop-ups or ongoing, how marketplace communication acts and reacts, as well as the value of trades, identifying traders (country, operational unit, market makers, types of trade). Outcomes a current and future understanding of the Darknet marketplace and mobility with a framework of the opaque layers where activity is lost and likelihood of whether the market will or has re-emerged elsewhere. This framework can be further built upon and potentially connected with the Track & Trace IT system under-development in section 2 above.
4. Tools for locating and mapping hidden service directories – Arising out of and in combination with the above points location and mapping tools detecting hidden service directories will be built and tested. The toolkit will contain web-crawlers and scrapers built to locate hidden service directories available on the Internet and as permissible in the TOR. The toolkit will include Timestamps to track mobility over time. The toolkit will be extendable allowing for bolt-on and additional criteria add-ins extending search capacity futureproofing the toolkit.
5. Tools for forensic analysis of digital media in order to identify digital currency datasets – researching potentially limited digital currency datasets requires ongoing development of tools for forensic analysis of digital media. Therefore, this work will be exploratory. Through the division of digital media unique tools will be developed to identify datasets that are digital currencies. This will require an initial identification of a digital currency or form of digital transaction that is accepted or recognised as a type of currency (money, crypto, trade product, service or other) and a currency topography for instance the value of things ie a child, drugs, arms etc. Outcome a preparatory toolkit with extensions as more datasets become available.
6. Data provenance models (providing evidence that is admissible in court), including the relationship between algorithmic proof artefacts and legal evidence – research and trials of data provenance models detailing the level of authenticity acceptable within a court of law. A combination of research between legal requirements and new sources of data, particularly digital data and algorithms (based on mathematical modelling programmes) will be tested and developed. Acceptability scales on digital authenticity including source ie public domain vs Darkweb, probability modelling (maths) and accuracy SD models applied to a process of deduction against what is acceptable within the legislative domain.
7. Approaches to identify new developments (new markets and networks; new modi operandi) – arising out of the above research, trials and operational models such as toolkits and protocols, approaches to identify new developments and modes of operation will be deduced. These approaches will be built into end-user practice, monitored and documented. Collaboratively the results will be shared, discussed and analysed. The resulting emerging set of practical and theoretical approach outcomes will be re-shared, put into practice with results over set-time periods analysed. This process will be repeated during the project capturing live and changing data to establish the most effective approaches capable of identifying new and changing operations, markets, networks etc. It is anticipated the outcome will have captured enough accountable detail to be applicable in practice as well flexibility to capture motion, mobility and new developments.

Research

Desk research will develop into practical application which will form research in action, the results of which will inform further developments of practical application. The consortium of policymakers, law enforcement agencies, private businesses and academic institutions will collaboratively source, research and bring into practice a series of toolkits and outcomes in response to this call. Until legislation and policy is realised supporting the outcomes of this work, this project is identified as a trial for future public and private sector purpose. The security level of this work and disclosure levels will be agreed and accepted by participating parties at the outset upon the project receiving funding.

Further Inclusion

The following details of the call will be absorbed and practiced in the above work. Details will be identified in the work packages; each consortium member will be expected to indicate how it will realise the following impacts within their work outcome and or through the overall work conducted in response to this call.

In all sub-topics and in order to facilitate the EU-wide take-up of new technologies, proposers are encouraged to include the design of innovative curricula for LEAs training and (joint) exercises, and of information packages for the wider public and civil society organisations.

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation including in the area of privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

• novel, user-friendly technologies, tools and/or systems, addressing traditional or emerging forms of crime and terrorism at acceptable costs;

• improved investigation capabilities, especially regarding quality and speed;

• increased efficiency and effectiveness of the information sharing among EU LEAs.

Long term:

• prevention/reduction of criminal and terrorist threats;

• harmonisation of information formats at international level, improved cross-border acceptance and exchange of court-proof evidence, standardised evidence collection and harmonised procedures in the investigation of trans-border crimes in full compliance with applicable legislation on protection of personal data.