Military Forensic Exploitation R&D Requirements

The Military Forensic Exploitation Symposium is being held to bring together relevant stakeholders to discuss key issues. The **Research and Development Workshop** will be held on day 1 of the symposium. The workshop will focus on current and future forensic science research and development with the aim to develop an integrated forensic exploitation research and development strategy.

The Australian Defence Organisation has produced unclassified research and development strategies that provide an overview of the Defence research requirements, including requirements for forensic exploitation. These strategies include:

- Shaping Defence Science and Technology in the Joint Domain 2017-2021, Joint Science and Technology Strategy, Australian Government Department of Defence, 2016
- Shaping Defence Science and Technology in the Land Domain 2016-2036, Australian Government Department of Defence, 2016
- Army Research and Development Plan 2016, part one: Science and Technology, Army, Australian Defence Force, 2016

The research and development strategies, along with data collected during semi-structured interviews with key stakeholders has been used to develop military forensic exploitation research, development, and innovation requirements (Table 1). The requirements have been grouped into four themes:

- Detection, collection, field analysis;
- Laboratory analysis, attribution, reporting;
- Force protection; and
- Situational understanding.

During the Research and Development Workshop breakout groups the four military forensic exploitation themes will be discussed with a view to add future requirements and discuss opportunities for research and development program. Table 1, forensic exploitation research requirements are provided as a guide to facilitate discussion and is not meant as an exhaustive list of requirements. It is anticipated that during the breakout discussion further requirements will be articulated along with potential research and development projects.

The data generated from the breakout research and development groups will be used to develop a military forensic exploitation research and development strategy. It is anticipated that the strategy will be used as the corner stone to develop a collaborative military forensic exploitation research and development program.

Detection, Collection, Field Analysis

Priority	Requirement	RD&I
Prevention, prediction, detection, neutralisation, mitigation and exploitation of improvised threats.[1] Including, Chemical, Biological, Radiological and Nuclear (CBRN) Defence[2] and improvised explosives.	Enhanced CBRN detection, field analysis, and laboratory analysis.[2]	
	Enhanced CBR detect to treat capability, including diagnosis from clinical samples.[2]	
Detection and collection of forensics and biometric items in a deployed contested environment.[3]	Techniques, tactics and procedures for the rapid detection and collection of forensic and biometric items in reduced turnaround time.Error! Bookmark not defined.	
	Field portable detection and collection capabilities of forensic and biometric items, including validation of equipment and processes.Error! Bookmark not defined.	
	Enhanced sample collection, recovery, sub-sampling, and recovery from degraded or compromised items.[3]	

Laboratory Analysis, Attribution, Reporting

Priority	Requirement	RD&I
Level 2 and 3 analysis of forensic and biometric items.[3]	New and emerging forensic and biometric exploitation technology is of potential utility to the ADF's development of a future forensic and biometric exploitation capability?[2]	
Provencing attribution.[3]	Provencing of person of interest to determine likely movements and origin.[3]	
	Provencing of agents and materiel to determine their origin.[3]	
Joint logistics including planning, acquisition, storage and distribution.[1]	Enhanced ability for store and transportation of forensic items and CBRN agents.Error! Bookmark not defined.	

[1] Shaping Defence Science and Technology in the Joint Domain 2017-2021, Joint Science and Technology Strategy, Australian Government Department of Defence, 2016
[2] Army Research and Development Plan 2016, part one: Science and Technology, Army, Australian Defence Force, 2016
[3] Research and Development requirement collected through interviews with key stakeholders, 2016

Force Protection

Priority	Requirement	RD&I
Force protection from Chemical, Biological, Radiological and Nuclear (CBRN) Defence and explosives.[2,4]	Understanding and mitigating the next generation of CBRNe threats, including improvised and high end).[4]	
	Reinforced Combat Brigade is able to survive and fight in a CBRNE environment.[4]	
	Strategic counter-CBRNE functions provided by SOCOMD.[4]	
	Reduce force exposure with autonomous detection and electromagnetic countermeasures to improvised explosive threats.[4]	
	Threat intelligence, surveillance and recon (ISR) system/weapon seekers indicate are key Signature Management defeat technologies	
	The deployed Land Force is able to detect threats and deny adversary electronic and cyber attack.[4]	
	Degrade an adversary's offensive and exploitation capability through disrupting electromagnetic spectrum system control.[4]	
Rapid modernisation of distribution system through the embracing of automated and autonomous technologies that reduce personnel threat exposure and provide a step-change in efficiency.[4]	Semi-autonomous casualty evacuation.[4]	
	Stand-off detection and collection of forensic and biometric items in a contested or contaminated threat environment.[3]	
	Semi-autonomous initial assessment and treatment of Battle Casualties.[4]	

[4] Shaping Defence Science and Technology in the Land Domain 2016-2036, Australian Government Department of Defence, 2016

Situational Understanding

Priority	Requirement	RD&I
Collection, fusion and targeting.[2]	S&T support to provide an enhanced collection, fusion and targeting.[2]	
	Refine the process of collection, collation (incorporating common operating picture dissemination and targeting.[2]	
Integrated biometric capability and exploitation.[2,4]	Limitations of the Army Full Spectrum Exploitation process and systems, particularly in relation to data and links to national and coalition systems and how these limitations are mitigated or improved.[2]	
	Policy, technical and organisational requirements to enable integration with coordinated whole-of-Government forensics and biometric enterprise.[2]	
	Enhanced facial recognition techniques and technology for operational use.[2]	
Intelligence, Surveillance, and Recon (ISR).[4]	Integration of ISR into the Joint domain with coalition interoperability, and resilience to degraded and contested environments while achieving information dominance over our adversaries.[4]	
	Development of an ISR enterprise with advanced analytics, intelligence fusion and efficient dissemination of information as a focus.[4]	
	Timely awareness through manned-unmanned teaming with ISR assets.[4]	
Technology foresighting, forecasting and preparatory scenario methods to mitigate against the strategic shock of emerging and disruptive technology.[4]	Joint counter improvised threat to identify the scope of potential future emerging improvised threats and the option to counter them.[1]	
	Early indicators and warnings. Investigate sources of potential technological strategic surprise to develop and respond to emerging opportunities and threats.[1]	