ISR Platforms and the Future of C4ISR[1] Systems Integration in the Gulf

Ralph D. Thiele

May 2014

Summary

The Gulf states have set ambitious targets for commercial growth that include the development of local businesses and foreign direct investment, as well as developing national-champion enterprises. Yet, within their long-term vision, security and defence capabilities need to have a particular place. An effective C4ISR system would help to prevent hostilities, to shape the security environment, protect critical infrastructure, borders and coastlines and would also contribute to military success.

Arabic League civil entities and GCC militaries are urgently looking at ways to integrate COTS and legacy communications, situational awareness and networked systems into an overarching system. The key question of today is what it needs to strengthen existing capabilities beyond what it has already achieved. Particularly airborne ISR systems have provided a critical edge in the conduct of security and military operations. Thus an "*airborne-centric*" ISR architecture has evolved, with a broad spectrum of capable ISR platforms – fast jets, rotary-wing assets, unmanned aerial vehicles and increasingly special mission variants of civil aircraft.

Beyond the platforms big data has become an issue: where does it come from, where to put it, and how to use it quickly and decisively. Another issue has become connectivity as it lies at the core of decision superiority. While technology is a major component, involved personnel need to be trained. A "*GCC Network Enabled Capability for Regional Training and Exercises*" could promote effective risk and crisis management through a Simulation Network linking the GCC Joint Command with member states. Such a network could

- Link the Gulf Cooperation Council (GCC) Joint Command to member state national command centres, etc.
- Focus on new and expanded security missions, including Humanitarian Assistance and Disaster Response (HA/DR) using "best of Web" technology to enable participation by leading institutions and individuals

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/defense. ISPSW network experts have worked – in some cases for decades – in executive positions and possess a wide range of experience in their respective specialist areas.

[1] Command, control, communications, computers, intelligence, surveillance, and reconnaissance

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

ANALYSIS

1. Strengthening existing capabilities

While the global redistribution of military and financial/economic power is continuing, the Middle East region clearly remains in a state of flux. The Gulf is a prosperous region. Its states have set ambitious targets for commercial growth that include the development of local businesses and foreign direct investment, as well as developing national-champion enterprises.[2] Yet, within their long-term vision, security and defence capabilities need to have a particular place. The territorial dispute with Iran, the threat of terrorism and the on-going state-building initiatives in the Gulf has been driving recent strategies. The Gulf States need to protect their critical infrastructure such as oil and gas facilities as they aim to diversify their economy and become more self-sufficient. To this end they are not only globally significant defence importers.[3] They have also been developing their own defence-industrial base through collaboration with leading original equipment manufacturers.

In the past decades, the Arab region has faced plenty of crises. These have led to the deaths of more than 100,000 people. There has been on-going instability among different political parties and religious sects. In the cyber domain malicious users and hackers have been attempting to take advantage of vulnerabilities to either profit or to land a blow to politicians. These and further challenges require readiness to deal with all phases of emergencies and ensure their competent management and full recovery. Thus in February 2014, when Dr Nabil Elaraby, the secretary general of the Arab League, addressed in Abu Dhabi the issue of "*The Future of Collective Arab Action*"[4], he asked member nations to develop common policies to deal with economic, political, social and security problems, as the region was facing challenges that affected its security and needed to be addressed through cooperation. He particularly mentioned that Arab countries have been surrounded by technologically advanced countries such as Turkey, Israel and Iran – countries with ambitions.

Consequently, Arabic League civil entities and GCC militaries are urgently looking at ways to integrate COTS and legacy communications, situational awareness and networked systems into an overarching system. Arab states have started working on a regional emergency network[5] to coordinate their response to crises ranging from political upheaval to armed revolt and natural disasters to pandemics.[6] A number of initiatives and awareness programmes have been taken by all of the regional nations, including general public security conferences, new security projects to increase protection and cyber monitoring. The Arab League has set up an early intervention centre to strengthen the capabilities of countries to manage risks and emergencies. The second phase of the project now foresees a network for all Arab countries to communicate in a crisis, a network to

[2] Abu Dhabi Council for Economic Development, 'The Abu Dhabi Economic Vision 2030', http://www.adced.ae/en/EconomicVision/
[3] The United Arab Emirates for example are the fourth-largest defence importer globally and are expected to spend about $52.3 billion on defence and security equipment in tthe next four years. *UPI*, 'Emirates Builds its Own Defense Industry', 18 March 2013, http://www.upi.com/Business_News/Security-Industry/2013/03/18/Emirates-builds-its-own-defense-industry/UPI-77731363633569/
[4] Caline Malek, The National, February 27, 2014 , page 4 http://www.thenational.ae/uae/gcc-agrees-to-closer-disaster-cooperation
[5] Anwar Ahmad The National, February 27, 2014, page 4
[6] Caline Malek, The National, February 26, 2014 , page 1 http://www.thenational.ae/thenationalconversation/editorial/arab-crisis-network-should-start-now

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

pool efforts and to ensure swift political response and action. Furthermore, a variety of multibillion-dollar infrastructure security projects are in development across the region. Many have C4ISR at their core.

Particularly on the military side the Gulf States have developed their respective defensive capabilities while at the same time strengthening their bilateral relationships. This process started in 1987, when the Gulf Cooperation Council (GCC) countries approved a comprehensive security strategy, in the form of a general framework for organizing cooperation to support mutual security covering cooperation in multiple aspects of defence and security. At that time the primary concerns were issues such as illicit trafficking, dealing with threat-based organizations, immigration, passports, airport security, drug fighting, weapons, explosives, border and coastal security and civil defence.

The increasing construction of regional security architecture in the Gulf started with the peninsula shield force. In December 2000 the member states agreed to a joint defence agreement based on the principle that any aggression against a member state would be considered as aggression against all the GCC states. The agreement obliges all the six states to provide mutual military assistance. It further established a Joint Military Committee to supervise cooperation and promote collaboration in joint military exercises and coordination in the field of military industries.

In 2006, Saudi Arabia circulated a proposal during the GCC summit meeting in Riyadh that called for the adoption of centralized command and decentralized forces. The kingdom proposed that each GCC state should designate certain military units to be part of the new structure and to station those units within each state's national territory. The units would then be linked to a unified central command. However, what emerged was the 2009 agreement to create a joint force for quick intervention to address security threats, as was demonstrated in the UAE-Saudi intervention in Bahrain in 2011.[7]

At the 2013 C4ISR Summit in Abu Dhabi, the GCC secretary general, Dr Abdullatif Al Zayani, told the summit that the GCC was politically in unison and called for the countries' militaries to follow suit: *"GCC countries have to be able to be integrated and interoperable to share intelligence and information and be ready to work together at a higher and more complete level*". Then in December 2013 Leaders of the GCC announced the formation of a unified military command for the GCC countries.

The council also announced the establishment of the Gulf Academy for Strategic and Security Studies in the United Arab Emirates. The academy aims to bolster military cooperation through a unified education based institution. The academy will look to increase knowledge transfer and greater comprehend a unified realization of threats across the entire GCC region. Its initial focus is to include missile defence, border security and counter terrorism. The key question of today is what it needs to strengthen existing capabilities beyond what it has already achieved. To this end the annual C4ISR Summit[8] in Abu Dhabi has become an agenda-setting event in the Gulf.

[7] Mustafa, Awad, Defense News, Dec. 11, 2013, GCC Announces a Joint Military Command, http://www.defensenews.com/article/20131211/DEFREG04/312110011/GCC-Announces-Joint-Military-Command
[8] http://www.c4isrsummit.com

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

2. Developing a C4ISR core

Today and tomorrow security operations including warfare will be conducted at longer ranges and with greater precision than ever before. Overall mission effectiveness increasingly depends upon systems and services external to a weapon system – C4ISR systems and services. C4ISR also has become a critical link of the global commons – maritime, air, outer space, and cyber space of course land. Exactly these links have been increasingly challenged by nations such as Iran or China, who have developed Anti Access and Aerial Denial strategies that consequently have become of particular concern to security and prosperity in the Gulf region and beyond.

In the Clausewitzian sense, „*frictions*" as well as the „*fog of war*" hamper decision makers to come timely to adequate decisions. C4ISR facilitates time sensitive decision-making. It allows to make informed decisions faster and also to translate these decisions precisely and rapidly into action. For the military, maximizing situational awareness and informational superiority via C4ISR translates not only into an operational advantage on the battlefield, but rather an advantage in all domains and global commons.

A plenitude of issues have been addressed in the C4ISR context, including service oriented architectures and interoperability, vulnerabilities and consequences, contingency operations and their organization, sensor-to-shooter challenges and time critical targeting, tracking & measurement association, airborne and space platforms i.e. unmanned aerial systems, sensors and sensor fusion, visualization and modelling & simulation, precision targeting & target location, the global information grid and satellite communications, tactical data and information links, etc. and last but not least cyber.

The complexity of building viable C4ISR processes and structures becomes obvious alone by the quantity of structural elements and processes supporting C4ISR capabilities, among those

- Sensor systems to include Radar, Electro-Optical (EO)/Infrared (IR), Electronic Support measures, Laser radar and Maritime Domain Awareness
- Command and Control (C2) Systems supporting the observe-orient-decide-act loop, Ground forces C2, Naval C2 Platforms, Air C2 Platforms, Network Enabled Operations Capabilities
- Communication systems to include radio frequency, optical and satellite communications
- Intelligence, surveillance and reconnaissance supporting processes and collection platforms
- Electronic Warfare capabilities to include electronic countermeasures and Counter-Countermeasures, support measures, IR countermeasures, lethal and non-lethal techniques
- Cyber Operations to include information operations and assurance
- Unmanned Systems to include unmanned aerial vehicles (UAV), unmanned Combat Aerial Vehicles, unmanned Surface Vehicles, unmanned Underwater Vehicles and unmanned Ground Vehicles
- Sophisticated Exercise, Training & Simulation environments to prepare individuals, operational units and staffs for their challenging missions

Command & control has been and will continue to remain a predominantly human activity. Yet, with the permanent on-going revolution in military affairs and the enormous growth of capabilities along with accelerating technological innovation cycles, technical systems, processes, and collaboration tools have

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

increasingly supported command. Effective exploitation of "*C4*" and "*ISR*" generates quality information to enhance human capacities in order to process information and make decisions. This is done through the fusion and sense-making of intelligence and information into actionable knowledge, followed by rapid dissemination to support the decision-making and actions of commanders and operational users. Consequently, C4ISR is fundamentally about sensing and sense making of the battle-space and the operating environment. The effective exploitation allows civilian as military security actors to operate as a comprehensive, integrated force because vast amounts of information can be stored, processed and then disseminated to multiple users in a short span of time.

Today big data analytics enable to automatically detect and report anomalies in all domains – land, sea, air, space, cyber space. Consequently potential incidents in airborne or maritime traffic may be discovered much earlier than ever before. Big data analytics help identify anomalies early and thus gain precious time to take counter-action. The significant increase in the detection rate compared to manual processing enables high performance. Naturally, it allows to focus expert time on qualifying alerts rather than on mass data inspection. Complex event prediction is another example how to utilize big data. Combining data analytics with the effectiveness of human experience and the efficiency of automatic data processing from different sensors or sources at any data rate provides for leveraging expert knowledge captured in the system at any scale required.

At the 2014 C4ISR summit in Abu Dhabi Brigadier General (ret) Robert Wynn, former Commanding General Information Systems Engineering Command, stated that an effective C4ISR system would help to prevent hostilities, to shape the security environment and would also contribute to military success. To be effective it would need modern, sufficient spectrum capacity, mature software, skilled, trained personnel and an incremental deployment plan. This is a brief but excellent description of why C4ISR is important to the Gulf region and what needs to be done.

3. Afghanistan, Iraq, and Libya Lessons and ISR platforms

Over the past decade the demands of the wars in Afghanistan, Iraq and Libya have globally shaped the development of C4ISR, i.e. a trend towards increased operational access, persistence, flexibility, and information sharing. Today, the C4ISR concept is delivering.

Particularly airborne ISR systems have provided a critical edge in the conduct of military or security operations. Thus an "*airborne-centric*" ISR architecture has evolved.[9] These have become the guiding principles:

- Increasingly unmanned
- Every platform is a sensor
- Every sensor is networked
- Data is discoverable & accessible by all
- Modular, scalable plug & play sensor payloads
- Common Control Stations
- Common interfaces, data formats & standards

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

On the world market the momentum is in the development of airborne sensor systems characterized by the demand for increased information retrieval and improved situational awareness while at the same time providing for reduced costs and easier usability. Airborne platforms have the potential to support a wide range of tasks – economic and governmental, civilian, police and military tasks across both the public and private security sector: civil protection, protection of major events, border security , critical infrastructure protection and counter-terrorism, etc. The industry is challenged to develop critical expertise, services and technology in the short term.

Successful ISR efforts over Afghanistan, Iraq and Libya have created expectations that ISR will be able to tell what is going on over the hill or on the battlefield. However, it should be noted that whenever control of the air, space, and cyberspace is contested, that proposition becomes far more complex. Yet, the growing reliance on airborne intelligence gathering has spurred the proliferation of specialised airborne platforms to support Intelligence, Surveillance and Reconnaissance (ISR) missions.

At the high end of the airborne ISR, armed forces use fast jet assets in a Non-Traditional Intelligence, Surveillance and Reconnaissance role. At the 2014 C4ISR Summit Lieutenant Colonel Nicolas Lyautey addressed lessons learnt from respective ISR Operations during the Libyan Conflict to include lessons from Afghanistan and Iraq with view to the "*ISR Capabilities of the Rafale*". He pointed out the significant role of fighter aircraft in terms of ISR particularly during the initial engagement phase, when air supremacy is not guaranteed. Fighter aircraft usually arrive first over the area of interest. They start the ISR process and provide orientation to subsequent missions of assets like UAVs. Optronic sensors have become a heart of the weapon system. Cross cueing between ISR assets such as Fighter Aircraft & UAV and Non Traditional ISR sensors has become critical to mission success in modern, combined, joint, network centric and asymmetric warfare. The competitive advantage of fighter aircraft is

- Quick reaction capability
- In non permissive environment
- High Speed
- Sensor to shooter capability
- Day and night capability

Naturally, LTC Lyautey still sees growth potential. Recent operations have highlighted that it is important to speed up the loop of the air planning process, to adapt to the versatility of modern threat, to include

- Real time planning
- Automatic analysis
- Data links and Satcom
- On board analysis.

Among the other jets that have demonstrated their mission effectiveness in Afghanistan is the RAF Tornado. The high-resolution motion-free images gathered by the Goodrich Reconnaissance Airborne Pod for Tornado have proved to be a particular valuable asset in Counter-Improvised Explosive Devices operations. Using the L-3

[9] *Schanz*, *Marc V.*, *ISR after Afghanistan*,
http://www.airforcemag.com/MagazineArchive/Pages/2013/January%202013/0113ISR.aspx

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Communications' Remotely Operated Video Enhanced Receiver system, Joint Tactical Attack Controllers on the ground can see the imagery from the Tornado's Litening III pod on a laptop. F-15E Strike Eagle and F-16C/D combat aircraft regularly use their AN/AAQ-33 Sniper pods to scan tracks for signs of Improvised Explosive Device emplacements or to support troops in contact.

Also rotary-wing assets have become important elements in ISR. The United States Marine Corps attack helicopters and Canadian Bell CH-146 Griffon medium-lift utility helicopters have been fitted with ISTAR sensor packages for operations in Afghanistan. The UK Joint Helicopter Command in Afghanistan has developed ISTAR capabilities for all its deployed helicopters. In addition, other Combat helicopters to include the AH Mk.1, AH-64D Apache gunships the A-129 Mangusta A/C/D, the EC-665 Tiger HAP, and Bell AH-1W Super Cobra have been employed with advanced mission systems in the ISR role.

Unmanned Aerial Vehicles (UAV) certainly have become particular valuable platforms in ISR as they have been providing

- Battlefield intelligence
- Attack capability for high-risk missions
- Platforms for research and development
- Platforms for civil and commercial applications

In recent military operations the use of UAVs has been firmly established. Technological progress enables significant extensions of previous uses. Modern wars have been decided for more than half a century in particular by weapons fire from airborne platforms – since roughly two decades increasingly in form of precision fire. UAV have become already a core element of this development. Under the generic term "Remote-Controlled Weapons Systems" they have been referred to in the study "Enabling the Future" by the European Union Institute for Security Studies as one of three key areas of an emerging revolution in military affairs next to "Counter-Intervention Systems" and "Directed -Energy Weaponry". The study has been pointing out that remote systems could already dominate the armed forces of major world powers by the year 2025.

Unmanned Aerial Vehicles are the fastest growing segment of the military aerospace market and their sensors and payloads form the key elements of UAV systems. A wide range of UAV payloads, including EO/IR Sensors, Synthetic Aperture Radars (SAR's), SIGINT and EW Systems, C4I Systems and CBRN Sensors, worth $3 billion per year currently, is forecast to increase to $5.6 billion annually by 2020. This military- technological trend is complemented by the desire for civilian use of unmanned aerial systems and their integration into civilian aviation and extended – even for police forces, fire and rescue, environmental protection, nature conservation and agriculture and many purposes in the private sector.

Among the well-proven UAV in recent operational environments have been

- RQ-11 Raven
  A small man-portable UAS that performs reconnaissance, surveillance, and target acquisition missions. The Raven includes a colour electro-optical camera and an infrared camera for night operations. The air vehicle is hand-launched, has a range of 10-15 kilometres and an endurance of up to 80 minutes.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Shadow 200
  A small, lightweight, tactical UAV system. The system is comprised of air vehicles, modular mission payloads, ground control stations, launch and recovery equipment. It has an endurance of up to four hours, at 50 kilometres from the launch and recovery site.
- MQ-1 Predator
  A medium-altitude, long-endurance UAV system. It is equipped with a colour nose camera, a day variable-aperture TV camera, a variable-aperture infrared camera for low light/night, and other sensors as the mission requires. The cameras produce full-motion video.
- RQ-4 Global Hawk
  A high-altitude, long-endurance unmanned UAV system with an integrated sensor suite that provides in peacetime, contingency and wartime operations for intelligence, surveillance and reconnaissance with global reach.

Of course many more could be mentioned – the spectrum and respective capabilities keep growing and growing.

A particular interesting development among the ISR platforms have become special mission variants of civil aircraft. Modern concepts of operations include a comprehensive payload of optronic sensors, which can be in a belly pod or a turret plus a state-of-the-art defensive aid suite and signals intelligence and communications intelligence packages. In the market sector of special mission aircraft the Gulf region is among the fastest growing worldwide[10]. With neighbours like Iran and Yemen and the Arabian Gulf as the principal sea line of communication for much of their trade, the region's interest in special missions and maritime surveillance capabilities has grown significantly. Naturally, this interest has been spurred by the capabilities of some of these systems to sense deep into neighbours' territory without crossing foreign borders.

Business jets and turboprops, from small, twin-engine platform suppliers like the Diamond DA42 up to Boeing's 737-based P-8A maritime patrol aircraft have evolved to become valuable assets. Among the business jets, the USAF's E-11A and the RAF's Sentinel R1 are both based on the Bombardier Global Express, while the USAF C-37A is a modified Gulfstream G550 aircraft. Variants of the Hawker Beechcraft King Air are the ISR platform of choice for many air forces. Boeing has agreed with Bombardier and Field Aviation to launch a maritime surveillance machine based on the Challenger 605. Equipped with a Selex ES Seaspray radar and FLIR Systems electro-optical and infrared imaging system and other sensors, the new platform is supposed to cost only roughly a third of the price of a P-8A. Saab has been offering a maritime surveillance aircraft equipped with a Telephonics surveillance radar, a retractable FLIR System EO/IR turret at a cost of approx. $20 million – a tenth of the price of a fully equipped maritime patrol aircraft.

In the past years there has developed a growing trend towards optionally-manned/unmanned applications with optionally-manned/unmanned ISR variants such as Piaggio Aero Industries' Avanti II and its newest unmanned twin the HammerHead, TECNAM's P2006T and Diamond Aircraft Industries DA42.

[10] C4ISR & Networks, Nov 24, 2013, Interest in Special Mission Aircraft High Among Gulf States, http://c4isrnet.com/article/M5/20131124/DEFREG04/311240003/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The HammerHead[11] is a new, state-of-the-art Unmanned Aerial Vehicle system designed for Intelligence, Surveillance and Reconnaissance (ISR) missions. It is derived from the successful Piaggio Aero P.180 Avanti II business aviation aircraft, and designed to fulfil a wide range of military and civil ISR and security applications, with specifically identified roles that include aerial, land, coastal, maritime and off-shore security surveillance together with communication and electronic intelligence collection and electronic warfare missions. The aircraft's mission suite builds on the Selex ES's skyISTAR architecture with a wide menu of sensor types to choose from including radar, electro-optical, hyper spectral, COMINT and ELINT equipment. Data fusion and management are further features.

After TECNAM's launch of the P2006T serial production in 2009 the Austrian Airborne Technologies has been developing the efficient multi-fuel twin-engine aircraft to a smart and efficient special mission aircraft. The TECNAM MMA[12] comes with a complete surveillance configuration to include Wescam MX-10 and BMS downlink system, a multifuel capability and very low operating costs. It focuses on fully customized special missions for example for pipeline surveillance at the Emirates and other Middle East countries.

The DA-42 Twin Star – a four-seat twin diesel-engine aircraft of composite construction – has been adopted by several air forces as an ISR aircraft while unmanned and optionally-manned variants have been developed to take full advantage of its 24-hour endurance. In its configuration as DA42 Multi-Purpose Platform[13] it is able to carry a gyro-stabilized daylight and thermal video camera, laser scanner and digital aerial cameras. A micro-wave up- and downlink system for high quality transfers with a range of more than 100 nm and beyond-line-of-sight satellite downlink. The DA 42 was first used by UK armed forces in Iraq when DO Systems Ltd of the United Kingdom leased three aircraft to the RAF. They accumulated in theatre some 2,000 hours of full-motion television surveillance captured using a FLIR Systems STAR Safire III HD optronic payload. It has also been employed to support Police operations in complex environments, anti-piracy operations in open waters and to protect critical infrastructure.

4. C4ISR beyond the platforms

The ISR mission is evolving rapidly. ISR capabilities need to function in a range of scenarios – from the permissive environment of Afghanistan to countries sheltered behind formidable anti-access, area-denial systems. Reflecting on the lessons learnt from Afghanistan operations, armed forces[14] have started adapting their C4ISR networks to an ever-altering security environment. To this end they have started centring their focus increasingly on data, in fact very often on "*big data*": where does it come from, where to put it, and how to use it quickly and decisively.

The issue of *"big data"* has been mentioned before. The private sector has been quick to engage with big data because of the monetary benefits on offer. Compared to the private sector, governments up to now have been largely slow to engage with big data. There is of course an undeniable need for them to catch up.

[11] http://p1hh.piaggioaero.com
[12] http://www.tecnam.com/Multimission/MMA.aspx
[13] http://www.diamond-sensing.com/index.php?id=da42mppguardian
[14] http://www.airforcemag.com/MagazineArchive/Pages/2013/January%202013/0113ISR.aspx

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Big data is concerned with the accumulation, tagging, storage and subsequent manipulation of large data sets. The precise definition varies, as what was considered a large dataset 5 years ago is today fairly standard. Consequently, large data can consist of anything from 10-100 Terabytes and up into the Petabytes. Naturally, armed forces as well as governments have a wealth of current and historical data often in the upper reaches of that scale, much of which is in urgent need of being accessed and analysed. A key problem is that time is of the essence. The longer it takes to establish a system, a software, a methodology, or a mindset, the larger the gap grows between the demand for data storage, evaluation and dissemination and the ability organisations have to manage its increasing magnitude.

One of the areas where governments have been catching up is geospatial information which is gaining in importance with view to practical all military and non-military security operations. At the C4ISR Summit Vesna Milinkovic from the London Metropolitan Police Service showed how effective and efficient use of geospatial information, open standard GI technologies, GI services and coupled with adequate user training would provide for

- Reducing the crime rate by 20%,
- Cutting costs by 20% and
- Increasing public confidence by 20%.

Mathew Wardle from the UK Met Office described the enormous benefits of successfully handling big data and delivering meteorological and oceanographic web services for consumption by Defence and Security Users of geographic information systems for all kind of contingencies and almost anywhere in the world – to include dust developments in Abu Dhabi.

Of course, the importance of providing a broad GIS data base has long been recognized in the Gulf region. Brigadier General Eng. Awni Mohd Kasawneh from the Royal Jordanian Geographic Centre highlighted how successfully integrating military and internal security forces' Geospatial Intelligence Programs enabled to come up with a broad scope of maps and data his centre keeps providing to the Jordanian government, its institutions to include the military as well as the intelligence community and the Jordanian people. Another example comes from Bahrain where Eng. Khalid A. Hammadi from the Bahrain Central Informatics Organisation outlined the deliveries of his organisation in order to maintain and administrate a National Geospatial Database and layers such as street centerlines, addresses, electricity & water transmission and distribution, telecommunications, Gas & Oil pipelines, sewerage & drainage, and the Satellite Image of Bahrain; all of these geospatial layers being consumed and disseminated through the Bahrain Spatial Data Infrastructure (BSDI) Portal.

Data, information and knowledge gained need to processed, exploited, and disseminated.[15] In Afghanistan, enormous amounts of ISR needed to be provided to ground combatants and decision makers to fill the demand for full-motion video and information from all sources – signals, imagery, geo mapping, and others. Data management and movement are particular vital to operations where control of air, sea, space and cyber space is contested. Thus fusion, storage, and use of this torrent of data have become a larger problem.

Information requires human eyes to sift through it. As Dan London, VP Sales, Marketing and Customer Support at BAE Systems, pointed out in his presentation at the 2014 C4ISR summit, referencing statistics show that

[15] http://www.airforcemag.com/MagazineArchive/Pages/2013/January%202013/0113ISR.aspx

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

analysts spend up to 50 per cent of their time alone locating the data required for their tasks. Consequently, machines and artificial intelligence tools have to help analysts and decision makers to get control of all this information. Commanders, analysts, and others need to have access to a fused product of cyber and human intelligence as well as other data from across the network, as opposed to having eyeballs watching a video. Additionally, unconventional and open source assets need to be fed into the evaluation. Also space and cyber operations need to be integrated.

Clearly, concepts have to be developed how this would operate in a more access-challenged situation. Where ISR is created, where it is stored, how to decide what to move, and when and where to put easy-access information have become critical questions. Connectivity lies at the core of decision superiority. The point lies in networking this capability and building command and control that effectively brings that information together. This is why collaboration plays such a vital role in ISR architecture. This is particularly true vis-a-vis allies and partners as the ability to leverage the ISR data that allies collect and share will prove valuable.

In between a couple of solutions have entered the market. Accenture – among the global market leaders in providing management consulting – for example has offered design, development and integration of complex C4ISR defense systems to include Maritime Domain Awareness and Coalition Data Sharing. It supports several C4ISR services, i.e. satellite communications, optimization of supply chains or solutions delivering multilevel security and critical information from multiple data sources. An all-source intelligence and target tracking system delivers near real-time „red force" tracking, i.e. information on foreign force activities and potential terrorist threats on and around the world's oceans.[16] Users may view only those aspects of the records or tracks they are authorized to see. Record labeling, combined with mandatory and discretionary access control technologies, ensures data is never improperly released. Worldwide mobile training teams provide customized instruction to each site, ensuring that users get maximum value from the platform.

At present particularly the Afghan Mission Network provides for a best practice example of a highly effective collaboration environment. With the Afghan Mission Network for the first time in NATO history a common C4ISR network has been established – in this case for all ISAF forces and operations consisting of the ISAF-Secret network as the core with national extensions. The Afghan Mission Network will soon evolve into NATO's Federated Mission Network which will enable in future a NATO Common Operational Picture (NCOP) to provide NATO commanders and operational staffs with essential and reliable information that enables their understanding of comprehensive security environments in order to significantly improving situational awareness and rapid decision-making.

5. Conclusion and recommendation

Gulf States have been striving for a deeper understanding of the operational principles and underlying technologies of modern C4ISR systems with a particular focus on the complex linkages between technology, people, process, tools, business benefit and balance of investment decisions. In the past years they have learned, that making significant investment in relevant S&T can lead to more effective defence systems.

[16] http://www.accenture.com/cn-en/Pages/success-us-space-naval-warfare-center-joint-cross-domain-exchange.aspx

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The Gulf region is globally one of the fastest growing markets for C4ISR capabilities.[17] Among the most wanted features are intelligence support outsourcing, communications, command and control (C2), geospatial, optical and radar sensors, airborne and space-based surveillance. Virtually every nation is looking to UAVs to provide or supplement their airborne ISR capabilities. Saudi Arabia and the United Arab Emirates are among the worldwide top 20 markets for C4ISR platforms. For example, Saudi Arabia has been equipped impressively with Boeing E-3A, RC-135, Erieye on Saab 340, Bombardier Q300 MPA and others. The Kingdom has been spending a lot of money on ISR aircraft for internal needs, including upgrades to their aging E-3 Tactical Airborne Surveillance System platforms, as well as participating in a multi-nation Long-Term AEW&C Solution Aircraft effort. The core C4ISR platform of the United Arab Emirates has been the Saab S100B.

Governments in the Gulf invest in solutions for ballistic missile defence, airborne ISR sensors and mission equipment packages. Instability in threats drives funding of sensors, and networks that enable sharing of ISR information and exercise of C2. Counter-terrorism requires identification and tracking of threats down to the individual level and communication of information down to the smallest unit. Sovereignty over ocean economic resources requires deployment of sensor platforms and communications networks.

With regard to building an effective C4ISR environment in the Gulf region, it would be important to come up with a valid strategy addressing both individual country needs and regional security concerns. Of particular importance for the Gulf will be to design the architecture and processes of a coherent, interoperable C4ISR system with the capability of fusing human and technical domains, standards and procedures as well as training and education. To this end data, information and knowledge dissemination and sharing between the partners operating needs to be ensured. A successful program requires a tightly knit partnership in which knowledge, material and risk are managed across all stakeholders. As there is a tendency that the planned lifespan of programs has increased, new and existing products need to be supported for years to come.

An important step to start the process would be an in-depth analysis of current gaps in C4ISR faced by countries in the GCC and an overview of the potential solutions being considered. Then a roadmap needs to be developed focusing on end-to-end C4ISR capabilities, from sensor to decision maker to effectors, to be supported with training and exercise simulation capabilities. This roadmap should include a broader C4ISR acquisition and application strategy in line with the dynamic changes occurring in the region and, of course, cyber security. The roadmap should specifically address joint and coalition requirements for air surveillance and reconnaissance including unmanned aerial systems and the integration of existing and planned air and missile defence systems.

At the 2013 C4ISR Summit Brigadier Alan Hill, head of information superiority at the British Army, highlighted that ensuring the acquisition and appropriate application of C4ISR capabilities and assets would guarantee informational superiority in a battle space. Yet, he also stressed the importance of training individuals who collect and use sensitive information due to its crucial nature. *"The technology is a major component but, at the human level, personnel have to be trained on how to handle the information as risks may occur from many sources."*[18] Following this suggestion at the 2014 C4ISR Summit Walter Christman, Chairman Global Challenges

[17] In a December 2012 "Global C4ISR Market Assessment" Frost & Sullivan estimates the C4ISR market with a trillion dollars over the next 10 years
[18] Mustafa, Awad, „Experts at Abu Dhabi summit want GCC military integration", in: The National, 17 April 2013, http://www.thenational.ae/news/uae-news/experts-at-abu-dhabi-summit-want-gcc-military-integration#ixzz2Ry7UlwDW (accessed 3 February 2014).

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Forum Foundation suggested to build a "*GCC Network Enabled Capability for Regional Training and Exercises*" to promote effective risk and crisis management through a Simulation Network linking the GCC Joint Command with member states.

Such a network could

- Link the Gulf Cooperation Council (GCC) Joint Command to member state national command centres, etc.
- Focus on new and expanded security missions, including Humanitarian Assistance and Disaster Response (HA/DR) using "best of Web" technology to enable participation by leading institutions and individuals
- Take advantage of an explosion of next generation training tools and designed to evolve as technology changes, primarily through scenario-based thinking that ties together and integrates diplomacy, defence and security, as well development and humanitarian threads for holistic national security solutions.

Introducing a training & simulation network as primary tools of regional integration is certainly a valid and thrilling concept. It could provide a variety of distributed simulation coalition exercises to ensure early and adequate training to maximize the efficiency and use of a Gulf C4ISR system as it develops in response to real world challenges.

***

Remarks:

Opinions expressed in this contribution are those of the author.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StatByrd Consulting. In 40 years of politico-military service, Colonel (ret.) Thiele has gained broad political, technological, academic and military expertise. He has been directly involved in numerous national and NATO strategic issues while serving as executive officer to the Bundeswehr Vice Chief of Defence Staff, Military Assistant to the Supreme Allied Commander Europe, in the Planning and Policy Staff of the German Minister of Defence, as Chief of Staff of the NATO Defense College, as Commander of the Bundeswehr Transformation Centre and as Director of Faculty at the German General Staff and Command College in Hamburg.

He has published numerous books and articles and is lecturing widely in Europe, Asia (Beijing, Seoul, Tokyo, and Ulaanbaatar) in the U.S. and Brazil on current comprehensive security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and defence and also historical issues.

Ralph D. Thiele is a member of the German Atlantic Association and member of the Defence Science Board to the Austrian Minister of Defence.

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de