Project Heikick: IMD Sufficiency for the F-35

Dragovic M[1]
[1]Dst Group

IMD Challenges from a Reprogrammer's Perspective, May 30, 2018, 9:45 AM - 10:45 AM

Project Heikick is an Australian Government research initiative initially aimed at investigating the relationship between the quality and quantity of Intelligence Mission Data (IMD) and F-35 performance. Future phases of Project Heikick will aim to explore concepts such as dynamic reprogramming and to quantify the benefits of proposed improvements to F-35 mission systems to aid decision makers voting on block upgrades. This presentation will outline the IMD challenges to support 5th generation platforms and detail a series of studies which will aim to better understand the performance of the Australian F-35 at Australian IOC (2020) with available IMD. The results of the studies could have both tactical significance and influence on IMD collection priorities.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Summarising network information for cyber situational awareness via cyber-knowledge integration

Sikos L[1], Stumptner M[1], Mayer W[1], Howard C[2], Voigt S[2], Philp D[2]
[1]University of South Australia, [2]Defence Science and Technology Group

Summarising network information for cyber situational awareness via cyber-knowledge integration, May 30, 2018, 3:00 PM - 4:00 PM

Cyber situational awareness is critical to applications such as network vulnerability assessment, attack prevention and network defence. However, cyber situational awareness is challenged by the increasing complexity, diversity, and dynamics of communication networks. In addition, developing an understanding of the network elements, how they are interconnected and how data flows around the network, can be a time-consuming manual process for analysts. Some sort of automated support is required. Using open standards, such as the Resource Description Framework (RDF), the semantics of network topology and traffic flow can be captured in a unified form, ready for machine processing. Based on the formally described knowledge, the integrity of datasets can be verified automatically, and new statements can be generated using strict rules to facilitate knowledge discovery. The output of these tasks can help analysts to better understand network information and find valuable, non-trivial information they could otherwise overlook. However, analysts may not consider automatically generated data authoritative. This can be addressed by capturing and representing data provenance information. Provenance gives valuable information about the data source (e.g., router configuration file, routing message, open data), the software that generated the data, and the person who was responsible for executing the network discovery task, thereby providing indicative measures on data trustworthiness, reproducibility, and accuracy.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration
in the Indo-Pacific Region
28 – 30 MAY 2018

Developing RF Vulnerability Awareness Tools for the ADF

Hansen H[1], Mason K[1]

[1]*Defence Science And Technology Group*

Developing RF Vulnerability Awareness Tools for the ADF, May 30, 2018, 9:45 AM - 10:45 AM

The effects of variability in atmospheric conditions on RF propagation are difficult factors to quantify for EW operations in tropical regions. These impact on the ability of the Command to accurately estimate current and near term vulnerability to detection by threat ISR or EW systems, and the ability of the Command to determine the level of radiated power to use when planning a precision EA mission. The underlying cause is the variation in propagation effects due to the complex dependency of refractive index on the meteorological humidity, temperature and wind parameters. The marine boundary layer environment is turbulent which leads to anomalous propagation effects which depending on the conditions, can either trap radiation and duct it to beyond line of site ranges thereby enhancing RF system performance, or steer radiation away from the surface thereby degrading RF system performance. The determination of validated meteorological inputs into RF system assessment tool is challenging but necessary for effective tactical tasking of RF systems. DST Group's program of work in this area comprises: (1) understanding of RF phenomenology, (2) developing tactical decision aides that exploit RF propagation models in the context of corporate information about nearby threats, and (3) staged demonstrations and evaluations of the program outputs. This presentation overviews an initial demonstration of a laboratory decision aide consuming environmental information for efficient determination that ducting effects can explain ES sensor measurements from vessels at ranges significantly exceeding normal ES detection ranges.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
28 – 30 MAY 2018
Interoperability and Collaboration
in the Indo-Pacific Region

Cyber & EW Division – An Overview

Szabo A[1]

[1] *Defence Science & Technology Group*

DST's Cyber and EW division was formed in 2014 to reflect the concept of a cyber-EW continuum. But is this structure as relevant today? The answer appears to be yes, but with some refinements. Here recent efforts to restructure Cyber and EW Division are described, along with the key programs being supported.

An Approach to Future Technology Assessment for EW

Szabo A[1], Herfurth S[1]
[1]Defence Science & Technology Group

An Approach to Future Technology Assessment for EW, May 30, 2018, 3:00 PM - 4:00 PM

An assessment of future technologies, and their game changing potential, is a key input into the construction of an EW science & technology program. Here efforts by DST's Spectrum Sensing and Shaping Major Science and Technology Capability to conduct horizon scanning and technology watch as part of an integrated technology assessment are described. Results from the 2017 technology assessment will be presented, along with future directions for this activity.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
28 – 30 MAY 2018
Interoperability and Collaboration in the Indo-Pacific Region

The Australian EW Enterprise – Future Workforce Requirements

Szabo A[1]

[1]Defence Science & Technology Group

The Australian EW Enterprise – Future Workforce Requirements, May 30, 2018, 1:30 PM - 2:30 PM

The 2016 Integrated Investment Program included an unprecedented investment in EW. Delivery of these capabilities is likely to challenge the Australian EW Enterprise, with workforce being a key stressor. Here a brief analysis of the current EW workforce is presented, along with the anticipated workforce required to deliver the planned EW investment. Some initiatives to grow the Australian EW workforce is also discussed.

Cyber Situational Awareness for Communication Networks

Philp D[1], Thomas L[1], Gilmartin D[1], Voigt S[1]
[1]DST Group

Cyber Situational Awareness for Communication Networks, May 30, 2018, 3:00 PM - 4:00 PM

Information integration across the defence enterprise relies on communication networks. Studying Cyber Situational Awareness and security of these networks is important to ensure timely and accurate decision making, especially for network defence. However, network routing – the critical control infrastructure managing network traffic – is becoming increasingly complex, relying on careful configuration and coordination of multiple technologies at different network layers.

Cyber Situational Awareness research for communication networks requires standard datasets – enabling reproducible experiments and comparison of different S&T techniques and algorithms. However, generating datasets using physical network routing equipment is expensive, time consuming, and inflexible. We need better network test and evaluation environments. Emulation software enables faster and cheaper prototyping of diverse network routing configurations. Emulations facilitate reproducible network experiments and hence S&T comparisons. We can study impacts of network vulnerabilities in a controlled software environment, as well as create detailed network models. Network models provide a common language for describing the complex relationships between multiple technologies – which facilitates information fusion across datasets.

This talk presents our novel network routing datasets and emulations based on a complex example. We show how comparing normal and abnormal datasets is important for network modelling, as well as Cyber Situational Awareness and network defence.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration
in the Indo-Pacific Region
28 – 30 MAY 2018

Impact of New and Emerging Technologies in Electronic Warfare

Andrews R[1,2]
[1]EWTE Consultants Ltd, [2]AOC

Impact of New and Emerging Technologies in Electronic Warfare, May 30, 2018, 9:05 AM - 9:35 AM

Commercial-off-the-shelf (COTS) technologies have changed electronic warfare and their adaptation and use by our adversaries in asymmetric warfare raises great concerns. However, many new and emerging innovative technologies, primarily COTS, are now being funded, developed and implemented into current and planned future EW systems.

The presentation considers some the game-changing technological events in the past two decades in EW and their effect on our ability to counter the resulting threats. Topics will include AESA multi-function radars, common aperture systems, open architectures, FPGAs, GaN amplifier technologies, software defined radios (SDR), drones and stealth. The future impact of COTS technologies in particular are addressed.

An overview of the current threats in the Middle East and eastern Asia will be provided with examples of the technologies employed in those systems including network-based warfare, together with EW Cyber operations.

Some current US and NATO government technology research programmes and their impact on future EW systems and operations are also examined.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration
in the Indo-Pacific Region
28 – 30 MAY 2018

Cross Domain Secure Collaboration

Gottwals (Dr) S[1]
[1]*Adobe Systems*

Cross Domain Secure Collaboration, May 30, 2018, 11:30 AM - 12:00 PM

Introduction

A major challenge with the interoperability and collaboration of sensitive information occurs in cross-domain systems, which possess separate ecosystems. Bringing these separate communities together, with their own unique authentication requirements, often creates a breakdown at the interface between the domains. Adobe offers a cross-domain secure collaboration solution comprised of Digital Rights Management (DRM) for maintaining the dynamic control over the confidentiality of information, a Cross-Domain Data Guard, to translate security policy across domains, and Security Analytics, to oversee and continuously monitor the collaborative environment.

Digital Rights Management (DRM)

To maintain confidentiality of sensitive information, and provide capabilities to establish controls, monitor access and automatically track information as it is shared with collaborators. DRM offers protective safeguards for content:

¥ Persistent protection
¥ Permissions
¥ Revocation
¥ Audit logs
¥ Authentication

Cross Domain Data Guard

A cross-domain transfer of protected documents is accomplished via a Data Guard sitting between the two DRM systems.

Security Analytics

In the cross-domain configuration, applying analytics to DRM audit events is especially important, as policy changes could present potential vulnerabilities. Geographic analysis, based on IP and host logging, provide further insight into access patterns within specific domains and across domains correlated against physical locations.

By adding the ability to collect document events, via a DRM Honey Pot in non-participating domains, like the Internet, potential spillage domains and sources may also be unmasked.

By combining Digital Rights Management (DRM), a Data Guard, and Security Analytics, we can enable cross-domain secure collaboration of sensitive information.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Unveiling Video Streaming Content From Encrypted WiFi Traffic

Jourjon G[1], Seneviratne S[2], Thilakarathna K[2], Xu R[3], Ni Y[3], Cheng A[4], Webb D[4]
[1]Data61-CSIRO, [2]University of Sydney, [3]University Technology of Sydney, [4]DST-Group

Unveiling Video Streaming Content From Encrypted WiFi Traffic, May 30, 2018, 9:45 AM - 10:45 AM

Proliferation of smart devices has led to an exponential growth in digital media consumption, especially mobile video for content marketing. Not only on-demand video distributors like YouTube and Netflix, but also social networking services like Facebook and Twitter feeds today are dominated by videos. This has paved an open free media to exploiters and attackers to distribute content such as fake, radical and propaganda videos. The problem becomes even more acute when majority of video traffic is currently end-to-end encrypted.

Recent advances in machine learning techniques have shown great promise in characterizing encrypted traffic captured at the end points. However, video fingerprinting from passively listening to encrypted traffic, especially wireless traffic, has been reported as a challenging task due to the difficulty in distinguishing retransmissions and multiple flows on the same link. We show the potential of fingerprinting videos by passively sniffing WiFi frames in air, even without connecting to the WiFi network. We are developing Deep Neural Networks (MLPs) and Recurrent Neural Networks (RNNs) that are able to identify streamed YouTube videos from a closed set, by sniffing WiFi traffic encrypted at both MAC and Network layers.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

SydNet: A Linked Data Quality Assessment Framework for Network Data

To A[1], Meymandpour R[1], Davis J[1], Jourjon G[2], Howard C[3], Voigt S[3], Philp D[3]
[1]University of Sydney, [2]Data61-CSIRO, [3]DST-Group

SydNet: A Linked Data Quality Assessment Framework for Network Data, May 30, 2018, 9:45 AM - 10:45 AM

With the massive increases in the scale and complexity of computer and communications networks, understanding the complex inter-relationships between elements in a communications network presents major challenges. However, performing this task competently is crucial to achieving adequate cyber-situational awareness for applications such as network traffic monitoring and management, vulnerability assessment, and defence. There is a range of disparate network data sources such as traceroutes, network diagrams, router configuration files, routing tables, routing protocol messages and open source data. Building computational tools to support this task is crucial for cyber situational awareness. However, information about the quality of the network data sources is essential in order to build analysts' trust in such tools.

We present SydNet, a novel Linked Data quality assessment framework based on semantic technologies to enable network analysts to define critical quality dimensions and compute metrics which can provide an accurate reflection of the quality and reliability of the data sources. The SydNet architecture also provides a number of novel heuristics and metrics which can be used to fuse data from various network data sources. We demonstrate the utility of the SydNet architecture using an experimental scenario in which network analysts attempt to discover which ISPs can provide guarantees that traffic remains within a given country, using BGP datasets.

Chasing the Challenges of Radar Design & Test

Wu R[1]

[1]National Instruments

Chasing the Challenges of Radar Design & Test, May 30, 2018, 1:30 PM - 2:30 PM

Modern radar systems take advantage of wider bandwidth radios, innovative waveforms for adaptability and electronic countermeasures, and the use of large multi-channel systems. These technologies introduce new design and test challenges for radar engineers. This paper examines best practices for solving the test and measurement challenges of modern radar systems, including synchronizing multi-channel RF systems, generating and analyzing wider waveforms, and reducing the cost of test through target emulation.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Multichannel Phase-Coherent Microwave Measurements: 5 Things to Consider

Wu R[1]
[1]National Instruments

Multichannel Phase-Coherent Microwave Measurements: 5 Things to Consider, May 30, 2018, 1:30 PM - 2:30 PM

In the area of military and defense electronics, electronic warfare (EW) and Radio Detection And Ranging (RADAR)
are two of the many applications that rely on multichannel and phase-coherent configurations for signal processing, analysis, and generation. These systems enable cutting-edge performance in some of the vital aspects of EW and RADAR applications, including radar cross-section (RCS) diversity, improved target localization and tracking accuracy, higher angular resolution, increased degree of freedom, increased waveform diversity, and increased number of uniquely identifiable targets. In essence, they form the backbone of a new generation of military and defense systems focused on multiple input, multiple output (MIMO) and intelligent wireless communication.

A Heuristic Connected Components Algorithm and FPGA Implementation for Radar Target Recognition

Cassidy P[1]

[1]Simbiant Pty Ltd

A Heuristic Connected Components Algorithm and FPGA Implementation for Radar Target Recognition, May 30, 2018, 3:00 PM - 4:00 PM

This paper presents a 4-connect Connected Component Analysis algorithm and applies it to the problem of radar target detection. The algorithm takes a heuristic approach thus greatly simplifying the implementation while maintaining all positive features of recent CCA algorithms. The presented algorithm is single pass, does not require random access or look-ahead, requires no retrace period, contains no merge chaining, has low data requirements and hence low hardware requirements, has memory requirements that are not dependent on image size, requires only one clock cycle per element, performs feature extraction on-the-fly, has time consumption that is independent of image complexity, and is adaptable at run-time to different image or Range-Doppler map sizes. The algorithm is of similar capability to that of Zhao et al (2013) but simpler and with lower memory requirements.

The application of the algorithm to radar target recogition and feature extraction from range/doppler maps is presented, using both procedural and FPGA implementations.

Some salient features of the FPGA implementation are presented.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration
in the Indo-Pacific Region
28 – 30 MAY 2018

Wireless Cyber-Situational Awareness through Deep Learning: Traffic-Identification from the Physical Layer

Kreicers H[1,2], **Smith D[1]**, Seneviratne S[3], Seneviratne A[2]
[1]CSIRO Data61, [2]UNSW, [3]University of Sydney

Wireless Cyber-Situational Awareness through Deep Learning: Traffic-Identification from the Physical Layer,
May 30, 2018, 3:00 PM - 4:00 PM

Situational awareness, with timely monitoring and assessing of wireless threats, is vital for future defence and national security. One key to assessing such threats, is identifying wireless traffic and application usage. Here we address this using deep machine learning to resolve the application-source of unknown internet data frames from wireless physical layer information. Deep learning is achieved by applying a recurrent neural network, training on three parameters: inter-frame arrival-times, frame length and received-signal strengths of successive frames.

The technique is validated through accurately identifying particular service from five common internet-applications (Youtube, Netflix , Spotify, Facebook and Wikipedia) across a wireless connection. Features were recorded for two sessions of 100k frames from each service, and a sliding window of size 1024, with stride 50 was used to divide the frames into training samples. 30k unique frames were captured and divided in the same manner to form the validation set. The recurrent neural network, for traffic identification, has a long short-term memory (LSTM) layer followed by two fully connected layers. After 300 epochs of training, the training and test accuracies were 99.9% and 96.6% respectively. Testing the same model on 50k new samples collected one week later yields a validation accuracy of 94.0%. We postulate that, over wireless internet, different traffic-sources can be well identified due to varying multi-frame protocols. Finally, we propose training on a deeper network, further data capture and more parameters, such as modulation-type across frames and data rate.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

A Novel Cross-layer Approach to Antenna Beam-Steering for Wireless Cyber-Situational Awareness

Smith D[1], Abbott D[1], Seneviratne S[2], Seneviratne A[3], Johnson M[1], Kajan A[1], Ni W[1], Suzuki H[1], Wijenayake C[3], Chen Z[1], Hedley M[1], Burdeniuk A[4]

[1]CSIRO Data61, [2]University of Sydney, [3]UNSW, [4]DSTG

A Novel Cross-layer Approach to Antenna Beam-Steering for Wireless Cyber-Situational Awareness, May 30, 2018, 1:30 PM - 2:30 PM

Timely monitoring of wireless cyber threats will be critical to the success of future Defence operations. To enable such situational awareness this submission describes a novel experimentally-validated cross-layer method for beam-steering, which enables direct monitoring of IEEE 802.11 Wi-Fi signals at range using cyber signal features. Information from both the link-layer (i.e., MAC address, SSID) and physical (i.e., RSSI, azimuth angle-of-arrival) OSI layers is fused to provide direct monitoring capability.

The experimental system leveraged the open-source Wireshark network protocol analyser and low-cost COTS Wi-Fi hardware, integrated with a computer-controlled antenna beam-steered in azimuth. The antenna is successfully steered by interpreting from RSSI associated to each particular monitored Wi-Fi MAC address. For experimental validation in an outdoor environment: an angular resolution of +/-2.5 degrees for angle-of-arrival estimation was verified according to MAC addresses of clients and access points . Future work will include validation at greater stand-off distances and incorporation of other Wireshark-captured radio features for deeper cyber-situational awareness. In development, also, is a fully digital 8-element phased beamforming array for faster-response, real-time operations of this system.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
28 – 30 MAY 2018
Interoperability and Collaboration in the Indo-Pacific Region

A Digital Beamforming Array Proof-of-Concept for Situational Awareness Algorithms

Suzuki H[1], Abbott D[1], Johnson M[1], Smith D[1], Ni W[1], Hedley M[1]
[1]CSIRO Data61

A Digital Beamforming Array Proof-of-Concept for Situational Awareness Algorithms, May 30, 2018, 1:30 PM - 2:30 PM

Wireless situational awareness, vital to next-generation defence operations, is gained well from digital beamforming receive arrays, using smart algorithms, which allow: signal separation and identification from multiple radio sources in a multipath environment; identification of radio source characteristics, when a radio source cannot be demodulated or decoded, with an estimation of whether the radio source is a target-of-interest; and synthesis of a virtual aperture from beam-movement of the listening array enabling localisation of target-of-interest.

Recent advances in software defined radio have led to low cost products capable of implementing digital beamforming receive arrays. In this work, the building blocks for a digital array antenna are an Ettus Research USRP (Universal Software Radio Peripheral) X310 fitted with two TwinRX daughterboards.   This system is capable of performing four channel digital beamforming with 80 MHz bandwidth at a carrier frequency anywhere between 10 MHz and 6 GHz. Multiple array building blocks can also be combined to improve the accuracy of the algorithms with a larger numbers of receivers. Real-time algorithms can be implemented on the Xilinx Kintex 7 field programmable gate arrays (FPGA) included in the X310, or on high performance computer hardware connected via 10 Gbps Ethernet links.

In this presentation, we then demonstrate from experiment how such a single array building block enhances the detection and decoding of multiple IEEE 802.11 (WiFi) wireless packets, in the presence of higher power interferers.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Designing a Generic, Software-Defined Multimode Radar Simulator For FPGAs Using Simulink HDL Coder and SpeedGoat Real-Time Hardware

Reynolds S[1], Woolford T[1], Michael T[1]
[1]Simbiant Pty. Ltd.

Designing a Generic, Software-Defined Multimode Radar Simulator For FPGAs Using Simulink HDL Coder and SpeedGoat Real-Time Hardware, May 30, 2018, 3:00 PM - 4:00 PM

We present a method for designing and realising Software-Defined Radar systems using Industry Standard software tools and COTS hardware (e.g. MathWorks MATLAB\Simulink and Speedgoat Performance real-time target machines). We describe how we built a generic multimode surveillance radar system in software, and how to interface the system to external RF systems by leveraging Field Programmable Gate Arrays (FPGAs). Using these techniques, we are able to increase simulation fidelity while reducing time to build and test our models.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

EW&C in the Era of Data Science

Brittan P[1]
[1] L3 TRL

EW&C in the Era of Data Science, May 30, 2018, 10:25 AM - 10:45 AM

At the heart of modern EW&C systems is a beautifully simple paradox. Often the most effective and discreet EW&C techniques require the smallest of changes to a waveform or binary sequence, at just the right moment. However, these changes often reflect a deep understanding of protocols and real-time analysis; and, therein lies the paradox: how to detect, classify, and action a change, given the vast quantities of data generated by contemporary ESM and IL systems.
In this paper, we discuss the potential application of three Data Science techniques (compressive sensing, deep learning, and hypothesis refinement) to reduce the time between data acquisition and data exploitation, within the EW&C processing pipeline.

Evolution of Mission Data

Uzunov K[1], Priest T, Gluscevic V, Cutler P
[1]Department Of Defence, DSTG

Evolution of Mission Data, May 30, 2018, 9:45 AM - 10:45 AM

Mission Data is static in nature. Certain limitations in the MD process can be overcome by evolving Mission Data from the present almost static paradigm to a truly dynamic, network-enabled system.

A Case Study in Real-Time T&E Situational Awareness

Jackman R

A Case Study in Real-Time T&E Situational Awareness, May 30, 2018, 9:45 AM - 10:45 AM

Characterizing system capabilities across an intended operational condition and verifying that testable requirements are met is key when developing Test and Evaluation (T&E) strategies, especially if it is a new technical effort or a significant improvement in capability. When executing a formal T&E program, whether it occurs on the range or in the lab, time drives cost as the dominant risk factor, and unanticipated events in the electromagnetic spectrum could severely corrupt the collection of data – for example incorrect signal levels, over ranged instrumentation, or systems under test that don’t behave as planned under a specific signal condition. The cost in time and money for a failed T&E event can be very high.

This case study examines how COTS equipment can be used to acquire up to 800MHz of instantaneous bandwidth of electromagnetic spectrum in real-time and transfer the data seamlessly to a recording device such as a disk array while simultaneously giving an operator the unique advantage of observing the complete spectrum whole still being in the real time transfer mode. This paper will examine a new and novel architecture for an acquisition system that solves many challenges regarding live recording and monitoring during the range test and evaluation phase of a program.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Antenna Simulation for EW Applications

Shar R

Antenna Simulation for EW Applications, May 30, 2018, 1:30 PM - 2:30 PM

This tutorial covers using off-the-shelf Antenna simulation software tools to evaluate a range of electronic warfare performance aspects and techniques

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
28 – 30 MAY 2018
Interoperability and Collaboration
in the Indo-Pacific Region

Cognitive Electromagnetic Battle Management

Hampson M, Kilfoyle D, Knight M

Cognitive Electromagnetic Battle Management, May 30, 2018, 9:45 AM - 10:45 AM

The growing agility and unpredictability of near peer RF threats demands an ability to learn new behaviors for tools across the electromagnetic spectrum warfare domain; not just jammers. In particular, battle management tools, both pre-mission and in-mission, will need to account for the fundamental uncertainties in future fights. This could be called cognitive battle management.

Key considerations include ensuring robust courses of action with effectiveness that degrades gracefully in the face of unanticipated threats, an ability to incorporate and use knowledge from each successive mission, a methodology to manage ad hoc teams and decision aids that support supervised learning that melds humans and machines in decisions. All of this will need to be supported by an open and modular distributed architecture in contrast to the point solutions of today.

The benefits and challenges associated with a new generation of cognitive battle management will be discussed

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018

Electromagnetic Maneuver Warfare and Broadband Solutions

Andrews G, Marr B

Electromagnetic Maneuver Warfare and Broadband Solutions, May 30, 2018, 9:45 AM - 10:45 AM

Electromagnetic Maneuver Warfare and Broadband Solutions As commercial and military devices proliferate throughout the radio frequency (RF) spectrum, electromagnetic maneuver warfare (EMW) becomes a critical strategy. RF is becoming more multifunction where a single device can prosecute multiple missions and functions. In addition, electronic warfare systems are becoming adaptive and more agile. Further, as these RF systems continue to move up into higher frequencies, RF bandwidths are becoming orders of magnitudes wider than in the past, all leading to great increase in spectrum use.
The next generation of RF system must be adaptive, agile, and ultra broadband to address these emerging needs and provide Electromagnetic Spectrum (EMS) Awareness. This talk will discuss how broadband RF drives increasing spectrum access and digital data processing and will require novel broadband system on a chip solutions. Spectral efficient technologies and reconfigurable RF Transceiver technologies will also be discussed to address the EMW mission.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC
2018
CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration
in the Indo-Pacific Region
28 – 30 MAY 2018

IMD CHALLENGES FROM A REPROGRAMMER’S PERSPECTIVE

Dundas A

IMD Challenges from a Reprogrammer’s Perspective, May 30, 2018, 9:45 AM - 10:45 AM

The Australian Defence Organisation (ADO) is currently grappling with the challenge of how to satisfy a growing appetite for Intelligence Mission Data (IMD) from the Electronic Warfare (EW) Operational Support (EWOS) reprogramming community. Traditionally, the EWOS community has had little influence over the IMD producers and has effectively had to “make do” with whatever IMD was available.

Several key factors are driving a change to this relationship in the ADO including increasing threat complexity and agility as well as the needs of fifth generation platforms for the ADO. This paper examines a number of the key challenges for the IMD producers including the R&D community to meet the current and emerging IMD needs of the EWOS community.

AUSTRALIAN CHAPTER OF THE ASSOCIATION OF OLD CROWS
AOC 2018 CONVENTION
ADELAIDE CONVENTION CENTRE
ADELAIDE, SOUTH AUSTRALIA
Interoperability and Collaboration in the Indo-Pacific Region
28 – 30 MAY 2018