Towards Integrated C4I – NATO Experience in Building C4I Systems

Ralph D. Thiele

January 2018

Summary

The rapid acceleration and hybridization of security operations has challenged national actors and international alliances to seek interagency and comprehensive approaches. Russia´s engagement in the Ukraine has been a wakeup call to the West. This development has led to a situation in Europe, where defence budgets are rising again. Consensus is that member nations maximize the value of their investments. With view to given hollow structures it is important that NATO members increase their investments in defence. It is even more critical to invest in the right capabilities.

In the given hybrid security environment decision makers require comprehensive situational awareness – delivered when and where it's needed supported by advanced Command, Control, Communications, Computers, Intelligence (C4I) capabilities. These will enable NATO to address not only the challenge of combat in wide-open spaces, against high-signature military targets such as armoured vehicles, extensive military infrastructure, surface to air missile sites and radar systems, but also low-signature guerrilla forces and terrorists deeply embedded within the civilian surroundings.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena 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, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

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. Complexity

Today's strategic environment is defined by complexity and unpredictability, underlining the necessity for nations and organizations such as NATO and the European Union to be more responsive, more resilient, and to work with a wide network of partners. The rapid acceleration and hybridization of security operations has challenged national actors and international alliances to seek interagency and comprehensive approaches. To take appropriate action, decision makers require comprehensive situational awareness – delivered when and where it's needed – to avoid acting too late or even targeting the wrong objective. Advanced Command, Control, Communications, Computers, Intelligence (C4I) provides the global collaboration environment. Well-orchestrated, interoperable, multiple services and countries employing network-enabled capabilities in a comprehensive approach to operations – this is not only the trend, but rather the requirement in modern security operations.

While complexity can be a challenge, political and military decision makers strive to make it rather an asset. Under the C4I umbrella, Command & Control encompasses all functions necessary for the planning of operations from plan development to mission execution and exploitation. Communications & Computers provide the secure communication means and automated data processing tools to create a collaborative environment fitting the complex requirements. It provides a means to link operational planning and relevant Intelligence – to include also Surveillance & Reconnaissance (ISR) – an activity designed to improve situational awareness and gather critical information about suspicious and opponent activities to feed the operational decision-making process. The ISR cycle connects the operations cycle with the intelligence cycle thus transforming information superiority into decision advantage.

2. Drivers

NATO's road towards C4I capabilities got kick-started with the experimental employment of JSTARS[1] during Operation Desert Storm in 1991. During the first ground engagement near Khafji in Saudi Arabia – attacked by the Iraqis on January 29 – JSTARS identified the location of Iraqi troops, when and where they were moving, and confirmed the absence of any reinforcements en-route. The Iraqi troops had little opportunity to resist and became finally something like targets on a shooting range. Step by step several applications were introduced to complete JSTARS. These have revolutionized the way NATO deals with combat and other security requirements.

Twenty years later during Operation Unified Protector 2011 in Libya JSTAR was still a key asset. In between NATO had worked on its own C4I capabilities. Yet, former NATO Secretary General Anders Fogh Rasmussen had to admit serious deficiencies. He stated in his remarks *at the Brussels Press conference on* 26 February 2014 that 'Unified Protector' has clearly "*… revealed shortfalls in precision-guided munitions; intelligence, surveillance, and reconnaissance assets; and experts trained to interpret the data they provide*".[2]

Until today NATO C4I systems have been operating well below their potential capabilities. Stove piped systems make it difficult and sometimes even impossible to collect, analyse, and disseminate critical threat and operations information, or obtain a complete, single view of the battlefield. Too often, commanders must log into

[1] Joint Surveillance Target Attack Radar System
[2] NATO. More than just information gathering. Giving commanders the edge. Brussels. 26 May. 2014. https://www.nato.int/cps/en/natohq/news_110351.htm?selectedLocale=en

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

multiple systems, each with separate displays, while war fighters in the field struggle to operate a variety of radio systems and communications protocols. Many applications and systems lack the interoperability, user friendliness, and technical capabilities that are readily available in commercial technologies as current acquisition processes cannot keep pace with technological change.

At several NATO Summits, Heads of State and Governments identified enduring C4I capabilities as amongst the Alliance's most critical capability needs. Already the 2012 Chicago Summit established the objective to strengthen cooperation and ensure tighter connections between Allied forces. During the Summit, the Allied Heads of State and Government expressed the ambition to provide NATO – as a core C4I capability subset – with an enduring and permanently available Joint Intelligence, Surveillance & Reconnaissance (JISR) capability, giving the Alliance the eyes and ears it needs to achieve strategic decision advantage.

The third driver of NATO C4I capabilities has become the shock when NATO (and EU) nations had to realize the impressive hybrid warfare capabilities which Russia employed in the Crimea and the Ukraine. Suddenly C4I became particularly important with view to the challenging spectrum of the upcoming hybrid threats[3] – 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 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. With a centre of gravity shifting to non-military engagements increasingly also civilian government agencies are finding C4I an indispensable asset for supporting their defense against hybrid threats.

NATO and EU have understood that they need to come up with integrated approaches and share best practices on how to lead and coordinate national efforts of self-assessment, threat analysis and comprehensive security response with C4I as a critical enabler.

3. Vision

It took a while until a coherent vision on C4I has been developed in NATO. A remarkable contribution came in 2005 by the NATO Joint Air Power Competence Center (JAPCC) that developed a roadmap for NATO C4I. Building on then existing NATO plans and programs underway the JAPCC identified the areas of alignment and the areas that need improvement with view to achieving the vision of a fully interoperable joint network enabled NATO C4I capability that enables decision superiority to achieve the desired effect. Since then, the evolution of sensor technologies has allowed to integrate plenty of further sub-systems into C4I capabilities.

Virtually anything can serve as a sensor and a source of data. There has been a vast explosion of sensors to include Open Source ISR. The rapid acceleration and hybridization of security operations has challenged national actors and international alliances to seek interagency and comprehensive approaches. Building on capable interoperable systems has become imminent. Well-orchestrated, interoperable, multiple services and countries employing network-enabled capabilities in a comprehensive approach to operations – this is the requirement and the trend in modern security operations.

Advanced sensors capture the full spectrum of intelligence signals. They can send full-motion streaming video, day and night. While sensor capabilities grow rapidly, they also get smaller. Ever more of them fit on a single

[3] European Commission. FAQ: Joint Framework on countering hybrid threats. Brussels 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

platform. Sensors fly on unmanned aerial vehicles, aircraft and satellites, ride on ships, submarines and land vehicles, or sit on the helmet of soldiers. Geospatial Information Systems, mobile and handheld devices, sensors in the Internet of Things, the convergences between Cyber and Electronic Warfare, as well as between kinetic and non-kinetic fires – the amount, velocity, and content of information produced via 24/7 news cycles and social media is nearly overwhelming.

To this end C4I and cyber security systems are aiming at providing

- Real time data, tactical communication and advanced battle management systems;
- Superior intelligence and surveillance systems for tracking opponent's activity;
- A broad spectrum of technologies that enables to manage a wide array of integrated ground, maritime, air and cyber forces, but also adds significantly to general security, coast guards, civil defence, and crisis management organizations;
- Situational awareness to senior decision-makers and commanders to plan, manage, and follow through operations even in tough times and under harsh circumstances such as wars, disasters and emergencies.

4. Getting there

Sharing of equipment, data and resources using an interoperable C4I infrastructure becomes prerequisite for operational success. Two initiatives have been fundamental to getting there.

a. MAJIIC

With the Multi-intelligence All-source Joint ISR Interoperability Coalition (MAJIIC) and the Battlefield Information Collection and Exploitation Systems (BICES) nations launched a project series that significantly boosted the Alliance's ability to tackle new challenges such as terrorism and piracy by rapidly sharing imagery and other information from intelligence, surveillance and reconnaissance assets.[4] Under the program, standards and technologies were developed that allowed NATO commanders to instantly tap into real-time data from several NATO and national systems. With MAJIIC NATO became able to deploy a wide array of air, ground and space surveillance assets, from different countries, and to them provide commanders with a single, coherent and detailed picture of what's happening on the ground thus breaking down former stovepipes in intelligence and surveillance systems.

In September 2007, MAJIIC had its first full-blown test of powerful new surveillance and reconnaissance technologies that soon could be deployed to Afghanistan. During a major NATO exercise in Norway it demonstrated impressive capabilities to include real-time manoeuvres by several thousand air and ground forces. At one instant, a commander could instantly access imagery from another Nation's UAVs, meaning that he did not have to deploy one of his own multi-million assets. Similarly, because the data is labelled, stored and shared across the coalition, national intelligence analysts could have far more useful material at their disposal. This has significant benefits in the fight against IEDs, or drug and arms smuggling through so-called "pattern of life" analysis. Particularly notable have been MAJIIC2's development of technical and procedural standards regarding the processes for Information Requirements Management and Collection Management and the technical

[4] Robert Murray. How NATO makes the Unknown known. JAPCC Journal ED 22. Kalkar 2016, pg. 14 - 15.

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

underpinning of the Coalition Shared Database[5] (CSD) servers.

Three particular lessons have emerged from MAJIIC:

- Services & Information Modelling can be used to define operational processes and procedures;
- Business Process Modelling drives clarity through discussion leads to a traceable, reconfigurable model of Mission;
- Modern, Open Architectures & Legacy systems can co-exist.

b. Unified Vision

Building on the MAJIIC achievements the trials of the Unified Vision series took NATO´s C4I capabilities to a new level.[6] These technical trials take place every two years to assess and demonstrate progress on the Alliance's JISR capabilities in a real-world environment. For example Unified Vision 2014, the biggest ever trial for JISR systems, 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 receiving ISR data from these platforms and sensors 'fused' intelligence products from the 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. Then in 2015, two major exercises – Steadfast Cobalt and Trident Juncture – validated the operational effectiveness of Joint ISR and paved the way for the Initial Operational Capability for JISR within NATO.

Unified Vision 2016 (UV-16) particularly explored how data collected from individual national aircraft – plus the alliance's new unmanned air vehicle capability – can be better used during joint missions. Clearly the processing, exploitation and dissemination (PED) of data has become a key area of development for NATO. To this end, UV-16 has been looking towards federated PED among allies also testing the dissemination of joint intelligence, surveillance and reconnaissance data.

At present NATO is planning Unified Vision 2018. Emphasis needs to be given to further testing the concept of a global federated PED process. With view to the boosting hybrid threats some targets must be hit in a matter of minutes or even seconds. Consequently, ISR is challenged to succeed within the context of time-critical respectively time-sensitive targeting. To this point, the given lack of appropriate doctrine has been hampering PED across national and geographic boundaries. This needs to be overcome based on lessons learned from Unified Vision 2018. Additionally, the issue of force protection will receive focus.

[5] CSDs are a type of digital organizational library that the Alliance can utilize to help process, exploit, disseminate and retrieve data throughout the NATO enterprise in a very rapid and efficient manner.
[6] NATO. NATO'S UNIFIED VISION 2014 Trial in Norway. Brussels. May 2014 - 28 May. 2014. https://www.nato.int/cps/en/natohq/photos_110396.htm and Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Deutsche Fähigkeiten für ein Joint ISR Cluster. Koblenz. April 2017. https://www-935.ibm.com/services/multimedia/160427_WhitePaper_Joint_ISR_Cluster.pdf

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

5. Key capabilities

Russia´s engagement in the Ukraine has been a wakeup call to the West. This development has led to a situation in Europe, where defence budgets are rising again. Consensus is that member nations maximize the value of their investments. With view to given hollow structures it is important that Allies increase their investments in defence. It is even more critical to invest in the right capabilities. The NATO Defense Planning Process is the primary means to identify the required capabilities and promote their timely and coherent development and acquisition by Allies. It is guided by NATO´s Strategic Concept and by operational requirements. The subsequent member nations´ political guidance aims at defining the number, scale and nature of the operations the Alliance should be able to conduct in the future and thus defines NATO's Level of Ambition. It also defines the qualitative capability requirements to support this ambition to include Allied Ground Surveillance (AGS), Joint Intelligence, Surveillance & Reconnaissance (JISR), Federated Mission Networking (FMN) and Cyber Operations.

a. Allied Ground Surveillance

With view to critical C4I capabilities Allied Ground Surveillance has a role. AGS provides an essential enabling capability for forces across the full spectrum of NATO's current and future operations and missions. Using advanced radar sensors, it will be able to continuously detect and track moving objects on or near the ground (i.e. tanks, trucks or helicopters) in all weather conditions and provide radar imagery of areas of interest on the ground and at sea.

The NATO AGS program uses the RQ-4 Global Hawk UAVs as a key asset for the alliance, like its shared AWACS capability. As of 2018 it will be a major contribution to NATO's Joint Intelligence, Surveillance & Reconnaissance capability. The AGS Core will be an integrated system consisting of air, ground and support segments. The air segment includes five Global Hawk aircraft.

A C4I grid that makes sense of what's happening and offers a range of effects, builds on sophisticated interaction with a sensor grid that sees what's happening and delivers tailored impact in all required domains – land, air, sea, space, cyber space to include the electromagnetic spectrum. Exploiting the opportunity of cross domain fires via shifting centres of gravity in a multi domain battle – this is tomorrow's challenge that needs to be prepared today. Here AGS is the elephant in the room.

b. Joint ISR

JISR functions as a cycle integrating 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] thus requiring extensive cross-community of interest coordination and interoperability. Joint ISR supports the coordinated collection, processing, and sharing within NATO of ISR material gathered by the future Alliance Ground Surveillance system, the current NATO Airborne Early Warning and Control Force (NAEW&C Force) and Allies' own ISR assets.

At the 2014 Wales summit NATO announced the establishment of a permanent 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. Thus, it recognized the fundamental importance of Joint Intelligence, Surveillance and Reconnaissance to NATO´s strategic preparedness and the

[7] NATO Communications and Information Agency. *Joint Intelligence, Surveillance and Reconnaissance.* Brussels 2017.

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

success of its operations and missions. To the military in NATO and the European Union ISR is considered as a *Joint* function and supposed to providing support to all involved military services. But, ISR is also vital for non-military operations as it provides information and intelligence to civilian decision makers, helping them make informed, timely and accurate decisions.

In early 2016, NATO defence ministers declared an initial operational JISR capability centred on enhancing the situational awareness of NATO's highest readiness forces. This initial operational capability was only the first milestone for the overall JISR initiative. Further work is ongoing to sustain these achievements and expand their scope. An enduring JISR capability is now being developed.

As over the next two years the Allied Ground Surveillance Core Capability becomes operational it will provide NATO with a collection and exploitation capability that will significantly boost C4I capabilities associated with Indication and Warning and Intelligence production. Of notably operational benefit has been already the expansion of NATO's Joint Intelligence, Surveillance & Reconnaissance capabilities into the maritime domain. Even small, targeted efforts have already disproportionately improved NATO's maritime situational awareness.

c. Federated Mission Networking

To this point the deliveries of Federated Mission Networking – i.e. a capability that aims to support command and control as well as decision-making in future operations through improved information-sharing – have been quite impressive. The FMN framework has become the centrepiece of ongoing work in NATO´s Connected Forces Initiative (CFI) that aims to enhance the high level of interconnectedness and interoperability NATO forces have achieved on operations and with partners. Its implementation strives for rapid interconnection within the Alliance, and with partners, in support of training, exercises and operations as well as day-to-day communications and activities. Exploiting technology to help deliver interoperability is a key component of CFI.

NATO´s Federated Mission Networking is based on the Afghanistan Mission Network lessons learned and the need for harmonized operational processes and scalable supporting systems for all future coalition missions. The objectives of FMN are to ensure consultation, command and control (C3) interoperability and readiness. Certainly, it underpins the Alliance's ability to connect its information systems and operate effectively together, including with partners, on training, exercises and operations.

d. Cyber

While Russia's 'little green men' are not necessarily different from earlier applications in unconventional warfare, their inclusion in multiple domains supported by expansive technology, social media, propaganda, and the malicious activity in the cyberspace[8] provides a far more complex problem-set than ever seen before. Today, NATO is getting positioned to anticipate this emergent phenomenon in conflicts and also innovate to leap ahead of new trends.

Cyber threats and attacks have become ever more common, sophisticated and damaging. State and non-state actors use cyber-attacks in the context of military operations or as part of hybrid warfare. With view to C4I, fast-rising cyber security threats need to be noted that can exploit vulnerable integration points and other weaknesses in systems that have been integrated after they have been developed and deployed. As NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks NATO needs to be

[8] Cyber has been declared as a domain at NATO's Warsaw Summit in July 20116.

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

prepared to defend its networks and operational capabilities against the growing sophistication of the cyber threats and attacks it faces.

Already at the Wales Summit in September 2014 NATO has adopted an enhanced policy and action plan to keep pace with the rapidly changing threat landscape. Yet, this has not become a truly comprehensive approach as it focused predominantly on building and maintaining a robust cyber defence – i.e. activities seeking via the use of cyber space to detect, analyse, mitigate and prevent vulnerabilities in order to protect computers, electronic information and/or digital networks. In between, NATO has learned that this is not enough. Not only defensive, but also offensive capabilities are required.

NATO has recently announced the establishment of a cyber operations centre. Defense ministers strive to integrate cyber into all NATO planning and operations to become just as effective in the cyber domain, as NATO is in air, on land and at sea.[9] The cyber operations centre could take on a role of a NATO special operations headquarters, include NATO-owned offensive capability, become a clearinghouse for coordination of nationally-owned offensive capabilities and serve as a pool of operational and tactical cyber expertise.

NATO also works with, among others, the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE). The Alliance's cooperation with other international organisations is complementary and avoids unnecessary duplication of effort. The EU and NATO have developed a shared interest in becoming more cyber resilient. Coordinating on cyber security and defence will facilitate the protection of critical networks. Recently, NATO and the EU have been cooperating more closely in this area than ever – sharing information between cyber crisis response teams, exchanging best practices, policy updates and working together on training, education and exercises. NATO's Cyber Defence Pledge and the implementation of the EU's Network and Information Security Directive have been reflecting this already. This increasingly coordinated effort is helping both organizations to better defend against cyber-attacks and enhance their resilience, which is critical to counter hybrid threats.

The private sector is a key player in cyber space, and technological innovations and expertise from the private sector are crucial to enable NATO and Allied countries to mount an effective cyber defence. Through the NATO Industry Cyber Partnership NATO and its Allies are working to reinforce their relationships with industry. This partnership relies on existing structures and includes NATO entities, national Computer Emergency Response Teams and NATO member countries' industry representatives. Information-sharing activities, exercises, training and education, and multinational Smart Defence projects are just a few examples of areas in which NATO and industry have been working together.

6. Integrated

The level of integration and interoperability across commands, service branches and agencies, weapons systems and forces, between nations and the private sector, is already high. Further integration will take place. Cyber has become a critical factor. Increasingly autonomous technologies are used to support and augment human capabilities in all domains of operational art. Advances in robotics, artificial intelligence, human-machine interfaces and sensors introduce the possibility to network intelligent, autonomous systems and human operators in multi-domain Battle Management Networks. The integration of intelligent and autonomous software, hardware and even weapon systems in complex security operations offers new operational

[9] NATO. Defence Ministers agree to upgrade NATO Command Structure. Brussels 08 Nov. 2017. https://www.nato.int/cps/en/natohq/news_148419.htm?selectedLocale=en

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

capabilities. At the same time, it challenges the classical military bureaucracies and its traditional decision-making processes.

This very development will boost the performance of emerging C4I. Yet, also the requirements grow as C4I systems need to share and analyse large stores of sensor and intelligence data, quickly and easily, using secure, interoperable networks and communications. Consequently, NATO respectively European Union member nations need to enhance the interoperability of their C4I capabilities to include those of different generational and technical levels through common doctrine, procedures and standards. They need an advanced, robust and modern C4I that generates actionable battle space information, timely response and reliable indication & warning.

Military and non-military security forces need a customised C4I system in which individual pieces are designed as part of an integrated system from the start.[10] Integrating C4I requires each new system to be conceived from the beginning with an eye toward its interdependent role in the larger C4I ecosystem as it will interoperate with a wide range of mutually supporting C4I systems. Integration needs to be organic to

- facilitate the interoperability of emerging technologies throughout a system's lifecycle,
- strengthen security, and
- ensure operator involvement to validate systems meet operational requirements.

Operational knowledge and experience is required when designing new systems and upgrading existing systems to ensure that C4I solutions are user friendly and tailored to battlespace realities. Engineering and technical skills are needed to ensure that architectures and processes are well architected to enable interoperability among systems, as well as to allow emerging technologies to plug into developing and existing systems. That kind of integrated C4I will certainly affect leadership concepts and service cultures.

Clearly, preparing for the 2018 NATO summit the Alliance is committed to developing superior C4I capabilities – capabilities urgently needed to address not only the challenge of combat in wide-open spaces, against high-signature military targets such as armoured vehicles, extensive military infrastructure, surface to air missile sites and radar systems, but also low-signature guerrilla forces and terrorists deeply embedded within the civilian surroundings. C4I has become an indispensable pillar of an effective defence as it provides critical information in a timely manner that enables political leaders, and civilian as military decision makers to see and understand an attacker's actions. The road towards integrated C4I leads to operational excellence.

***

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

This paper was presented in a key note at the opening of *The 2nd International Conference on C4I Solutions 2017* at the King Saud University in Riyadh, Saudi Arabia, Oct 17-19, 2017 on the "NATO experience building C4I capabilities in a broad Alliance".

[10] Greg Wenzel, Steve Soules, Trey Obering. Integrated C4ISR. 2015. https://www.boozallen.com/d/insight/publication/integrated-c4isr.html

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 President of EuroDefense Germany, 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 also a member of the ISPSW Speaker Management Team. Further information at ISPSW website: http://www.ispsw.com/en/speaker-management/


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