Big Data meets Gulf Security – Exploiting the Strength of Networked ISR Systems

Ralph D. Thiele

June 2016

Abstract

The recent meeting of GCC leaders with U.S. President Barack Obama in Riyadh have highlighted that GCC security planning points at security capabilities across all domains, furthering the interoperability in joint, multilateral, and inter-government operations. As interoperability and integration have become a new benchmark priority to the Gulf nations it remains of particular importance to implement an own interoperable C4ISR system with the capability of fusing human and technical domains, standards and procedures as well as training and education. Recently there has been a quantum shift in technology effecting C4ISR capabilities. Particularly the emergent technologies of Big Data analytics, autonomy, sensor miniaturisation and the exponential growth of processing power provide extraordinary opportunities for collecting and analysing ISR data in novel ways and in particular to deliver the right information to the right people, at the right time. Interoperability among GCC nations requires highly capable, networked ISR systems, which can plug and operate. As networked ISR is building on very complex and demanding processes the experiences gathered at GCC level – to include also experiences with further international partners – would be of particular importance as it would certainly also prove to be valuable in support of homeland operations.

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 impartial to party politics.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, that bring 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 relating to politics, economy, international relations, and security/defence. ISPSW network experts have operated in executive positions, in some cases for decades, and command wide-ranging experience in their respective areas of specialization.

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

"... 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 ...".

Dr Abdul Latif Al Zayani, Secretary General of the Gulf Cooperation Council at the 2013 C4ISR Summit in Abu Dhabi[1]

1. New Era

The GCC nations are facing unprecedented challenges to their security, as they worry about threats from their unstable neighbours, including Syria, Iraq and Yemen. From their perspective, these countries are breeding grounds for extremist groups and places where Iran can bolster its influence and threaten the security of peaceful Arab states while these aim at consolidating a new Arab political order thus bringing order and stability to the heart of the Arab world.

At the same time, the era of Pax Americana in the Gulf, and the broader Middle East, is fading. Former almost exclusive U.S. access and control has been replaced by a more permissive system with increasing regional engagement of powers such as Russia, China, India, the United Kingdom, and France. Of course, the United States is still militarily dominant.

Consequently, GCC leaders have started developing the capacity and capabilities for their countries to jointly address the security challenges facing the region. Joint military operations by the GCC's 30,000-strong Peninsula Shield Force have shown in the recent past how effectively it can protect its members. Yet, faced with modern, but disparate, proprietary, stove piped systems, government and military leaders express an understandable degree of frustration. Non-interoperable legacy systems cost too much to operate, consume excessive resources and ultimately disrupt mission readiness. Thus, interoperability and integration have become a new benchmark priority. To the Gulf nations it remains of particular importance to implement an own interoperable C4ISR system with the capability of fusing human and technical domains, standards and procedures as well as training and education.

Additionally, C4ISR has gained particular importance with view to the challenging spectrum of the upcoming hybrid threats[2] ranging from cyber-attacks on critical information systems, through the disruption of critical services, such as energy supplies or financial services, to undermining public trust in government institutions or exploiting social vulnerabilities. Meanwhile also civilian government agencies are finding C4ISR an indispensable asset for supporting their missions as hybrid challenges come as a mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare increasingly. Against this background both, civilian decision-makers and military commanders, need to be enabled to take timely decisions, based on the right understanding drawn from accurate information and intelligence.

The recent meeting of GCC leaders with U.S. President Barack Obama in Riyadh have highlighted that GCC security planning points at security capabilities across all domains, furthering the interoperability in joint, mul-

[1] Awada Mustafa. The National. UAE. 17.04.2013. Remarks of Dr Abdul Latif Al Zayani, Secretary General of the Gulf Cooperation Council at the 2013 C4ISR Summit in Abu Dhabi. http://www.thenational.ae/news/uae-news/experts-at-abu-dhabi-summit-want-gcc-military-integration
[2] European Commission. FAQ: Joint Framework on countering hybrid threats. Brussels 6 April 2016.

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

tilateral, and inter-government operations.[3] Focus areas for security cooperation include counterterrorism, ballistic missile defence, military preparedness and training, streamlining the transfer of critical defence capabilities and cyber security. Dedicated security initiatives address Special Operation Forces, Intelligence Exchange, Maritime Cooperation etc. A major U.S.-GCC military exercise has already been scheduled for March 2017 to demonstrate the full scope of joint, multilateral, and inter-government security capabilities across all domains thus furthering interoperability requirements. Clearly, the backbone of such capabilities will be networked ISR systems. This should be a GCC owned backbone, shouldn't it?!

2. Quantum Shift

Recently there has been a quantum shift in technology effecting C4ISR capabilities. Sensors fly on UAVs, aircraft and satellites, ride on ships and land vehicles, or even sit on the helmet of soldiers. Virtually anything can serve as a sensor thus turning any portable device into a source of data. Advanced sensors, modern radar systems, electro-optical/infrared sensors, electronic support measures systems etc. have reached new levels of sensitivity and accuracy providing for enormous volume, velocity, veracity and value. They capture the full spectrum of intelligence signals and can send full-motion streaming video, day and night. While sensor capabilities grow rapidly, they also get smaller, so more of them fit on a single platform. Increasing interoperability ensures that available data can produce remarkably accurate and effective common operating pictures for situational awareness.

Thrilling developments competently address unmanned aerial vehicles, modern unmanned surface vehicles and unmanned underwater vehicles, maritime domain awareness, command and control systems, network enabled capabilities, tactical radio frequency communications, optical communications, satellite communications, the electromagnetic environment, countermeasures against the modern IR threat, suppression of enemy air defences, cyber, information operations etc. Breakthroughs in geospatial analysis, geo-location and geo-visualization continue to advance the capabilities and value of C4ISR. Layering vast amounts of data from multiple sources and putting it on the map in increasingly useful and timely displays, geospatial solutions are critical to making situational awareness easily understood in time for users to take effective action. The real-time situational awareness that C4ISR provides vastly increases the agility of forces to manoeuvre and respond.

To ensure, the right data doesn't get lost amidst the massive amounts of data the systems need to turn the collected data into useful, actionable information. The emergent technologies of Big Data analytics, autonomy, sensor miniaturisation and the exponential growth of processing power provide extraordinary opportunities for collecting and analysing ISR data in novel ways and in particular to deliver the right information to the right people, at the right time.

Another focus is better exploitation of existing assets and utilizing low-cost, high-reward technology, such as in greater incorporation of Big Data and enhanced communications and networking. The C4ISR world is working to keep up with the capabilities of commercial Smart Phones, Smart Pads, and an array of other mobile devices such as Cameras, radios, GPS receivers, accelerometers, health monitors etc. With the right level of security, these devices can be integrated safely into global C4ISR networks. Thus cyber security has become critical as C4ISR of this scale and complexity to work must be assured at the highest level of security. It should be added

[3] The White House Office of the Press Secretary, April 21, 2016, FACT SHEET: Implementation of the U.S.-Gulf Cooperation Council Strategic Partnership https://www.whitehouse.gov/the-press-office/2016/04/21/fact-sheet-implementation-us-gulf-cooperation-council-strategic

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

that in the past years Cyber has become in some nations alongside army, air force and navy an own military service with tailored offensive and defensive capabilities.

Against this background, many national services around the globe are readdressing their individual airborne ISR capabilities, investing in a broad range of capabilities to improve situational awareness and understanding to include in the maritime domain. In the coming years, we will see maritime and airborne autonomous systems as a key means of increasing mass and agility in the ISR space. Consequently it comes as no surprise that the global C4ISR market is highly competitive with registered revenue US $99 billion in 2015. It is expected to touch US $125.46 billion by 2020.[4] It is primarily fuelled by greater demand for integrated and interoperability solutions, in developing countries for networked communication, sensor upgrades, intelligence and electronic warfare systems. And it is expected to register tremendous growth in India and China. Growing domestic production, coupled with government incentives will likely drive the market for sea based C4ISR systems in Asia and Middle East. Airborne systems are seeing the highest demand and growth rates.

3. Joint ISR

An essential basis of decision making in crisis management are skills for intelligence, surveillance and reconnaissance. Yet, increased collect does not equal to increased understanding. It is of key importance to understand context and commit appropriate processing effort – both human and machine-based. In NATO this capability is addressed under the term Joint Intelligence, Surveillance, Reconnaissance – Joint ISR. Joint ISR encourages the dynamic, agile and coordinated use of platforms, sensors and systems to support a wide range of staff functions allowing the right information provided to the right person at the right time in the right format. It may also include collection from systems not primarily known as an ISR collection system, commonly known as non-traditional ISR, such as reconnaissance imagery captured using a targeting pod on ground attack aircraft.

NATO Joint ISR Doctrine Development defines Joint ISR as *"an integrated intelligence and operations set of capabilities, which synchronizes and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of planning, preparations, and execution of operations."* [5] Joint ISR employs the enormous potential of Big Data and thus creates the basis for a superior situational awareness and understanding of decision-makers and actors in crisis management. The requirement to generate understanding of the operational environment, across the physical, virtual and cognitive domains has become more vital than ever. Developing security challenges in the Gulf region underline the imminent importance of superior situational awareness.

Already NATO's Operation 'Unified Protector' over Libya in 2011 exposed various capability gaps of NATO forces, including for co-ordinating and deploying its member's ISR assets. NATO Secretary General Anders Fogh Rasmussen noted at that time particularly that the operation "*revealed shortfalls in precision-guided munitions; intelligence, surveillance, and reconnaissance assets; and experts trained to interpret the data they provide*"[6]. In fact, NATO JISR until today

[4] Research and Markets. Global C4ISR Market 2015 – 2020, Feb 19, 2016. http://www.prnewswire.com/news-releases/global-c4isr-market-2015-2020---platform-region-and-vendors---harris-corporation-rheinmetall-defense-raytheon-are-key-important-players-300223095.html
[5] *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* - AJP 2.7SD2
[6] NATO Secretary General Anders Fogh Rasmussen. Press conference. Brussels 26 Feb 2014. http://www.nato.int/cps/en/natolive/opinions_107408.htm

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

- Is unable to satisfy information requirements primarily due to the fact that its systems, architectures and processes were designed for a very different operating environment.
- Lacks the required number and mix of collection capabilities. JISR assets are few and are owned by the Nations who are not always able or willing to share them with partnes. Some are also of limited capability.
- Lacks inter-organization coherence and cooperation. Headquarters, staffs and individuals are still working in a stove-piped manner, instead of integrating in an environment where information sharing and tasking extend to all dimensions.
- Lacks the ability to effectively access or share intelligence and information with other elements of allies, partners and non-traditional actors in the theatre of operations in a timely manner for technical, procedural and cultural reasons.

At both the 2012 Chicago and 2014 Wales NATO Summits, Heads of State and Governments identified enduring ISR capabilities as amongst the Alliance's most critical capability needs. Successfully delivering these capabilities now more than ever depends upon effective partnering, coordinated collaboration and the timely acceptance and utilisation of various C4ISR capabilities that are being made available. In Wales NATO announced the establishment of a permanent Joint Intelligence, Surveillance and Reconnaissance (JISR) system to "*provide information and intelligence to key decision makers helping them making well-informed, timely and accurate decisions"* thus exemplifying the benefits of multinational cooperation.

The Joint ISR core activities focus on the JISR cycle - comprising of Tasking, Collection, Processing, Exploitation and Dissemination -, thus requiring extensive cross-Community of Interest coordination and interoperability. To achieve the effective and efficient exchange of information within the Alliance, the involvement of the operational, intelligence and communication/information systems communities is required. Consequently, the Joint ISR initiative also addresses organisational structures, related hardware and physical assets, software applications, procedures and doctrine, training and education, networking environments, experimentation and trial. Consequently, NATO is building its Joint ISR capability – via the Connected Forces Initiative and joint training exercises – upon three pillars:

- NATO ISR procedures,
- a JISR networking environment, and
- JISR training and education.

The Joint ISR cycle includes planned and dynamic aspects. It integrates Alliance and National Intelligence, Surveillance and Reconnaissance capabilities, policies, procedures and systems to provide information support to leaders, commanders and decision makers through political and strategic domains down to the tactical level.[7] The types of supported operations include:

- Joint Intelligence Preparation of the Operational Environment
- Targeting and Battle Damage Assessment/Combat Assessment,
- Maritime Operation
- Air Operations
- Land Operations

[7] NAO. 10 Feb 2016. http://www.nato.int/cps/en/natolive/topics_111830.htm

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

- Special Operations
- Counter-IED Operations
- Force Protection
- Civil-Military Co-operation

In sum, as Joint ISR synchronizes and integrates operations and intelligence capabilities and activities, it is geared to provide timely information to support decisions it particularly contributes to the provision of Situational Awareness.[8]

4. Best Practices

During his recent visit in Abu Dhabi U.S. Secretary of State John Kerry floated the notion of a formal security partnership between the GCC and NATO. It will be thrilling to see whether and how this will materialize at the upcoming NATO Warsaw Summit. Interestingly, the United Arab Emirates (UAE) is among NATO's most active and valuable partners. In 2012, in the framework of the Istanbul Cooperation Initiative, the UAE has become the first and only country in the Middle East and North Africa to open a mission to NATO. It has held joint consultations and exercises with NATO in numerous areas, including maritime security, counter-piracy, proliferation and energy security. At the 2014 NATO Summit in Wales the UAE has become partner of the then launched Interoperability Platform, assembling partners that have demonstrated their commitment to reinforce their interoperability with NATO.

An excellent best practice underlining how such cooperation and interoperability could be promoted not only with NATO but also within the GCC has been set by NATO nations, when they conducted in May 2014 with *Unified Vision 2014* the biggest ever trial for joint intelligence, surveillance, and reconnaissance systems. The scenario included a crisis situation that began locally, but developed into a full international conflict. The trial brought together nearly 2,000 personnel, satellites, aircraft, unmanned aerial vehicles, navy ships, ground sensors, and human intelligence assets from 18 NATO members – to include Belgium, Canada, the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Lithuania, the Netherlands, Norway, Poland, Romania, Spain, Turkey, the UK, and the United States – thus testing NATO's ability to gather information and fuse intelligence from multiple sources at different stages of a crisis.

Frequent NATO partner Australia served on an assessment team, and Sweden and Finland provided observers. Sensor platforms included the Predator, Global Hawk, Hunter, Raven, and Puma UAVs; a NATO Airborne Warning and Control System aircraft; a naval corvette; and reconnaissance vehicles. NATO analysts received ISR data from these platforms and sensors fused intelligence products from various incoming imagery, communications, human intelligence, and open source information. Rather than floating commanders with information from different sources, they were provided with a common operational picture and situational awareness derived from multi-national assets so that they were enabled any time to take informed decisions.

As a follow up earlier this year NATO's *Unified Vision 2016* (UV 16) took place exploring how data collected from individual national aircraft – plus the alliance's new unmanned air vehicle (UAV) capability – can be better used during joint missions. As the processing, exploitation and dissemination (PED) of data has become a key area of development for NATO, UV 16 has been looking particularly towards federated PED among allies also

[8] NATO Communications and Information Agency. Joint Intelligence, Surveillance and Reconnaissance. https://www.ncia.nato.int/Our-Work/Pages/Joint-Intelligence-Surveillance-and-Reconnaissance.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

testing the dissemination of joint intelligence, surveillance and reconnaissance data into the command and control system so that it is less stove piped to each nation. Wouldn't such exercises as a GCC trial be a great opportunity also for the GCC military? In the end, even sophisticated C4ISR systems are not useful if not trained and exercised properly.

Another best practice with relevance to GCC nations in the context of ISR is the European Framework Nation Concept (FNC) that – with adaptations – could be well applied in the given GCC setting. The Framework Nations Concept is a key contribution to the European defence cooperation debate with view to a fading U.S. engagement in Europe. It aims at preserving European capabilities through sustained cooperation, and thus guarantees for European militaries the continued capacity and capabilities to act.

According to the logic of the FNC European states form clusters, i.e. groups of smaller and larger states, that will coordinate closely who will provide which assets and troops on a long term basis. The respective ‚Framework Nation' takes the lead of such a cluster. It provides the group with the respective backbone, i.e. command & control, logistics, Big Data evaluation etc. Into this frame, smaller nations plug in their specialized – sometimes niche – capabilities. Thus the entire cluster becomes significantly more effective and sustainable, capable of carrying out longer and more complex operations than any national approach could provide for.

With view to the European and NATO Joint ISR capability gap Germany has volunteered in the context of the Framework Nations Concept (FNC) cluster to support joint ISR as framework nation, thereby playing a long-term leading role. The corresponding joint ISR element will be an internationally deployable Joint ISR capability. Other European members of NATO have decided to join the capability cluster. Particular small states can make a difference. By matching the needs of their allies and partners, by providing high quality ISR products and by serving each other's purposes, a small nation can definitely "punch above its weight". Given their outstanding ISR capacity the Emirates could well perform such a framework nation function in a GCC Joint ISR capability cluster.

5. Knowledge is power

While the 21st century battle space is growing more dynamic, reactive and flexible then ever, lines between operations and intelligence are blurring – interdependent in near real-time. Networked ISR is in an evolutionary state. Yet its products are urgently required. To this end doctrine needs to evolve, holistically focusing on operations. Already two decades ago Joseph Nye stated that "*knowledge, more than ever before, is power.* … [He highlighted the] *comparative advantage* … [of the] *ability to collect, process, act upon, and disseminate information*."[9] In fact, today governments and their civilian and military instruments of power have to learn to exploit available information and knowledge in order to gain the required edge in meeting challenges to security, stability and prosperity.

In the context of Clausewitz' strategic theory the effective exploitation of ISR facilitates a better view "*through the fog of war*" and also better decision-making. The exploitation of networked ISR systems as an enabler helps overcome traditional time-and-space barriers imposed on communications and generates a shared awareness that is able to reduce the traditional "*friction of war*." It allows joint and combined forces to fight as a networked force because vast amounts of information can be stored, evaluated, processed and then disseminated

[9] Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge," Council on Foreign Relations, March/April 1996, http://www.foreignaffairs.com/ articles/51840/joseph-s-nye-jr-and-william-a-owens/ americas-information-edge.

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 multiple users in a short span of time.

In the past, information was typically stove piped within organizations. Different systems and platforms couldn't talk to each other. For many reasons, the defence and intelligence communities remained isolated from each other. And information sharing with coalition partners was infrequent at best. Today, this has turned around – joint operations are the norm. The level of integration among systems and forces, including weapons systems, is high and further integration is vital. Consequently Joint ISR has become a force multiplier – militarily and even in the interagency context.

NATO Secretary General Jens Stoltenberg praised in his meeting with Foreign Minister Sheikh Abdullah bin Zayed Al-Nahyan in Abu Dhabi on 2 March 2016 the Emirates' contributions to NATO-led missions in Bosnia, Libya and Afghanistan. He stressed that there is scope for more participation by the UAE in NATO exercises and interoperability programmes, as well as further joint work on defence capacity building and civil emergency planning. Both, NATO and the United Arab Emirates expressed their determination to enhance cooperation in addressing common security challenges.[10]

It was the famous Prussian General Gerhard von Scharnhorst – by the way also teacher and promoter of the later even more famous Carl von Clausewitz – who said: ***"Why should anybody who cannot defend himself get others to join in as partners?"*** By the end of the day cooperation of GCC nations with NATO will require inter-operability among GCC nations themselves and highly capable, networked ISR systems which can plug and operate – if it becomes necessary – with capable partners. As networked ISR is building on very complex and demanding processes the experiences gathered at GCC level and with further international partners would be of particular importance. This very experience in the field of C4ISR would certainly also prove to be valuable in support of homeland operations. Consequently building and training this very capability should be a focus area in the GCC military, perhaps even with UAE leadership as a kind of framework nation?

***

Remarks: Opinions expressed in this contribution are those of the author. This paper was presented by the author on the C4ISR Summit Middle East on May 30, 2016 in Abu Dhabi, UAE.

[10] NATO. 2 March 2016. NATO and UAE determined to enhance cooperation in addressing common challenges. http://www.nato.int/cps/en/natohq/news_128753.htm

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 StratByrd 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