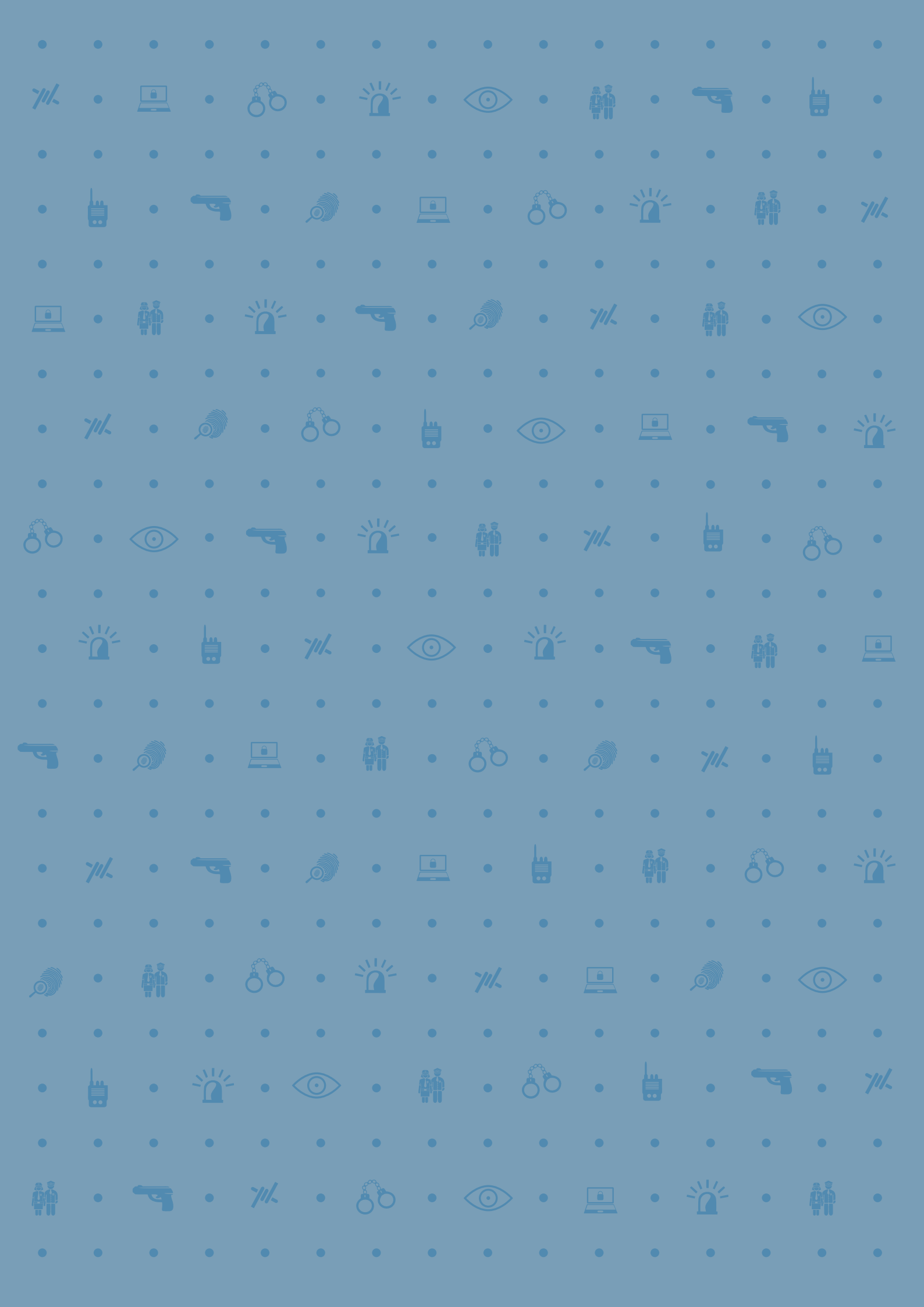
CENTRIC

Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

Counter-Terrorism Edition

April 2019



“Terrorism is not new.
But, amplified and accelerated by the reach and tempo of technological change, it is now more global, more multi-dimensional and of a different order of pace and intensity”

MI5 Director General Andrew Parker

Source
https://www.mi5.gov.uk/news/director-general-andrew-parker-speech-to-bfv-symposium

FOREWORD

Roger Eccleston
Pro Vice Chancellor for Research and Global Engagement

I am delighted to have this opportunity to provide a foreword to this report on CENTRIC's research activities. Our mission, at Sheffield Hallam University, is to transform lives through education and research. We expect the outcomes of our research to result in benefits to individuals and communities in the UK and across the globe. We focus our research in three platform areas: Thriving Inclusive Communities; Healthy, Independent Lives, and Future Economies.

Within these pages you will find examples of CENTRIC research that epitomise our mission and address all of our platform areas, but predominantly contribute to the safety of individuals, communities and society in the UK and across the globe.

The challenges CENTRIC researchers address are complex, requiring an approach that works across academic disciplines, across the security landscape and in collaboration with a wide range of partners locally, nationally and internationally. The CENTRIC approach to partnership and collaboration links practitioners, private industry, academia and the public to create a unique capability for applied research in the security domain.

CENTRIC research on security challenges is broad and comprehensive – ranging from the 'soft' security issues such as community policing and migrant integration that build societal resilience against crime, to the 'hard' security issues of counter-terrorism, organised crime, human trafficking and child sexual exploitation, issues that undermine society.

The work featured in this report provides excellent examples of the quality of research conducted by CENTRIC and demonstrates how CENTRICs unique capabilities and partnerships make a real impact on making people's lives safer.

4

PRELUDE

John Parkinson OBE
Chair of the CENTRIC Advisory Board

> "CENTRIC's innovative approach to applied research provides them with a clear opportunity to address the security challenges of today and tomorrow"

It is with great pleasure that we present to you 'Focus on Counter-Terrorism' from the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC). The publication of this review is timely given that it is set against a background of conflict, insecurity and the resurgence of violence both at home and abroad. For the United Kingdom, like many other nations, we remain under constant attack from all manner of hazards including terrorism as well as organised crime and cyber-related threats that, if left unchecked, can cause untold harm to citizens, communities, public services, businesses and the wider economy.

In recognition of these challenges, CENTRIC takes an innovative approach to research that brings together practitioners, private industry, academia and the public to focus on applied research in the security domain. This multidisciplinary approach seeks to inform operational policy and practice alongside the development of tangible solutions that can be employed by practitioners on a day-to-day basis. In doing so, CENTRIC strives to make positive contributions towards citizen safety in all corners of the world and push professional practice beyond the current state-of-the-art.

CENTRIC has quickly established itself as a dynamic, progressive and innovative centre of excellence, priding itself on making a difference through its unique collaborative approach. May we take this opportunity to thank all of the CENTRIC team for their energy and enthusiasm, and wish them continued success in the future. We are delighted that CENTRIC continues to develop its capacity and capability, ensuring that all in authority are better informed today to meet the security challenges of tomorrow.

ABOUT CENTRIC

The Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) is a multidisciplinary, security focused research centre at Sheffield Hallam University. CENTRIC collaborates with a number of academic, law enforcement, government and industry partners from across the globe to provide solutions to some of the most pressing contemporary security challenges. By delivering ground-breaking research, advanced technological capabilities, professional expertise and training to law enforcement and other security stakeholders, CENTRIC is in a unique position to offer innovative solutions informed by the operational reality of modern day law enforcement.

To find out more about the activities taking place within CENTRIC visit: research.shu.ac.uk/centric or follow us on Twitter @CENTRICResearch.

7

RESEARCH TO REALITY

Professor Babak Akhgar
Director of CENTRIC

> "CENTRIC is at the forefront of providing solutions to tackle some of Europe's most pressing contemporary security challenges"

The ability of law enforcement agencies to keep citizens safe and secure around the world has never been more keenly tested. Police, governments, and other security services now require innovative, and often technological, solutions to help them face the security challenges of the future. The unique multidisciplinary approach of CENTRIC has shown that we are well placed to work with such organisations to help them embrace and overcome these challenges.

Since its inception, CENTRIC's research and development portfolio has increased rapidly owing to many successfully completed projects and innovative collaborations. We now have our own dedicated facility to provide direct support for the activities of the Open Source Intelligence Hub, training areas, virtual reality experiences and space for security practitioners to undertake secondments within CENTRIC. This space now houses a growing team of over 40 dedicated, security-focused staff delivering expertise across all of our key domain areas and core capabilities.

Our objective has always been to bridge the gap between the operational reality of policing and security and the original research and expertise brought by academia. Through CENTRIC, practitioners, policy makers, software developers, and researchers have been given a clear platform for collaboration to support exceptional applied research in the security domain. As we have grown these collaborations have continued to flourish, providing the solid foundations that CENTRIC is built on today.

The success of CENTRIC can be attributed to the hard work and dedication of its team, external collaborators and advisors, and the efforts of the board itself. It is upon these relationships that a successful foundation and a future for CENTRIC is built and, while the achievements to date have been nothing less than exceptional, I am even more excited about what the future holds.

DOMAIN AREAS

CENTRIC boasts an expert team with a passion for research and innovation that aim to address a broad range of contemporary security issues. Our research often traverses several specialisations, bringing together multidisciplinary expertise from a wide range of domains.

- **Counter terrorism and radicalisation**
- **Child sexual exploitation**
- **Community policing**
- **Crisis management and disaster resilience**
- **Cybercrime and cyberterrorism**
- **Humanitarian actions and migration**
- **Intelligence management**
- **Open source intelligence investigation**
- **Serious and organised crime**

CORE CAPABILITIES

CENTRIC strives to deliver cutting-edge breakthroughs in research and technological development to ensure that those entrusted with safeguarding our society are best equipped to prepare for, respond to and recover from the threats faced on a daily basis.

CENTRIC's research team holds specialist skills in range of fields.

- **Data mining, analytics and visualisation**
- **Data protection and ethics**
- **Knowledge management**
- **Mobile application development**
- **Practitioner-driven, evidence-based applied research**
- **Serious games development and training**
- **Situational awareness systems**
- **Social media, digital communication and technology**
- **User requirements, interface design and prototyping**
- **Virtual and augmented reality**

Situational Awareness

Systems and applications that support situational awareness have and continue to be a key element of CENTRIC's research and development portfolio. Good situational awareness can apply to an individual, team or organisation and means being able to understand the current situation, interpret what that situation means in the context of the environment and then using this information to predict what may happen in the near future. The application of situational awareness to the security domain has a clear rationale and directly supports the majority of command and control operations in a range of scenarios.

Staff safety and security

All organisations have a duty of care to their staff in terms of maintaining their safety and security even when operating in challenges circumstances. From humanitarian to military, and from blue light services to international corporate companies staff can be put at risk because of the locations they work, the environments they operate in and the sensitive nature of the decisions they make. Management within these organisations have a obligation to maintain good situational awareness of their people, their reasons for travel and the ongoing and future events. Modern commodity technologies such as smartphones, watches, trackers and beacons supporting GPS and simple notifications and alerting can be invaluable in situations of peril. Connecting them to map-based dashboards in pre-existing 24/7 command and control centres can take an organisation's staff safety and security provisions to the next level. For more information of our staff safety and security solutions read up on our SCAAN project.

Major incident management

When a major crisis happens anyone can be on the scene: victims, bystanders, law enforcement, civil contingencies, and even the military. From the moment they arrive through smart phones, IoT devices and social media they become a transmitter of potentially vital information that can shape and influence first responders' decisions and actions. Collating this information and using it to provide situational awareness to operational, tactical and strategic command structures can save lives and resolve incidents faster. Provision of this information through smartphones, informational dashboards and in the field through heads-up displays has the potential to revolutionise major incident responses. Through Athena and now our CONNEXIONs projects we are exploring how next-generation information technology can support responders in the most challenging of situations.

Horizon Scanning and Threat Assessment

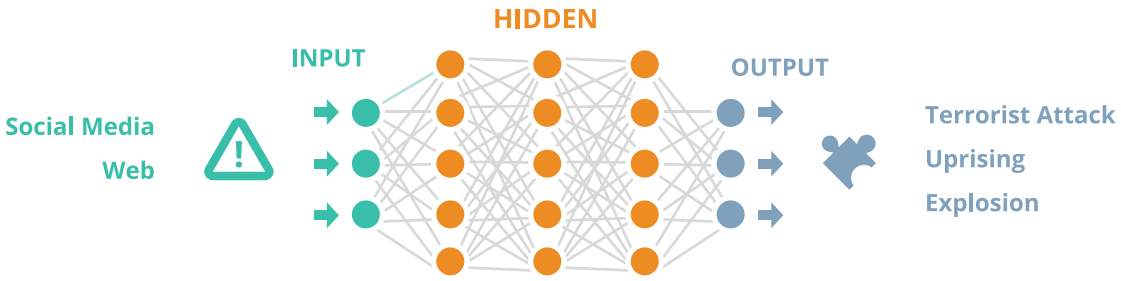
Detecting instances of organised crime, terrorist threats and other serious crimes in advance of the time they happen requires a proactive policing approach as opposed to a reactive one where intervention is likely to happen too late. Situational awareness can apply beyond live incidents to the proactive tracking and monitoring of on and offline threats. Having an accurate understanding of the intelligence picture and a clear insight potential implications of specific connections, interactions and pronouncements allows law enforcement to remain one step ahead of criminals. TENSOR, CONNEXIONs and ePOOLICE all investigate methods of providing law enforcement with a better understanding of their intelligence giving them the agency to make the right decisions at the right time.

Artificial Intelligence

Artificial intelligence, deep learning, machine learning are are finding real and beneficial application across all major sectors, security has already proved a fertile ground for the application of such techniques. However, they initial hype and relative black-box nature of current implementations has caused concern to both privacy and equality advocates. CENTRIC takes a pragmatic approach to the use of artificial intelligence and machine learning focusing on applications that can support human decision making.

Incident detection and alerting

Systems that monitor incoming intelligence from the web, social media and also intelligence and reporting systems can use this information to alert users to spikes in specific incidents through techniques such as burst detection as well as providing added value to incident classification. In our staff safety and security system SCAAN, localised incident detection and classification using media from national, regional and hyper-local channels can be used to quickly alert staff to serious threat-to-life incident nearby before such news has reached the command and control centre. In intelligence investigations it can be combined with domain ontologies to inform investigators when key pieces of intelligence are added to their case based on prior designations of specific interest points.



Decision Making

Simple machine learning decision making models can improve efficiency and the consistency of decision making when dealing with datasets that contain analytical data. Models can support human investigators and analysts in interpreting their data in consistent and predictable ways. In our project that works with a forensic science team analysing samples for the presence of drugs and alcohol, we use machine learning models to interpret analytical data from metabolites with environment data to determine the presence and extent of drug or alcohol abuse more accurately and consistently. These techniques are exploring the use of explainable AI to support the use of such models in court.

Activity detection

Suspicious behaviour and activity often coincides with unnatural behavioural patterns different to those around them. Experienced law enforcement officers have often developed this ability through years of practice. By applying advanced object detection and tracking techniques, we apply machine learning algorithms to help identify suspicious behaviour at border crossings in the ROBORDER project. This detection is not only limited to humans but also to vehicles and water vessels as well.

Crowd Behaviour and simulation

One of the long term applications of artificial and machine intelligence has been for the modelling of crowd simulation in various scenarios. Effective crowd simulation relies on understanding the goals and motivation of individuals. Individuals usually follow the flow of movement until this prevents them from achieving their goal. If an individual is more motivated to reach their goal, e.g., panic, then they may attempt to navigate more directly through the crowd flow. In less dense crowds, individuals will navigate more directly to their intended destination, taking into account the need to avoid hazards and obstacles. These goals can quickly change, for example in response to a terrorist attack or a public order incident. Each individual is controlled by AI algorithms that determine whether their goal is being achieved and decide what they should do once they achieve their goal.

FOCUS ON COUNTER TERRORISM

Understanding, combatting and countering terrorism has been a core theme in the development and focus of CENTRIC over several years. During this period we have seen the rise of the Islamic State culminating in several terrorist attacks across Europe, whilst the growing threat of far-right extremism has been brought to the fore recently with the attacks in Christchurch, New Zealand and Pittsburgh, United States. CENTRIC seeks to address the area of terrorism from several angles - from the sociological to technological - and across a range of ideologies - including domestic extremism, far-right and Islamic.

STRATEGIC PROJECTS

Within CENTRIC, we are delivering several strategic projects each focusing on different aspects of counter-terrorism. Our flagship TENSOR project is motivated by the goal of providing technological tools that directly support investigators and analysts working in law enforcement agencies to track and prevent the spread of terrorist and extremist content online. The CENTRIC OSINT Hub has been instrumental in bringing software developed throughout our research projects into operational investigations including but not limited to terrorism. AUGGMED sought to train firearms officers reacting to a terrorist threat while SCAAN supports and enhances the safety of humanitarian staff worldwide, especially those stationed in conflict zones. MINDb4ACT and PROPHETS both seek to understand factors that influence radicalisation building on TRANSRAD, which specifically aimed at achieving a better understanding of approaches to tackle violent and political extremism. Our forthcoming Master's course on International Security Management will take many of these lessons learned and use them to educate the next generation of law enforcement leaders across Europe on the current and emerging threats in terrorism and the wider security landscape.

This project has received funding European Commission Horizon 2020 research and innovation programme under Grant Agreement No 700024.

September 2016 - August 2019

TENSOR

Retrieval and analysis of heterogeneous online content for terrorist activity recognition

www.tensor-project.eu

> **The spread of terrorism-related material fuels radicalisation and violent extremism. The rapid identification and analysis of such content will enable LEAs to respond and counter these threats more effectively.**

LEAs across Europe face diverse challenges in how they identify, gather, interpret and react to extremist and terrorist content online. They must limit its spread and detect who is creating, accessing and being influenced by such content. In addition to traditional sources, such as forums and social media, the dark web presents additional challenges due to its ephemeral nature and alternative mode of access.

Given that undetected terrorism-related material can contribute to violent extremism and radicalisation, LEAs must also try to remove such content from the web. To facilitate these tasks, automated tools which tackle the challenge of extraction and analysis of meaningful and relevant content hidden in huge amounts of online data must be developed in order to assist LEAs in their investigations and reduce the strain on their resources.

TENSOR provides a powerful intelligence web-based system to assist LEAs in the challenges that they face identifying, gathering and interpreting online-based terrorist generated content by delivering fast and reliable analytical support for the early detection of terrorist activities and content.

The TENSOR application discovers content from the web and social media through focused and directed searching, crawling, scanning and gathering of specific information. This content is enriched through text and multimedia extraction, filtering and classification. The results are presented through analytical and visual interfaces aligned to the workflow of analysts supported by robust, automated auditing. Ultimately, the TENSOR platform will bring significant advantages to LEAs' operational capabilities in identifying terrorist generated content and activities.

CENTRIC is the technical coordinator of TENSOR and has responsibility for the overall development and creation of the TENSOR system including the creation of an intuitive intelligence dashboard interface. Our expertise is utilised in the modelling of the terrorism domain realised through the creation of terrorism taxonomy and ontology. We are applying our knowledge of web crawling and scraping to content from the surface and dark web as well as social media platforms and ensuring that such sensitive data is stored and accessed both efficiently and securely. Our experience of data mining is used to cluster and group elements within the data to highlight key patterns and insights that can be utilised by law enforcement investigating terrorism offences.

The prototype system developed within the project is already being trialled by several law enforcement agencies to support their online investigations into terrorist generated content and activities.

CENTRIC OSINT Hub

OPEN SOURCE INTELLIGENCE HUB

Open source intelligence (OSINT) can be a vital tool in the box for law enforcement. The evidence obtained from information available online can make a crucial difference to an investigation's outcome

The internet brings forward unprecedented challenges and opportunities for modern policing, combatting serious and organised crime, and countering terrorism. The CENTRIC OSINT Hub is a joint venture between academia, next-generation research and law enforcement that assists local, regional and national agencies with open-source investigative support predominantly focused on the trio of internet, intelligence and investigation.

The OSINT Hub, housed in a dedicated facility within CENTRIC, leads the way in developing OSINT investigations through the development of capture tools, automated technologies and analytical processes. CENTRIC maintains a commitment to delivering exceptional intelligence quality, bespoke technological innovations and an adept understanding of the continually evolving UK and EU legal directives, regulations, and best practices for the application of OSINT. Our unique positioning within academia enables the OSINT Hub to provide world-class services, tailor-made to specific operational needs of law enforcement across the globe.

EXPERTISE

The CENTRIC OSINT team consist of a group of security-vetted former law enforcement officers, academic and industry researchers, and qualified investigators with a diverse background of knowledge and experience in criminal investigations, radicalisation, terrorism, serious and organised crime, and cybercrime. The foundations for the Hub have been built alongside support from Home Office CAST (Centre for Applied Science and Technology) and a number of police forces from across the UK. The Hub has already provided operational support to forces investigating a range of serious crimes including domestic extremism, hate crime, child sexual exploitation and sexual assault.

SERVICES

Targeted Investigations - We undertake bespoke and targeted investigations carried out by the accredited in-house OSINT specialists who bring leading best practice approaches in areas such as data capture, auditing, and protecting lines of evidence. These investigations also support the discovery and validation of new approaches and the development and deployment of training to domain practitioners.

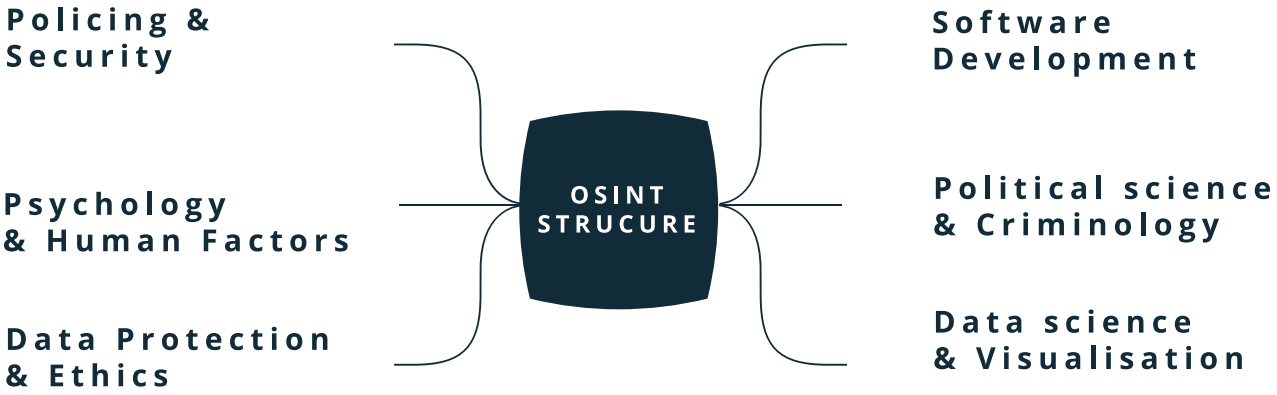
Situational Awareness - We can support the proactive monitoring of potential threats maximising the potential of open source data such as that from social media, surface and dark web. These investigations utilise the modelling, capture and analysis of crime indicators and can be conducted at a regional, national and international level.

OSINT Training - We are currently developing an OSINT training course for individuals working as part of, or, alongside law enforcement. Please get in touch for further information and to discuss your organisation's specific requirements.

The next pages preview our OSINT approach, capabilities and offerings in more detail.

OSINT Approach

We aim to develop a community of practice for OSINT between our delivery team and wider partners. The goal of this unique collaboration is to establish a breakthrough interdisciplinary hub of excellence focused on the modern triad of internet, intelligence and investigation. While we place a specific focus on the implementation our ideas into analytical software tools, our open-source approach as a whole spans a range of domains each supporting and feeding into a comprehensive OSINT offering that applies across the OSINT Hub as well as aligning with our projects and future roadmap. Our OSINT approach focuses on overt and covert internet research but does not stray into undercover investigations.

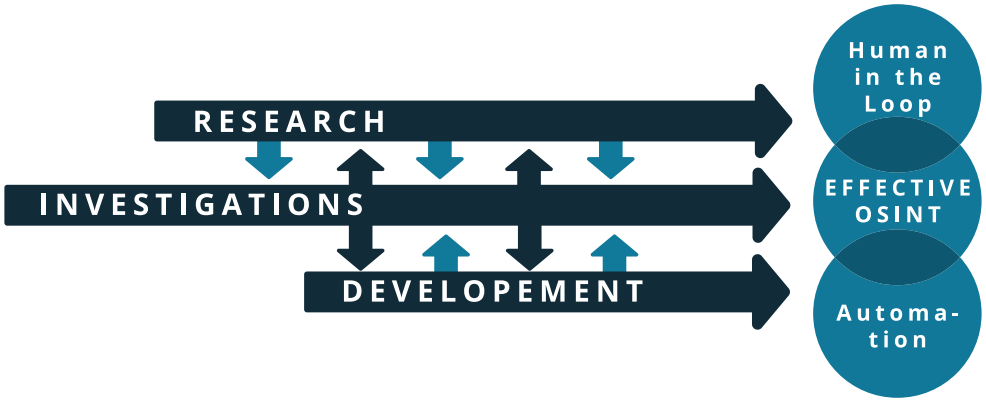


Delivering Value

We take a three pronged approach to delivering effective open-source solutions to law enforcement and other organisations. Our research is oriented directly to funded projects such as TENSOR and CONNEXIONs and manifests itself in practical publications such as the Open Source Intelligence book and the forthcoming publications on Dark Web Investigation and Big Data Analytics for Safety and Security. The research conducted within CENTRIC also lays the foundation for operationally-motivated software development that puts a greater emphasis on delivering tools directly aligned with the immediate requirements of law enforcement.

Lessons learned from research activities and large-scale evaluations and exercises provide a solid basis for the transformation of research software into commercially-viable solutions ready to be trialled in operational environments and utilised to deliver intelligence. The final transformative aspect of our approach to open-source investigation is to work directly with law enforcement officers and analysts on real, live investigations to orient our tools and workflows with those who need them most.

CENTRIC open-source intelligence tools are designed to support the investigator by automating common tasks that take time and require manual data collections. This means moving them towards automated process that maintain the investigator first approach.



Effective OSINT is not about giving control over to a machine, we see the investigator as the cornerstone of any open source investigation. Any tools and technologies should help the investigator understand their data faster, more deeply, connect the dots more easily and ultimately give them the information that allows them to find the intelligence they need. The analyst should drive the investigation, with the machine following the investigator rather vice versa. Despite the vast powers of modern day computing, many cannot deliver the innate pattern matching and reasoning natural to experts, which is why the tools CENTRIC develops put the investigator first and keep the human firmly in the loop.

Key Technologies for OSINT

Open source information does not exist in a vacuum. It is most powerful when it is fused with other investigative information. CENTRIC tools and techniques are developed with the vision of enabling easy integration from law enforcement intelligence systems through a range of different connections. The team can support alignment of intelligence system exports with that of CENTRIC technologies, the support of common data exchange formats, such as exports/imports from iBase as well as direct integration through customised APIs. Use of our tools follow a common analysis workflow that synchronises with the intelligence cycle.

Social Media Extractor

CENTRIC has developed a bespoke solution for extracting information from social media whilst minimising the investigator's footprint and the need to acquire API keys whilst maintaining the human-in-the-loop. The approach supports proportionality by preventing investigators from consuming and collecting excessive amounts of collateral information, distant from the subject under investigation. The solution ensures investigators remain focused on their current task whilst providing a natural paradigm that follows existing manual open-source investigative flows, maintains the 'one-look' convention preferred by many law enforcement agencies to separate open-source investigation from surveillance, and supports concurrent data collection to enable post-hoc analysis. The extractor currently supports data and image extraction from Twitter, Facebook, Reddit, Instagram, VK and Telegram channels.

Graph Modelling and Analysis

'Everything is connected'. Graph based models are a perfect for online investigations as the data acquired combines the POLE (people, objects, locations, events) model with the natural relationships between these entities. Graph models combined with intuitive visualisations also enable investigators to see connections they were not aware of previously and begin to make links. Aggregations of the model are used to cluster similar nodes while graph distances from defined central nodes can be used to determine relevancy and focus investigative search.

OSINT Intelligence Toolkit

Our OSINT intelligence platform brings together our social media extractor with web crawling and social media monitoring technology to deliver an analytical intelligence toolkit. Beyond the import of data from the web and social media, the toolkit delivers entity and media extraction, secure data storage, graph data modelling, and visualisation. The toolkit provides a solution for law enforcement's governance of open-source data through functionalities that support intelligence management, organisation, exploration and presentation.

This project has received funding from the European Commission Horizon 2020 research and innovation programme under grant agreement No 653590.

AUGMED

June 2015 - May 2018

AUGGMED

Automated serious game scenario generator for mixed reality training

www.auggmed-project.eu/

Police and emergency services need to be at their best when the worst happens. AUGGMED emmerses first responders into a virtual and augmented reality environment to enhance their ability to respond effectively to crises.

Fortunately, major incidents such as terrorist attacks and explosions are relatively rare. Nevertheless, LEAs, first responders and other emergency services must ensure their response to such incidents is near impeccable to minimise the impacts of such events when they unexpectedly occur. The opportunities to train for these responses are usually limited to paper-based and table-top exercises with occasional live-play simulations. Live exercises are often costly to organise and offer few chances to analyse, review and repeat the scenario to implement the lessons learned.

AUGGMED is an immersive serious game platform that enables individual and collaborative training of law enforcement and first responders to react effectively in major incidents.

This training takes place using mixed virtual and augmented reality environments coupled with multi-modal interfaces and cutting edge haptic feedback and control systems. The platform generates non-linear scenarios tailored to suit the needs of individual trainees. Its learning outcomes improve emotion management, analytical thinking, problem solving and decision making skills. The environments utilise large-scale artificial intelligence to formulate realistic crowd behaviour, enabling them to react authentically to fire, explosions, exit choke points, and smoke inhalation. The simulation features three environmental scenarios: an airport, train station and marine port, each requiring different responses. It delivers a fully immersive, adaptable and realistic training experience that can be tailored to the needs of specialised trainees responding to a variety of terrorist and organised crime threats.

Our role in AUGGMED was to develop the trainer tools and interfaces. These enable trainers to configure scenarios to their specific training needs, observe multiple trainees live within a simulation and, if required, 'step in' to change parameters within the simulation; as well as being instrumental in the development of the demonstration and evaluation metrics that proved the benefits of the technology.

The serious games team within CENTRIC are currently building on the results of AUGGMED by working with local law enforcement agencies to develop a solution to train officers in the management of public order incidents.

If you or your organisation would interesting in supporting the development of virtual and augmented reality applications for security then please get in touch with our serious games team using centric@shu.ac.uk

International Organization for Migration (IOM)

Over the past two years, CENTRIC has been collaborating with IOM (International Organisation for Migration - the UN Migration Agency) on a number of technology innovations which support IOM's vision to ensure the orderly and humane management of migration for the benefit of all.

SCAAN

Security communications and analysis network

SCAAN connects field staff operating in conflict and crisis zones directly to security units to provide high-level situational awareness of risks and threats.

As a large organisation with staff distributed across the world, often in zones of conflict or humanitarian crisis, the ability of IOM to monitor and ensure their staff's safety is of utmost importance. By collaborating with IOM's staff security centre, CENTRIC has developed a digital platform and mobile application designed to provide more efficient communications and assistance to field staff. SCAAN enables users to send information directly to the staff security team, receive real-time news relevant to their current mission and alert their security team if they are in serious danger.

SCAAN provides a mobile reporting application for both iOS and Android devices in order to connect field staff with their security focal points and their overarching staff security unit via the SCAAN Dashboard. SCAAN enables high-level situational awareness and management of staff involved in or within close proximity to major incidents and events through the following key features:

01. Geolocation
02. Panic button
03. Rapid reports and communication
04. Status requests and headcounts
05. Incident alerts and broadcasting
06. 24/7 live monitoring

Taken together, the SCAAN Dashboard and SCAAN App provide an online digital situation room for agency headquarters and relevant offices with real time visualisation of security incidents across the globe. One of the key components to the SCAAN project is the exploitation of commodity and ubiquitous technology in order to deliver fast and agile results to the industry.

SCAAN is a bespoke software development project which is being adapted directly to the evolving needs of the organisation. New features on the roadmap for implementation in 2019 include the warden system for performing regional headcounts, SMS fallback to support operations in areas where data signal may be limited, vehicle tracking and satellite integration, and live incident detection. To better support organisational requirements analytical security bulletins are currently under development that will support managment in reviewing SCAAN usage over the past month helping to align SCAAN protocols with standard security operating procedures.

Within IOM, SCAAN is currently deployed to over five thousand active staff all across the globe. Since its development, SCAAN has been deployed by the World Health Organisation to support its staff in the Democratic Republic of Congo managing the Ebola crisis whilst operating in a delicate security situation and the whilst the team have also recently won a tender to deliver the SCAAN system to a large, intergovernmental organisation focused on security.

If you would like to deploy a instance of SCAAN to your organisation please contact us using centric@shu.ac.uk to discuss your requirements.

September 2017 - August 2020

MINDB4ACT

Mapping, identifying and developing skills and opportunities in operating environments to co-create innovative, ethical and effective actions to tackle radicalization leading to violent extremism.

www.mindb4act.eu

> **Radicalisation has a destructive impact on individuals and society. MINDb4ACT brings together research, policy and practice to enhance interventions against radicalisation.**

The radicalisation of European citizens is a potentially devastating process, for individuals, their families, wider society, the state and international community. During the radicalisation process, an array of observable behavioural traits, such as changes in attitude, aptitude, beliefs, choice of company (and, equally, choice of isolation), act as warning signs. Additionally, a variety of risk factors that indicate vulnerability to radicalisation have been identified like social marginalisation, identity crisis and significant experiences of loss. Identifying these traits early may lead to more successful interventions and subsequent reintegration into society.

MINDb4ACT aims to improve current counter-radicalisation policies through the collaborative use of innovative, open, participatory and user-centred environments. This will be achieved by co-designing research, exchanges, strategic-policy exercises, training courses and pilot projects based on social innovation and civic engagement schemes across five specific domains: prisons and the judiciary system, migration hotspots and asylum centres, schools, cities and the internet and media.

The results of MINDb4ACT are being delivered through four key priorities:

01. Systematising the available knowledge and expertise to support strategic decision-making

02. Enhancing interdisciplinary fieldwork on terrorists' recruiting grounds through socialisation and other techniques

03. Utilising big data in order to analyse the information related to the communication practices of violent radicalisation

04. Improving existing links between academia including non-EU researchers, policy-makers and other stakeholders

CENTRIC leads work stream that provides new insights on violent extremism by identifying deficits in knowledge transfer and providing new opportunities for researchers on radicalisation. We coordinate surveys of the main actors involved in national action plans on radicalisation and investigate how to improve current research and innovation infrastructures by systematising and collecting current data, analysing how empirical evidence is transferred into policy frameworks and practices used by LEAs and frontline practitioners operating in the field.

This project has received funding from the European Commission Horizon 2020 research and innovation programme under grant agreement No 740543.

MINDb4ACT

May 2018 - April 2021

PROPHETS

Prevention of radicalisation online through the proliferation of harmonised toolkits

www.prophets-h2020.eu

As the intersections between terrorism and organised crime deepens in the cybersphere, public security risks falling behind emerging threats.

The lines between contemporary terrorism, organised crime and cybercrime are blurred. Increasingly, cyberspace is used to illegally fund, recruit, train and incite individuals against European social and democratic ideals. This problem extends far beyond Jihadist terrorism into the violent extremism of the far-right and far-left at domestic, EU and international levels.

Recent events highlight the need for further research to improve our understanding and develop tools to combat the process of online radicalisation. PROPHETS researches into how individuals become radicalised and what technologies and tools can be deployed to reduce related cybercrime. The main goal is to prevent serious crimes by building resilience in people and society.

PROPHETS looks at the wider psychological and behavioural dimensions of radicalisation, providing a methodology for detecting, investigating and monitoring concerning trends and indicators for a wide variety of criminal actors, this moves beyond the traditional classification of radicalisation for violent extremist and terrorist narratives, and applies to organised criminal networks and individual «cybercrime as a service» providers. In order to evaluate these potential harmful behaviours, the PROPHETS project will focus on two distinct groups with the potential to become radicalised in a societally damaging manner; these groups are specified as being 'vulnerable' and 'influential' actors.

PROPHETS delivers four strategic outcomes:

01. Analysis and synthesis of behavioural radicalisation

02. Open-source investigation and analysis tools

03. Best practice roadmap and policymaking toolkit

04. Proactive stakeholder and citizen awareness raising activities for cyber risks

A key output of the project will be a real-time expert notification portal that will provide a central pool of advice from approved and vetted experts to assist law enforcement with ongoing investigations.

In PROPHETS, we are responsible for crafting the user and socio-economic requirements for the technology development, leading the research into the human factors underpinning online crime and radicalisation, and developing the best practice roadmap and policymaking toolkit. CENTRIC is also the technical lead in PROPHETS and oversees the harmonisation and alignment between the research, requirements, development and evaluation phases of the project alongside dedicating specific development capacity to the real-time expert notification portal.

This project has received funding from the European Commission Horizon 2020 research and innovation programme under Grant Agreement No 822380.

January 2017 - December 2019

ISM-KA

International security management knowledge alliance

www.ism-ka.eu

> **A master's degree programme delivering a comprehensive understanding of the security domain to future leaders in law enforcement, local government and security policymaking.**

Reacting to and preventing security threats demand collaborative security solutions across a wide range of stakeholders. Natural hazards, mass immigration, terrorism and the growing interdependencies within critical infrastructure have brought home the message that security management has exceeded the local level. Yet, clear concepts, structures and mindsets for a truly European security system are still missing.

ISM-KA addresses this issue by creating sustainable and concrete resources to foster international security collaborations. The ISM-KA undertakes horizon scanning to identify emerging security threats and synthesise this knowledge into a platform for public and private security experts. ISM-KA will deliver a multidisciplinary accredited MSc curriculum alongside online security education programmes to deliver these outcomes for the wider public.

The guiding principles of the project are multi-stakeholder involvement, evidence-based management, co-creation, and policy-practice alignment, all taken from an international perspective. ISM-KA will establish an international learning, teaching, and knowledge-sharing environment that will contribute to the development and professionalisation of leadership, innovation and operational proficiency in the field of international safety and security.

The course will take a wide-ranging approach to delivering international security management enabling students to choose their own path within the programme which delivers a balanced approach combining rigourous research with operational relevance. Students who enroll in the masters will graduate with an extensive understanding of the key opportunities and threats working in modern day, international law enforcement environments bring.

CENTRIC is designing and developing a number of modules for use within the MSc programme, these modules range from cybercrime to open source intelligence to counter-terrorism.

A trial of the programme is expected to commence from January 2020. If you, or your organisation, wishes to enrol or discuss your requirements for such a course, please contact the CENTRIC team using centric@shu.ac.uk.

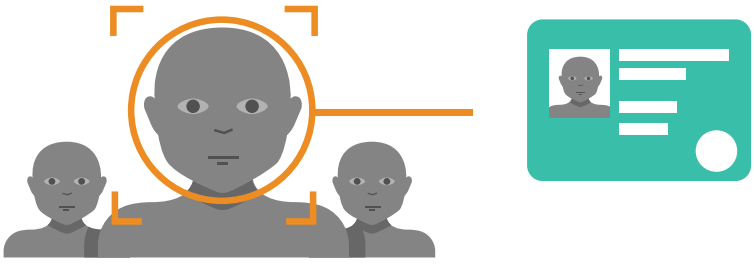
Co-funded by the Erasmus+ Programme of the European Union

Future Operational and Research Programmes

CENTRIC is constantly looking to break in to new areas and domains to keep pace with the forefront of technological challenges in the security sector brought forth by both criminals and LEAs. We have highlighted three key developments that have the potential to significantly impact the way LEAs operate, challenges they need to overcome and the technologies available to support them with these goals.

Applications of AI for situational awareness

Situational awareness (SA) is a environment ripe for the intelligent application of machine learning and artificial intelligence (AI). AI can be applied to detect and predict major incidents using data from social media, crowd-sourced reports and other contextual information while different techniques can be applied to the same data to identify misinformation and disinformation, assess sentiment and extract meaningful entities and objects. The amount of visual media available is exceeding that of text, AI can provide near real-time analysis of images and video extracting objects, voice, text, iconography and pattern matching as well as supporting unparalleled opportunities for face detection and recognition. Finally, as data sets grow more disparate, linking of actors, events, locations and plans will rely even more heavily on sophisticated algorithms to help connect the dots in meaningful ways to investigators to speed up intelligence analysis and provide better threat detection and early warning capabilities.



Augmented reality for LEA training

In the past five years, the go-to technology for training law enforcement officers has been to simulate environments using virtual reality technologies. Augmented reality (AR) has the ability to provide a halfway house between live-play exercises and entirely virtual ones. As AR headsets have moved towards lighter, wireless form factors officers can now wear and train with them without being tethered to a nearby computer allowing them to bring near limitless scenario configurations. AR and head-up displays canbe used to provide contextual informtion to officers during live-play exercises in the form of building layouts, colleague and adversary positions, and other situational information. Alternatively, AR itself can be used to simulate the existence of other actors in the field creating a richer scenario without employing further manpower. In CENTRIC, we see AR as a key future technology for law enforcement operating in counter-terrorism, CBRNE, and public order environments. LEAs that invest in such technologies early will see widespread benefits in the range of training they can offer their officers and the skill levels they can reach.

Internet intelligence and investigation

CENTRIC is now delivering several products and services focused around internet intelligence and investigation (III), as wel move forward into the next year we expect that several of these services will be in full operational deployment in law enforcement agencies across Europe. Our initial three key focus areas for III are to support LEAs in proportionate but automated information extraction from the web and social media using a variety of retrieval and investigator-led techniques, to ensure that this information extraction is fully auditable through employing robust chain of evidence collection methods and to provide advanced analytical support to ensure that, once collected, investigators are able to extract maximum value from the data they hold. New opportunities in III are to consider the impact that cryptocurreny has had on financing organised crime, terrorist and child sexual exploitation and the methods to follow, track and trace such flows.

September 2018 - August 2021

CONNEXIONS

Interconnected next-generation immersive IoT platform of crime and terrorism detection, prediction, investigation, and prevention services

> **Next-generation technology to ensure that LEAs are equipped with the tools to stay ahead of cyber criminal and terrorist threats.**

As crime and terrorism evolve, the range of technologies available to criminals is ever increasing. LEAs must be capable of providing effective solutions to detect, predict, mitigate and prevent as well as investigate such activities and counteract the use of advanced technologies.

CONNEXIONS delivers next-generation detection, prediction, prevention and investigation services for law enforcement agencies using information fused from a wide range of sources including online, IoT sensors, video streams and traditional command and control. It will be presented to investigative teams, field officers and command and control through a variety of modalities that are tailored to the needs of the particular investigation. CONNEXIONS will be validated through three key use cases: a counter terrorism operation at a public event, a human trafficking investigation, and a crime scene investigation.

Through CONNEXIONS, CENTRIC will deliver social and web content acquisition, misinformation and disinformation detection as well as robust measures for secure data management and auditing to support

CONNEXIONS has received funding from the European Commission Horizon 2020 programme under grant agreement number 786731.

VISER

Virtual Investigative Simulation Environments for Radicalisation

VISER is an innovative new approach for both raising awareness in the general public as well as providing specialist training to first line practitioners in the field of countering radicalisation. VISER was developed to resolve a distinct challenge and gap in the operational-market for CVE (countering violent extremism) products and courses. CENTRIC's experience of working alongside law enforcement and CVE opractitioners on projects such as TRANSRAD, MINDb4ACT and PROPHETS have allowed for several research opportunities wherein a clear need for more engaging and interactive CVE training packages has been requested.

Through a developed gap-analysis, CENTRIC has developed a series of simulated environments to be experienced through the HTC Vive VR kit. These environments, built in the Unreal engine and utilising photogrammetry technologies, allow for the rapid construction of flexible simulation environments that are filled with relevant 'props' that investigators or the wider public may search for. These items may include propaganda newspapers and documentation, photos of notorious extremist influencers, weapons and explosives, flags, clothing and other iconography, controversial reading and video material, as well as signs of concern indicators and violence in the environment.

The inclusion of these replicated materials provides for an engaging interactive environment, in which for educational and awareness purposes, the knowledge transferred to participants may have increased impact and a longer term retention period.

November 2013 - May 2016

TRANSRAD

Transversal Bridge

> **Developing effective counter radicalisation programmes across all forms of violent extremism required in-depth understanding of the links and synergies between different radical groups.**

Whilst much attention is paid to Islamic radicalisation, the growing threat of violent and political extremism emerging from both right and left wing factions cannot be ignored. These factions form alliances across Europe to strengthen and amplify their messages. However, understanding these alliances play little part in anti-radicalisation approaches.

TRANSRAD addressed the emerging threat of transversal terrorist alliances for European nations and communities by detecting and profiling the emerging threat of transversal European radical groups and by raising the awareness of institutional bodies and civil society about the potential risks of these "radical bridges". The research within TRANSRAD comprised of several counter-radicalisation case studies enabling the identification of new and emerging cross-cutting threats and the connections between different groups, individuals and narratives. From the project, CENTRIC delivered delivered an interactive training package to support institutional bodies, statutory organisations and NGOs in delivering anti-radicalisation training.

TRANSRAD was co-funded by the Prevention of and Fight against Crime Programme of the European Union

November 2008 - April 2011

ODYSSEY

Strategic pan-European ballistics intelligence platform for combating organised crime and terrorism

> **Innovation around crime and security is hampered by a lack of interoperable datasets and unwillingness to share data for the greater good. In this increasingly digital age the more organisations collaborate, the better results they will achieve.**

LEAs recognise the investigative challenge brought about by the variety of data systems in operation across Europe. It is not possible to collectively analyse ballistics data extracted from the heterogeneous systems currently in use.

Odyssey sought to develop an interoperable process to analyse ballistics data to tackle organised crime and terrorism. Odyssey automatically combined data from disparate high volume data repositories for cross-correlation and automated analysis using this to extract intelligence using advanced semantic knowledge and data-mining to facilitate appropriate, fast and responsible decision making and alerts.

Odyssey was the catalyst for the creation and formalisation of CENTRIC as an independent research centre within Sheffield Hallam University. Odyssey provided CENTRIC with a clear platform for future research and many of the themes explored within the project have evolved in line with our core capabilities.

ODYSSEY has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement number 218237.

Other projects

ATLAS

Advanced training, learning and scenario simulator

> **Realistic training in virtual reality simulations to enhance real-time decision making in the field.**

Atlas is a virtual reality training simulation for field operatives working for the International Organisation for Migration (IOM). The scenario supports IOM's hostile environment awareness training package and allows the wearer to experience and react to an ambush during a convoy in Sudan.

Realistic training simulations through virtual reality can make reactions in emergency and stressful situations feel like second nature, enabling trainees to make better decisions when they are faced with difficult situations in the field.

Unpacked VR

Advanced training, learning and scenario simulator

> **Realistic training in virtual reality simulations to enhance real-time decision making in the field.**

When Syrian artist, Mohammed Hafez sought to raise awareness of the turmoil that refugees experience he teamed up with writer Ahmed Badr to create a unique, highly impactful exhibition called Unpacked Refugee Baggage. The exhibition displayed opened suitcases containing models of the homes of refugees that had been destroyed by war complete with audio narration. CENTRIC developed an accompanying virtual reality model of one suitcase which allowed users to enter and experience one of the homes.

Community Response

> **Community Response streamlines communication and data collection for humanitarian missions in developing countries, bringing donors and beneficiaries**

Sharing messages in countries which may have more ad-hoc communication strategies and infrastructure has made it challenging for organisations to disseminate important messages to populations in those areas. Several years ago, IOM developed the Community Response Map (CRM) to bring together gift aiders and receivers, enabling beneficiaries to provide better feedback in a simple and expedited workflow.

Building on the CRM project, CENTRIC were approached by IOM to develop a companion mobile application to improve and speed-up data collection as well as standardise survey creation and responses. The application has three main roles: capture and share migrants' stories, collect digital consent forms in the field and share project impacts with key stakeholders. The app is being used across the work and is supporting the ongoing Migrants as Messengers campaign which engages returning migrants to share their stories about their experience of irregular migration.

November 2018 - October 2021

MIICT

ICT Enabled Public Services for Migration

MIICT delivers ICT-enabled services co-created and co-designed on the realities of migrant experiences to enhance integration for the benefit of all.

Discrimination, unemployment, and limited access to education rank highly among migrants of varying demographics; including different age groups, genders, education levels and immigration status and are a barrier to integration in European societies. MIICT aims to design, develop and deploy solutions to help address the challenge of migrant integration. The project works directly with migrants, refugees, NGOs (Non-Governmental-Organisations) and public sector services to co-create and co-design ICT-enabled services around the socio-cultural, economic and legal circumstances of migrants.

Specifically, MIICT looks to address the management of migrant integration, the customisation of services to match migrants' needs and the need for sustained and improved inclusion of migrants. This evidence-based and inclusive software solution aims to improve labour market access, matching individuals with jobs and development opportunities based upon their specific and unique contexts.

CENTRIC is the coordinator of the MIICT project meaning we are responsible for the project's implementation as a whoel. in particular we place specific emphasisis on the inspiration and ideation phases.

MIICT has received funding from the European Commission Horizon 2020 research and innovation programme under grant agreement number 822380.

CYBER CENTRIC

Building cyber resilience in small and medium sized enterprises

Providing serious games training to SMEs based on real world scenarios will enhance their security and resilience against a plethora of cyber threats.

Currently there are few opportunities for small and medium sized enterprises (SMEs) to improve and increase their cyber resilience and protect themselves from a cyber-attack, loss of data or even inadvertent misuses of their network or data. Equally, SMEs are often at a greater risk of experiencing a cyber incident due to a lack of dedicated IT teams, financial resources and ad-hoc procedures.

The Yorkshire Cyber project developed a choose-your-own-adventure serious game as part of a training platform and associated programme to deliver cyber security training to SMEs in various locations across the Yorkshire and Humberside region in the United Kingdom. The player is lead through a number of cyber related scenarios, asking them to make a series of decisions which can have financial and reputational impacts or increase their cyber resilience. The current scenarios are based on threats via social engineering, ransomware, data theft, denial of service attacks and GDPR infringements.

Following the successful completion of the Yorkshire Cyber element of the project, the team was approached to increase the scope of the game and introduce a story mode that allows players to move through the game seeing the impact of their decisions as they move forwards. This reinvention of the game goes under the banner Cyber Centric.

Cyber Centric has recently been the recipient of two national cyber awards: the Learning Innovation in Cyber Awareness Award and the Most Original Cyber Security Product.

May 2017 - April 2020

ROBORDER

www.roborder.eu

> **Drones and robots can go and see places border patrols could never reach. Combining them with human-in-the-loop command and control operations can vastly increase threat detection.**

Border authorities and LEAs across Europe face important challenges in terms of how they patrol and protect borders. Unmanned vehicles provide opportunities to patrol such areas remotely, improving efficiency and allowing human patrols to focus on specific areas. Currently, border authorities do not have access to an intelligent integrated platform that brings together functions that support integrated border surveillance.

ROBORDER seeks to develop and demonstrate a fully-functional, autonomous border surveillance system utilising unmanned mobile robots. It will include aerial, water surface, underwater and ground vehicles. Using data from multimodal sensors attached to the robots and existing static sensors, border authorities will be provided with a complete and detailed situational awareness picture of the area under their command. ROBORDER will have the capacity to detect threats such as criminal activities and hazardous incidents as well as support command and control teams in their

Roborder has received funding from the European Commission Horizon 2020 research and innovation programme under Grant Agreement No 740593.

May 2018 - April 2021

CIVILNEXT

Next generation of information systems to support EU external policies

www.civilnext.eu

> **With a growing number of CSDP operations being undertaken by joint civilian-military missions, effective information sharing and communication is critical to their success on the ground.**

The European Union undertakes several overseas missions which utilise both civilian and military capabilities. These missions take place across Europe, Asia and Africa and fall under the EU's Common Security and Defence Policy (CSDP). Recently the EU Global Strategy on Foreign and Security Policy has highlighted a need to improve its civilian missions through better communication, information sharing, joint reporting, analysis, and response planning between member states, EU delegations, European Commission Services, the EU External Action Service and the CSDP missions themselves.

CIVILnEXt is a pre-commercial procurement action that aims to contribute towards the next generation of information systems to support EU external policy. The aim of CIVILnEXt is to develop, test and validate a cost-effective and interoperable Operation Control Platform (OCP) that will support the execution of civilian CSDP missions; facilitating greater information exchange and supporting situational awareness and operation control in diverse theatres of operation.

CIVILNEXT has received funding from the European Commission Horizon 2020 research and innovation programme under grant agreement No 786886.

May 2015 - April 2018

UNITY

Strengthening the connection between the police and their communities
www.unity-project.eu

> **Community policing enables the police and their communities to work together to proactively solve the problems that affect them directly**

Unity created a new, community-centred approach to policing by developing new tools, procedures and technologies that put people at the heart of identifying policing priorities and ensured that citizens are an integral part of developing sustainable solutions. Unity achieved this by capturing the best practices, developing technologies and delivering training and awareness raising activities that delivered enhanced cooperation between police and the communities they serve.

As a result of the Unity project six key pillars of community policing have been identified: accountability, addressing local needs, building trust and confidence, information sharing and communication, collaboration and preventing crime.

CENTRIC developed a mobile application to support communication between citizens and LEAs. The application provides citizens with the opportunity to keep up-to-date with their local community, engage in discussion with the police in an informal manner and organise meetings and events. As an added-value to the project, CENTRIC developed a simple adventure game, AESOP, which aims to educate community members on ways of identifying and addressing key local issues through proactive engagement with LEAs. The game currently features scenarios which tackle street drinking, begging and vagrancy, domestic violence, parking, speeding and modern day slavery.

UNITY has received funding from the European Commission Horizon 2020 research and innovation programme under grant agreement No 653729.

December 2013 - November 2016

ATHENA

Empowering citizens, protecting communities
www.projectathena.eu

> **Social media can be a lifeline in a crisis. Bringing victims, citizens and first responders together through technology enhances situational awareness for all.**

During a major crisis event the public are under-utilised crisis responders, as they are often first on the scene and vastly outnumber emergency first responders. They can be creative and resourceful, self-organise into voluntary groups, adapt quickly to changing circumstances, and emerge as leaders to perform countless life-saving actions.

Athena aimed to develop a holistic solution for utilising citizens and social media in the midst of a crisis or disaster. The two main outputs of Athena project were a set of best-practice guidelines for first responders and citizens in the use of social media and mobile communications in crisis situations; and a situational awareness platform which realised and validated the use of social media and mobile communications for crisis response across a number of live, simulated crisis events. This situational analysis platform went on to form the basis of the SCAAN project which is now providing operational support to staff from the International Organisation for Migration across the

Athena has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 313220.

May 2014 - April 2016

COURAGE

Cybercrime and cyberterrorism European research agenda
www.courage-project.eu

> **Providing a blueprint to effectively tackle cybercrime through innovative investigation strategies.**

The pace of change within the area of cybercrime makes it difficult to identify long-term future research challenges which can be utilised by researchers and policy makers to improve the safety of citizens, critical infrastructure, and support cybercrime investigators. The results of COURAGE delivered an overarching, definitive research agenda for cybercrime that will help deliver the long term strategic goals of the EU in tackling the threat of cybercrime by bridging the gap between research and the operational front-line of cybercrime investigation. The multidisciplinary research of COURAGE constitutes a major innovation in policing research to tackle the most pressing contemporary security challenges.

COURAGE has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement number 607949.

September 2014 - August 2016

UINFC2

Engaging users in preventing and fighting cybercrime
www.uinfc2.eu

> **With swarms of illegal content circulating on the internet every day, UNIFC2 helps investigators detect and investigate cybercriminal activity.**

UINFC2 aimed to build and strengthen the capabilities of LEAs, citizens and EU bodies to strategically combat cybercrime. UINFC2 designed, developed and pilot tested a multi-lingual, online platform for automatically detecting illegal content from social media, blogs, and underground communities. This information is used to determine investigative priorities. In particular, UINFC2 focused on online Child Sexual Exploitation (CSE) and facilitated the formal exchange of compiled information, produced by intelligent analysis of online intelligence in order to enhance collaboration and effectively counteract cybercrime. This supported the mission of the recently founded European Cybercrime Centre (EC3) in Europol by producing reports on cybercrime trends and emerging threats in order to provide comparable statistics among Member States.

UINFC2 has been co-funded by the Prevention of and Fight against Crime Programme of the European Union.

August 2018 - November 2019

INFIRST

Intelligent interpretation of forensic information in substance misuse cases

> **Harnessing advances in data mining and machine learning to enable analysts to make accurate assessments in substance misuse investigations.**

Many services require an understanding of whether someone has a history of alcohol or drug abuse. Forensic analysis of hair, urine and nail samples can indicate whether the drugs themselves or their metabolites are present in the system. However, simply the presence of these substances does not necessarily indicate the level of use. The presence of certain substances instead may be caused by transference from the environment or lower than expected values may be found due to the impact of daily activities such as hair treatments. Furthermore, if multiple substances are taken together this may impact levels of certain metabolites in the samples taken.

CENTRIC has recently embarked upon a project with a company that specialises in the collection and analysis of hair, nail and urine samples for the purposes of detecting the presence of alcohol and a wide range of illicit substances. The project utilises the latest advances in data mining and machine learning to support their analysts' decision making when determining the extent to which the person under investigation has consumed certain substances and how their usage of such substances may have changed over time.

May 2014 - April 2016

ePOOLICE

Early pursuit against organized crime using environmental scanning, the law and intelligence systems
www.epoolice.eu

> **Organised crime happens in the shadows. Connecting the dots between seemingly disparate events can uncover long-term organised crime threats that might otherwise go undetected.**

Organised crime is becoming more diverse in its activities and methods as criminal groups across Europe collaborate and cooperate across borders. ePOOLICE developed a system for the scanning and analysis of a variety of information streams including open source social media, public and government databases as well as making use of internal law enforcement data whilst analysing their reliability and relevance.
By identifying stakeholder needs and the tools required to combat the problem, an efficient and effective environmental scanning system was created. ePOOLICE detects early warning signs of organised crime. It specifically focuses on drug and human trafficking as well as evaluating trends and factors driving 'future crime' in order to identify potential 'weak signals' in emerging organised crime trends.

ePOOLICE has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 312651.

SELECTED AND FORTHCOMING PUBLICATIONS

- Application of Big Data for National Security
  Babak Akhgar, Gregory B. Saathoff, Hamid Arabnia, Richard Hill, Andrew Staniforth, and P. Saskia Bayerl
  2015

- Application of Social Media in Crisis Management
  Babak Akhgar, Andrew Staniforth, and David Waddington
  2017

- Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities
  Babak Akhgar and Ben Brewster
  2016

- Community Policing – A European Perspective: Strategies, Best Practices and Guidelines
  P. Saskia Bayerl, Ruza Karlovic, Babak Akhgar, and Garik Markarian
  2017

- Cyber Crime and Cyber Terrorism Investigator's Handbook
  Babak Akhgar, Andrew Staniforth, and Francesca Bosco
  2014

- Intelligence Management: Knowledge Driven Frameworks for Combating Terrorism and Organised Crime
  Babak Akhgar and Simeon Yates
  2011

- Open Source Intelligence Investigation:
  From Strategy to Implementation
  Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson
  2016

- Strategic Intelligence Management
  Babak Akhgar and Simeon Yates
  2013

- The Routledge Companion to UK Counter-Terrorism
  Andy Staniforth
  2012

- Big Data analytics and Situational awareness for Security, Safety and Policing
  Babak Akhgar, Tony Day and Helen Gibson.
  2019

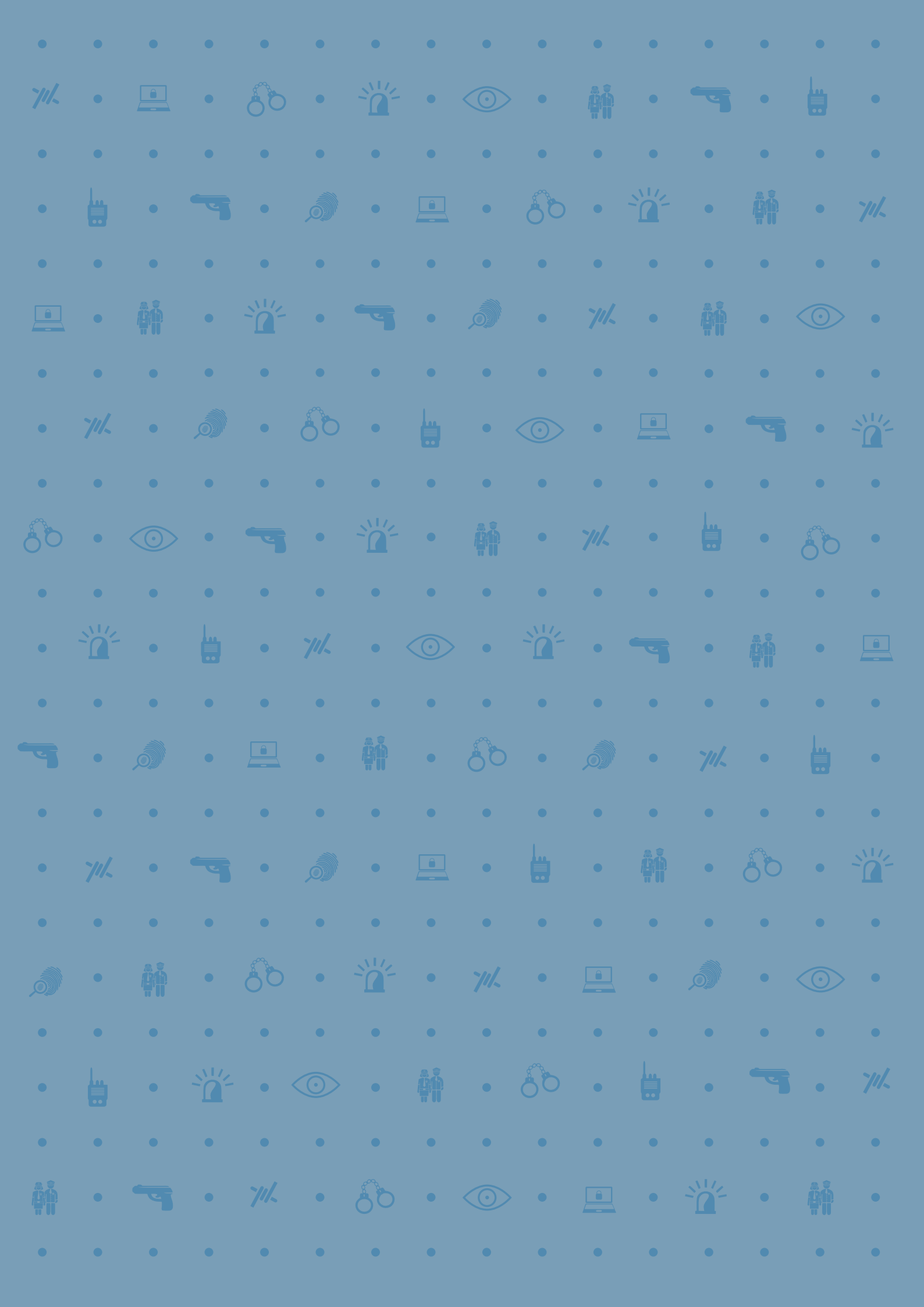
- Dark Web Investigation.
  Babak Akhgar, Marco Gercke and Stefanos Vrochidis.
  2019

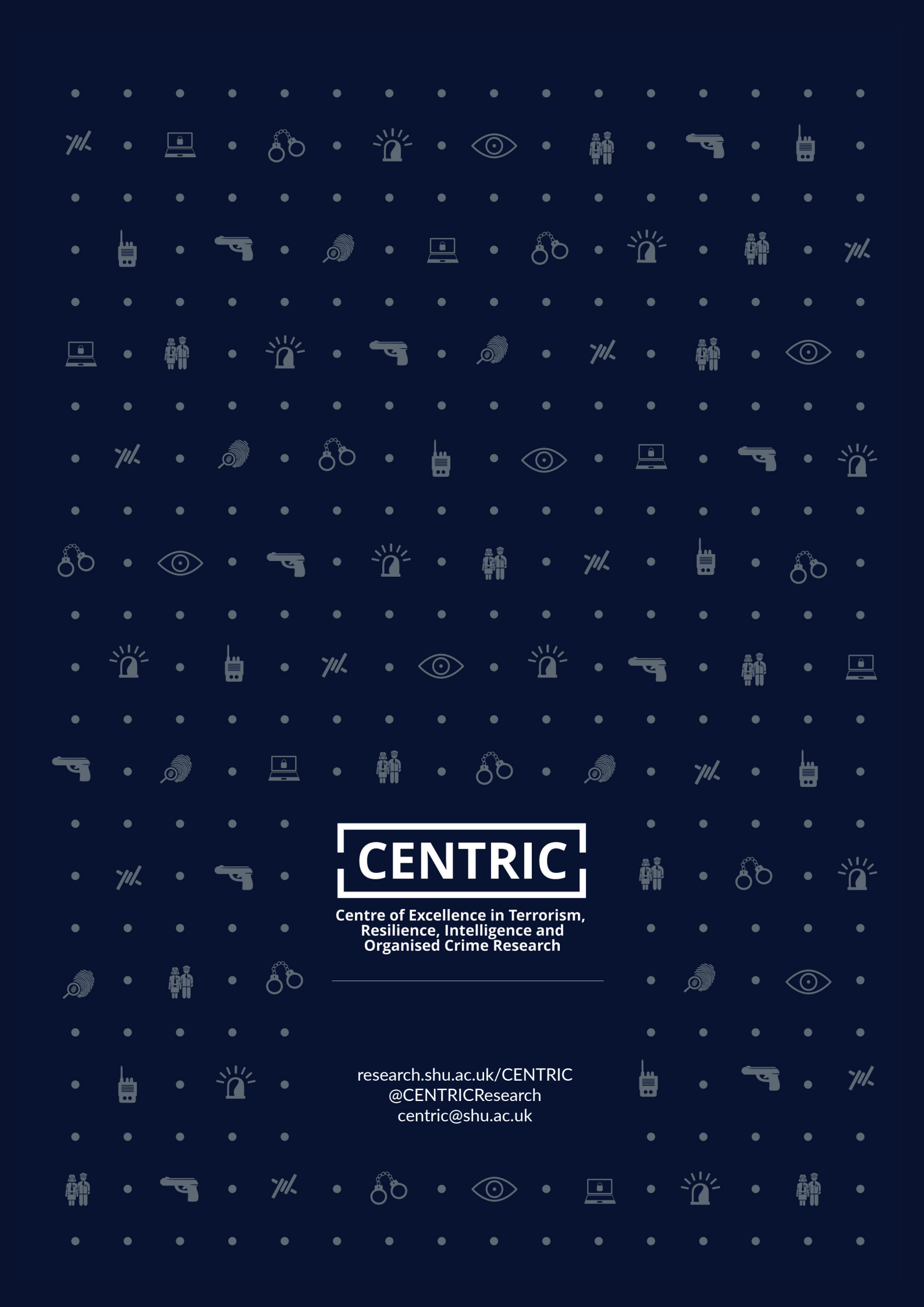
- Global Counter-Terrorism.
  Andy Staniforth and Babak Akhgar
  2019

- Serious Games for Enhancing Law Enforcement Agencies - From Virtual Reality to Augmented Reality
  Babak Akhgar
  2019

- Social Media Strategy in Policing: From Cultural Intelligence to Community Policing.
  Babak Akhgar, P. Saskia Bayerl, and George Leventakis.
  2019

- Technological Tools for Investigating Radicalization Trends - Case Studies in Europe and Asia.
  Babak Akhgar, Douglas Wells and José María Blanco
  2019





CENTRIC

Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research

research.shu.ac.uk/CENTRIC
@CENTRICResearch
centric@shu.ac.uk