Building C4ISR Capabilities in and for the Gulf

Ralph D. Thiele

May 2013

Abstract

While the global redistribution of military power is continuing, the Middle East region is clearly in a state of flux. Over the past decade, the Gulf States have made important strides in developing some of their own defensive capabilities, strengthening their bilateral relationships with Western militaries, and integrating their armed forces. The key question of today is what it needs to strengthen existing capabilities beyond what it has already achieved. This paper analyses the possible benefits of focusing on C4ISR. It suggests that the acquisition and appropriate application of C4ISR capabilities and assets in the Gulf would offer for outstanding situational awareness, rapid decision-making and decisive action. For the military maximising situational awareness and informational superiority via C4ISR translates not only into an operational advantage on the battlefield, but rather an advantage in all domains, including air, land, sea, space, and most recently, cyberspace. But also the political leadership and business would profit from attaining cutting edge C4ISR capabilities technology as it will ultimately enable rapid response to emerging threats in a dynamic and changing region.

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.

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. Security Dynamics

Nations are confronted today with a multitude of security risks. Global security risks are joining those already existing and developing in the region. Defence capabilities remain key to safeguarding security and prosperity, but so is the protection of critical infrastructure as it is the backbone of any functional economy and society. Further focus needs to be given to the protection of borders and coastlines.

In most circumstances, no single agency, government or organization is able to protect these without the support of the others. Continuously altering requirements and responsibilities and the need to cooperate closely with a plenitude of controlling authorities, involved organizations and even nations ask for synchronized, integrated solutions. Yet, there is a degree of inadequate preparedness for the existing and upcoming challenges.

There has never been a period in recent history where the Middle East was so volatile. While the global redistribution of military power is continuing, the Middle East region is clearly in a state of flux. The events of the Arab Spring, the confrontation over Iran's nuclear arsenal and the possibility of an Israeli attack, the lessons learned from Iraq, Afghanistan and Libya, they all indicate: crises and conflicts can occur at any time, on short notice and without prior warning and may require a rapid response. Prevention and responsiveness are of particular importance – in every respect.

A confluence of events in the Middle East – the withdrawal of American troops from Iraq, the Arab Revolutions in 2011, and the on-going concerns over Iran's nuclear program – have raised questions about the security of the Gulf region, as well as the capability of the six states of the Gulf Cooperation Council to successfully meet challenges to regional security. The Gulf region has been and continues to be a region of strategic importance. It is home to more than half of the world's oil reserves and over a third of its natural gas. The stability of the Persian Gulf is critical to the global economy. Free traffic movement through the Gulf region is key to world economy, energy and politics. Of course, Gulf security also affects the stability oft he countries within the regions themselves, including coalitions and alliances.

Much attention remains focused on the strategic consequences of the Arab Spring, particularly on the civil war in Syria. While Syria will not be another Libya, events in that country will provoke concerns about the aftermath of a regime collapse. Of course, Iran is of importance. In the Gulf, states see Iran as the main threat to regional stability, notably through its ballistic missile and nuclear programmes. But Iran has also upgraded old air defence systems. Additionally, the Iranian creation of hybrid systems based on out-dated weapons, but supplemented with modern subsystems, and deployed using asymmetric tactics has become of concern. All together this has an important influence on the Gulf States' military programmes.

Until recently, nobody would have guessed – given America's gigantic appetite for foreign oil and gas – the U.S. would ever loose its interest in the Arab world. The discovery of vast quantities of shale gas in the U.S. has altered the historic equation. The International Energy Authority estimates that the U.S. will be almost 'energy self-sufficient' by 2035. That prospect means that America will inevitably begin to reconsider the monstrous sums it spends protecting its interests in the Persian Gulf. The U.S. Fifth Fleet, which is almost entirely respon-

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

sible for patrolling the key shipping channels of the Middle East, costs the U.S. taxpayer up to $80 billion dollars a year. But why should the U.S. sustain this effort? Most of the oil ends up in China and Europe.

Over the past decade, the Gulf States have made important strides in developing some of their own defensive capabilities, strengthening their bilateral relationships with Western militaries, and integrating their armed forces. Already today a variety of multi-billion dollar infrastructure security projects in development across the region have C4ISR at their core. Key projects include the Kingdom of Saudi Arabia's Ministry of Interior Modernisation Programme, which requires the integration of C4ISR systems and supporting infrastructure across 900kms of the Saudi Arabian land border with Iraq in addition to its southern land border with Yemen. In the United Arab Emirates[1], the first phase of the UAE Command and Control System[2] is currently under development. This major C4ISR project aims to maximize the combined efficiency of the UAE Armed Forces through the federation, integration, and coordination of UAE military assets.

Since its foundation in 1981 the Gulf Cooperation Council has proven to be an important security structure for the states of the Persian Gulf littoral. This has become even more important with view to an Iraq whose future is uncertain, and that could potentially threaten to destabilize the region either by sliding back into civil war or emerging as a new dictatorship and to cope with the changing balances of power in the region, as well as in the wider world. Ideally the GCC would help the states of the region navigate those shifts. In fact, all of these developments argue for greater cooperation on security matters within the Gulf. The key question of today is what it needs to strengthen the GCC structure beyond what it has already achieved.

In mid April 2013 international defence experts met in Abu Dhabi for the region's first C4ISR[3] Summit. Among top representation from the region was the Gulf Cooperation Council[4] secretary general, Dr Abdullatif Al Zayani who told the summit that the GCC was politically in unison and called for the countries' militaries to follow suit. He specifically called on Arabian Gulf countries to establish military command systems able to exchange and share information at the click of a button: *„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."*[5]

Obviously, the question on the minds of the GCC and regional military commanders responsible for increasing situational awareness and interoperability via the integration of C4ISR capabilities technology is how to further attain a more complete integration of C4ISR systems across all relevant domains. At the summit Major General (ret.) Sadek Al Juhaiman, a Saudi Arabian Ministry of Defence consultant, pointed out that the main threats affecting the region were from non-conventional warfare vandalism, cyber attacks on key networks, cyber attacks at installations and direct attacks on targets*. "The revised regional defence key objectives now cover all domains - sea, land, air, space and cyber,"*[6] he stated to add that adaptable and interoperable capabilities would allow the region to operate with its regional allies. General Al Juhaiman advised that apart from the three armed forces services (army, navy and air force), critical national resources need to be integrated and

[1] UAE.
[2] ECCS.
[3] Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance.
[4] GCC – Saudi Arabia, Kuwait, Bahrain, Qatar, the United Arab Emirates (UAE), and Oman.
[5] 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 30 April 2013).
[6] Ibid.

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

pointed out: *„... the near-term objectives for the region should be to, ultimately, build a system that is interoperable with regional systems and resources, to establish a regional interface that is activated only when needed and combined operational exercises."*[7]

2. Defining C4ISR

The C4ISR concept addresses the provision of information, intelligence and knowledge to decision makers in order to provide for superior situational awareness and decision-making with regard to achieving desired effects. Today and tomorrow military 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. Those systems and services fall in the domain of *C4ISR*, a complex web of sub-systems. C4ISR in today's operational environment is a process exploiting this web - a broad set of capabilities.

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 increasingly supported command. Command has been joined by, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities - an interconnected system at the disposal of the political, civilian and military leaders.

C4ISR provides for information, knowledge and intelligence along with comprehensive situational awareness to decision makers that enable superior decision necessary to execute governmental/coalition decisions in order to achieving desired effects. The envisioned outcome is a comprehensive network enabled capability, which includes technological aspects such as command and control, communications, sensor data fusion as well as human aspects including concepts, doctrine and educational principles.

The quality of command and decision-making has been key to success in warfare throughout the history of mankind. Command aims at superiority, at taking the right decisions at the right time. C4ISR capabilities enable the OODA-Loop – observe, orient, decide, act – as the decision making cycle in the complex and time critical environments of comprehensive security provides effectively for modern defence, to protect people and borders, coastline and critical infrastructure, to support first responders in fire fighting and catastrophic events – natural or man made – and to ensure maritime domain security. The OODA-Loop is based on a demanding observation and action model and offers the capacity to disrupt the decision making cycle of any criminal, extremist or other opponent actor and to keep him from executing its plans. In case damage cannot be avoided, it supports situational awareness and immediate response to reduce the damage to the very minimum possible.

The C4ISR environment is essentially a marriage between Command & Control, Communications, Computer and ISR. Traditionally, Command & Control systems were defined to resolve specific issues in specific environments. As each battle space has been unique and has required a tailored product to maximize results C4ISR has gone through a long development and will continue to change dynamically.

[7] Ibid.

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

To come to an understanding of C4ISR it is necessary to examine the processes affected or influenced by C4ISR. The ISR process is a core process within C4ISR and includes the IS(TA)[8]R collection within the intelligence cycle. It goes further to include knowledge development, knowledge management, knowledge sharing and lessons learned. Good decision-making is dependent on superior knowledge. Knowledge has become the decisive resource of all social processes and social organizations.

For example, decision-making in NATO and the European Union recently has been built on knowledge, derived from a holistic analysis of the challenges to be addressed. To get there, a continuous system of systems analysis needs to be conducted, taking account of the knowledge requirements of all stakeholders. To this end, the Allied Command Operations Comprehensive Operations Planning Directive (COPD)[9], dated 25 February 2010 constitutes an important milestone as it covers in detail planning principles, doctrine and processes. It is the repository of planning knowledge and therefore details and explains each step of operations planning at the military strategic and operational levels of command in Allied Command Operations. It brings together, in one place, theory and practice, process and products.

The COPD already has been shaping NATO's operational planning as an approach in which systems in the operations environment are analysed i.e. through systems analysis, knowledge about the different political, military, economic, social, infrastructure and information domains of the strategic environment will be developed in order to understand the behaviour and capabilities of key actors, their interaction within the operations environment and to make informed decisions that are specific to each of the stages of the planning process.

Intelligence is an activity, which depends on Surveillance and Reconnaissance, for data/information to analyse and assess. Of course, this does not necessarily mean that an additional collection platform, will automatically deliver better advice to decision makers.

Similarly, good data and the intelligence it derives is only of value if we have the communications and computing capabilities to deliver it in a timely, suitably configured, manner. Information exchange via real-time tactical data links remains the backbone of tactical command & control systems. Tactical data links solutions evolved as independent stand-alone systems to meet unique service and functional unit requirements for real-time information exchange. Moreover, the very same mediums are then necessary to deliver the intent of political leadership and military commanders, along with situational awareness and any control constraints and limitations, across the battle space to those units and personnel responsible for execution.

Unfortunately, what C4ISR does not have yet is a sufficiently fused community to address the operational needs of today and the future. In ISR we can observe 'I'-communities which are isolated from the 'S(TA)R' communities. Of course, personnel involved still are learning about the challenging environment. However, there is a clear need for strategic direction to fuse the community.

A plenitude of further issues needs to be 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

[8] TA = Targeting, Acquisition
[9] Simon, Geza/Duzenli, Muzaffer (2009): The Comprehensive Operations Planning Directive. *NRDC-ITA MAGAZINE*, 14, 1-4. Online: http://www.nato.int/nrdc-it/magazine/2009/0914/0914g.pdf (accessed: 30 April 2013).

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

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.

Particularly cyber security is likely to become a complex, demanding challenge in C4ISR. Unlike other domains the cyber domain owes its development to the creative strength of humans. It is man made and provides the actors involved with largely universal access and ever more extensive options of action. With relation to *C4ISR* future cyber weapons may aim to constrain the ability of political leaders, military commanders and/or CEOs to manoeuvre, coordinate or synchronise, and to divert them from focusing on the achievement of their own objectives. Conceptually, unsettling the consciousness of an adversarial actor, causing a loss of belief in his ability to control events and depriving him of control, helps disrupt an adversary's ability to fulfil its objectives.

A threat that has not yet emerged is the use of advanced technology to deny access to disputed areas – the anti-access area denial[10] threat. A2AD is an acronym for getting control of the area someone is going to operate in – air, sea, space, cyberspace, etc. – and making sure you deny that area to a given adversary. To this end a key challenge has become to identify how we to could defeat an adversaries A2AD capabilities such as missiles, mines, or cyber attacks. As soon as the A2AD threat starts materialising, counters are likely begin to appear. This can be expected by the end of this decade.

The cyber threat is perfectly suited to highlight the A2AD challenge. Whether you are operating from a submarine or driving an unmanned vehicle, the domains – air, land, sea, undersea, space – are highly dependent on the cyberspace. And cyberspace is both an exponential force multiplier and a critical vulnerability. In the past governments and their respective instruments of power had the luxury of constant, assured access to cyber space. Although there has never been enough bandwidth for data-thirsty military operations, cyberspace was more or less always usable. As we wind down and try to move these bandwidth-intensive technologies and advancements to counter other potential adversaries, we should understand that owning the cyberspace domain would not always be possible. Our dependency on this connectivity might just be our Achilles heel. Consequently, a growing A2AD threat would drive funding to develop advanced sensors and data links that can operate in the face of an A2AD threat. The *C4ISR* systems require platforms that can operate in the face of that threat. The fielding of platforms and systems that create an A2AD environment is a political decision.

Despite of all these considerations, until today *C4ISR* capabilities rather reflect patchworks than design. This is not only true within the Gulf region. It is also true for NATO, which is still lacking a valid overarching concept, a comprehensive strategic direction for C4ISR. Up to now, NATO Nations have been pursuing their own national C4ISR interests and are acquiring many different capabilities. Nations have in most cases not joint networks. Nations are developing national defence networks that are either not connected, or only partly connected to the NATO network along with a broad range of national Intelligence. Consequently, present C4ISR capabilities have rather been shaped by intent than through strategic direction. Legacy mind-set, in association with the challenges of transformation, balanced against financial austerity in defence budgets, present difficult obstacles for the necessary effectiveness.

[10] A2AD

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

Consequently in NATO a vision for C4ISR needs to emerge in order to build a fully interoperable and interdependent net-centric Joint C4ISR capability that enables decision superiority. Principally such a vision is also required for the GCC in order to derive a coherent C4ISR acquisition and application strategy.

3. Situational Awareness

Accurate and timely data exchange within a C4ISR architecture between all systems involved and other multinational and national information systems are critical to the development of a common operational picture for enhanced situational awareness. Within NATO's operational planning process situational awareness has gained an indispensable function in developing and maintaining a level of understanding to support operational assessments, the provision of operational level advice, and decision making during the planning for and conduct of operations. The purpose of *situational awareness* is to generate actionable knowledge. Its products include

- commander's requests for information;
- key judgements about the situation in the area (risks and threats);
- conditions, trends and tendencies in the area;
- assessment of indicators and warnings.

Situational awareness is the prerequisite of *comprehensive security.* Particularly NATO and the European Union have chosen the comprehensive approach as the principal vision for managing a global landscape in transition is supposed to enable the collaborative engagement of all requisite civil and military elements of international power to prevent crises, to manage them well, to terminate hostilities, restore order, commence reconstruction, and begin to address the conflict's root causes, to integrate all authorities responsible for public security, including the state and police, medical services, fire brigades, intelligence services etc.

To this end, pre-established information sharing, comprehensive planning methods, role integration and ultimately operational support are needed. The close integration of political, military, economic, humanitarian, policing and intelligence instruments is the core of a comprehensive answer to the issue of effective structures for cooperation between the public sector and other parts of society – at the national level and, in particular, across borders.

To work closely on a comprehensive approach NATO and the European Union have principally four instruments of power available:

- Military instruments refer to the application of military power, including the threat or use of lethal and non-lethal force, to coerce, deter, contain or defeat an adversary, including the disruption and destruction of its critical military and non-military capabilities. Of course military instruments can also make a contribution to reconstruction and stability building.
- Political instruments refer to the use of political power, in particular cooperating with various actors in the diplomatic arena, to influence an adversary or to create advantageous conditions.

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

- Economic instruments generally refer to initiatives and sanctions designed to affect the flow of goods and services, as well as financial support to state and non-state actors involved in a crisis.
- Civil instruments refer to the use of powers contained within such areas as judiciary, constabulary, education, public information and civilian administration and support infrastructure, which can lead to access to medical care, food, power and water. They also include the administrative capacities of international, governmental and non-governmental organizations.

Situational awareness will be generated within given C4ISR architectures and processes via platforms, sensors, links, data & sensor fusion, change detection, decision support tools, open source intelligence, and knowledge development. The quantity and depth of information collected from these various sources need to be fused to enrich a *common relevant operational picture* that can be – role-based – distributed among relevant users.

Situational awareness is of outmost importance in complex A2AD environments. To this end countries are seeking increasingly to deploy a comprehensive communications network to exploit information provided by new and upgraded ISR platforms. Consequently, the largest functional segment is Multi-Role Electronics; essentially sensors and mission equipment packages on airborne ISR and maritime patrol platforms. Network Infrastructure is another significant function including radios & terminals, surveillance & reconnaissance, battle management & tactical networks.

Military vehicles are being turned into situational awareness hubs with multi-role functionality. Most wheeled or armoured fighting or command & control vehicles that have recently been contracted by defence ministries in countries such as Brazil, Turkey, India, South Africa and Saudi Arabia have computing systems on board an advanced open Vehicle Electronic Architecture. This enables integration of all elements of total situational awareness, i.e. communications, surveillance, navigation, detection, blue and red force tracking, fire control, and survivability & protection systems[11] into a common display with the aim of providing comprehensive force protection on the frontline.

Situational awareness needs to be shared. Information sharing needs to be pre-established. It requires comprehensive planning methods, role integration and ultimately operational support in order to project all available instruments at an early stage and in an integrated fashion in order to achieve a maximum outcome. Sharing means less to integrate established, proven systems into a single new one, but rather to consolidate comprehensive data and information from sources and inventories of the acting decision-makers and related personnel. An information turntable provides the information from multiple sources, inventories and databases. A particular challenge is the collection, fusion and dissemination of enormous quantities of data drawn from military and civilian government agencies, international coalition partners and forces, and commercial entities.

A role-based approach, rules and workflow modelling structures enable situational awareness environments to push information to stakeholders within and across organizations while ensuring the security of the information. The role-based approach ensures that stakeholders are able to communicate through a variety of means and maintain role-focused situation awareness throughout the organization and among organizations – many

[11] i.e. Counter-IED

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

are looking at different situational pictures, but all look into the same situation with a common shared situational awareness.

Two recent important initiatives in NATO have been driving situational awareness within the Alliance

- a common C4ISR network – the Afghan Mission Network – has been established for all ISAF forces and operations consisting of the ISAF-secret network as the core with national extensions. In times of austerity cuts these national extensions have an enormous shaping impact on national C4ISR structures. Consequently, NATO is planning to expand this approach to build a Future Mission Network.
- NATO can build its situational awareness and decision-making on a Common Operational Picture providing NATO commanders and operational staffs with essential and reliable information that enables their understanding of comprehensive security environments.

On a global scale, both developments have served as best practice examples for security forces and security business. Consequently they keep shaping both, requirements and markets.

4. Way ahead

In the wake of the U.S. pivot towards Asia and under the impression of Iran's possible development of a nuclear weapon, there is a strong rationale for the states of the Persian Gulf region to consider how best they can bolster their own security. The centrepiece of a framework ensuring prosperity and security in the region is deepening security cooperation, both bilateral and multilateral, with the six states of the Gulf Cooperation Council. Although the UAE and Qatar have demonstrated a willingness to operate in the coalition environment, most Gulf States are not yet fully capable of independently sustaining significant tactical support to Western partners in times of crisis. Thus it is important to cultivate the capabilities of GCC partners in select defensive missions, such as missile defence, combat air patrol, and maritime security, while building capacity through deployments in other theatres such as Libya and Afghanistan.

To clearly understand, what could and should be done, it may be useful take a look at the situation in Korea[12], which has elements that may be comparable to the situation in the Gulf. For South Korea, having just successfully overcome a series of North Korean aggressive acts, any future North Korean attack is much more likely to be asymmetric, coming in the form of limited, rapid, and possibly even plausibly deniable strikes, rather than in the form of a head-on assault by out-dated platforms over land, in the air, or at sea. Such asymmetric strikes have characterized the North's attacks in recent years, including surprise attacks by surface vessels in the West Sea; massive cyber attacks on South Korea's banking, media, and government information infrastructure; the sinking of the South Korean corvette *Cheonan*; and the strike against Yeonpyeong Island in late 2010. None of these attacks allowed the South to leverage its advantages in topographical defences or its advanced technology platforms. Instead, they struck at perceived weaknesses in the South's defence posture. The Gulf states should be better prepared to meet comparable challenges, in particular as Iran develops

[12] Harold, Scott W., „Obama-Park Summit a Critical Opportunity for the US-Korea Alliance", in: PacNet #25 Wednesday, 17 April 2013.

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

asymmetric capabilities similar to those of North Korea.

South Korean leaders have invested in the past heavily in large prestige platforms, such as advanced tanks and armoured personnel carriers, surface vessels, and advanced fighters. Yet, the South's defences need to be improved rather by acquiring additional capabilities in command, control, and communications; intelligence, surveillance, and reconnaissance (ISR); counter-artillery, -rocket, -mortar, and -missile defences; improved cyber capabilities; *brown-water* or coastal defences; and countermine and anti-submarine warfare. Particularly *situational awareness* is key of what's happening on the ground, in the air, on and under the surface of the ocean, and in the space and cyber realms, giving national leaders better options to respond quickly and effectively. In principal many of these observations apply to the Gulf region as well.

The legendary Admiral Cebrowski used to say *"… C4ISR is about the co-evolution of technology, organisation (i.e. architecture & processes), ... and people."* [13] In fact, *C4ISR* is enabling decision makers by systems to increase their level of situational awareness to make the right decision at the right time. Rapid technological developments are breeding disruptive technologies in the defence industry more than ever. The markets have begun understanding *C4ISR* as a service – a service primarily to satisfy immediate mission needs. Instabilities and difficult security situations drive funding of sensors, and networks that enable sharing of ISR information and exercise of C2. The *C4ISR* market is worth a trillion dollars[14] over the next 10 year and runs the gamut from the extensive United States intelligence support outsourcing to communications, command and control (C2), geospatial, optical and radar sensors to *C4ISR* aircraft, unmanned aerial vehicles and space-based surveillance, much of it in large support contracts.

To this end defence majors have started developing solutions for existing respectively anticipated capability gaps and business model that allows them to eventually hand those managed assets back to the end user over a good period of time through a systematic training and support program. For example counter-terrorism requires identification and tracking of threats down to the individual level and communication of information down to the small unit. Sovereignty over ocean economic resources requires deployment of sensor platforms and communications networks. Most of the systems that will be produced and deployed within the coming decade to meet these threats will be technology just completing development or available as mature off-the-shelf technology. Handheld C2 systems in particular will tend to be commercial-off-the-shelf[15] devices. With view to innovation cycles of 2 years and less sensors on existing platforms need to be upgraded as well as existing data links.

A driving trend for governments has become identifying common threats across multiple agencies, particular security agencies. Economies of scale and the required efficiency can be achieved through increasing the commonality of systems used by different end-user groups. Common products, systems, and services will increasingly meet the requirements of multiple agencies in a country, an organisation. This has triggered programmes to integrate command & control, communications, IT, surveillance including UAS ground stations and radars, C-IED and detection assets under a scalable C4ISR architecture.

It appears that the C4ISR market is not investing any longer in system development like it used to do. Most of the market has embraced upgrades to existing systems or off-the-shelf solutions. Governments will only invest

[13] JAPCC
[14] IHS Jane's Defence Insight Report, „C4ISR & MISSION SYSTEMS" Janes, April 2013, p. 4.
[15] COTS

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

in solutions where industry simply cannot assume the risk of developing advanced technology to unique but important requirements. The most significant exception is cyber security and cyber attack that show growth. The largest investment within the next decade can be expected in ballistic missile defence. Other large segments deal with sensors, mission equipment packages on ISR platforms and intelligence analysis of data.

As it is difficult for organisations to keep up with breakthrough technologies at each segment level due to the significant investment involved defence majors are currently pursuing three complementary growth strategies[16]

- expanding their respective geographic footprint as defence budgets particular in transitioning markets are on the rise due to economic growth;
- expansion into adjacent commercial markets, where skills and capabilities can be applied;
- providing improved value for money through efficiency savings in both project and support, and increasing the use of Commercial Off the Shelf technologies and products.

At the C4ISR summit in Abu Dhabi Brigadier Alan Hill, the 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. He 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."*[17] General Al Juhaiman strongly supported Brig Hill's views and stressed that security awareness and training should be increased among staff: *"Strict procedures should be applied for material transfer to the system as the possibility of compromising all the data and systems is viable".*[18]

How to get there? With regard to building an effective C4ISR environment in the Gulf region, it will be important to come up with a valid strategy addressing both individual country needs and regional security concerns. In order to develop a perspective for the way ahead in the C4ISR arena it is necessary to

- create a vision statement;
- identify the methodology to transform the vision into a roadmap focussing on end-to-end C4ISR capabilities, from sensor to decision maker to effectors
- develop the Roadmap itself addressing
  - a C4ISR acquisition and application strategy in line with the dynamic changes occurring in the region;
  - current gaps in C4ISR faced by countries in the GCC and an overview of the potential solutions being considered;

[16] Frost & Sullivan, „Global C4ISR: The Growth of "Transitioning Markets", September 2012 http://webcache.googleusercontent.com/search?q=cache:__YOvkSkDG4J:www.frost.com/prod/servlet/cio/267161924+frost+and+sullivan+c4isr&cd=1&hl=de&ct=clnk&gl=de. (accessed 30 April 2013)
[17] 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 30 April 2013).
[18] Ibid.

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

- a cyber security approach building on valid C4ISR architectures and processes;
- a concept to developing and integrating C4ISR systems across all divisions of the armed forces in order to combat emerging regional threats;
- requirements for air surveillance and reconnaissance including unmanned aerial systems;
- the integration of existing and planned air and missile defence systems;
- early and adequate training to maximise efficiency and use of C4ISR systems.

Of key importance to improve the current situation will be

- leadership – a change in culture, attitude and mind-set in order to start thinking network-centric;
- integration – the the fusing of human and technical domains, standards and procedures as well as training and education;
- interoperability – data, information and knowledge dissemination and sharing between the partners operating within a given C4ISR system;
- partnership – with nations and coalition partners in order to achieve coordination, integration and even synergetic action. Partnership with industry is essential to go for available solutions building on proven technology inside and outside the military.

To this end I would recommend

- creating a governance body looking across the whole spectrum of C4ISR capabilities and requirements in the GCC;
- enhancing cohesion within the GCC C4ISR community through increased awareness;
- building Joint Intelligence, Surveillance and Reconnaissance;
- introducing a GCC communication and information systems that supports high operational tempo also in planning and logistical functions;
- developing a C4ISR guidance in line with the GCC's level of ambition;
- building an effective training and development environment for the GCC C4ISR community;
- designing a concept of operations that builds on advanced Information and knowledge management;
- establishing a "need to share" mind-set;
- implementing a multilevel security system for automatic data exchange;
- establishing a concept development and experimentation capacity that proactively integrates lessons learned into current operations.

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

Clearly, the acquisition and appropriate application of C4ISR capabilities and assets in the Gulf needs to provide for outstanding situational awareness, rapid decision-making and decisive action. For the military maximising situational awareness and informational superiority via C4ISR translates not only into an operational advantage on the battlefield, but rather an advantage in all domains, including air, land, sea, space, and most recently, cyberspace. But also the political leadership and business will profit from attaining cutting edge C4ISR capabilities technology as it will ultimately enable rapid response to emerging threats in a dynamic and changing region. This will provide for sustained prosperity and security in the Gulf.

***

Remarks: Opinions expressed in this contribution are those of the author.

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 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 security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and 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