Towards Comprehensive Capabilities

Ralph D. Thiele

September 2013

ANALYSIS

I Introduction

The Asia/Pacific region is confronted with the same new global threats as the rest of mankind, i.e. climate change, scarcity of resources, migration, terrorism, health risks and environmental hazards. Asia and Europe together should strive for common comprehensive capabilities to meet the challenges ahead. In the future, decision-making processes will rely on an even closer integration of political, military, economic, humanitarian, policing and intelligence instruments for conflict prevention and crisis management. This integration 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 national level and, in particular, across borders – necessary in view of the changed security situation. Getting to respective capabilities though requires a challenging change management addressing people and their mindsets, organization – i.e. processes and architecture – and last but not least technology, where situational awareness has gained a key function in order to generate actionable knowledge.

II Comprehensive Avenues

The time has come to make the comprehensive approach work – not only for the European Union and NATO, but also beyond.[1] The comprehensive approach has an added value for everyone involved. The underpinning logic – the distinctive civil-military approach to crisis management – has already proven its validity. Asia and Europe together should strive for common comprehensive capabilities to meet the challenges ahead.

When the Berlin Wall fell the world began to change. The end oft he Cold War meant to Europe the beginning of a new era of integration and joint development as attested to by the enlargement of the European Union and NATO. Meanwhile the geopolitical point of gravity has been shifting towards the Asia/Pacific region. Europe's Asian/Pacific partners are fully aware of the interconnectedness of European and Asian security. Not only is their security precarious – there are some regions where political stability is fragile. The Asia/Pacific region is confronted with the same new global threats as the rest of mankind, i.e. climate change, scarcity of resources, migration, terrorism, health risks and environmental hazards.

[1] Ralph Thiele, "Europe's Security Policy – A long-term, comprehensive Perspective," in: *Comprehensive Security in the Asia-Pacific Region*, ed. Hari Singh and Colin Dürkop (Seoul: Konrad Adenauer Stiftung, 2010)

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 the early 21st century the world is characterized by uncertainties and vulnerabilities. The geometry of global power is becoming more distributed and diffuses while the challenges to security have become more complex and crosscutting. Political and technological changes are allowing huge numbers of people around the world to influence events as never before. New actors are reshaping the international security environment. Maintaining and building alliances, partnerships and coalitions across the oceans for common action has become both – more complicated and more important.

A fragile network of values, connections, and infrastructure defines the security of developed societies. It is not possible anymore to clearly classify them and very difficult to limit them – both in terms of quality and geography. Dangers threaten completely different areas like health, the ecological balance, or the peaceful coexistence of social groups. Factors like organised crime, illegal immigration, social and economic underdevelopment, lack of democratic institutions and respect for human rights, failed States, ineffective multilateral institutions, ecological problems, climate change etc. have come to the fore. These constitute the underlying causes of terrorism or of armed conflict between or within third states, or have the potential to intrinsically affect the values and interests of nations – factors that are much more difficult to grasp than the previous clearly identifiable threat. The number of international players – governmental and non-governmental, legal and illegal – has increased too. Security has become a multidimensional concept with a focus on dialogue, cooperation and partnership.

The background to this development is globalisation. Interdependency at the global level has proven to be much more than just economic; it also has important political, cultural, ecological and security aspects. This interdependency implies that events anywhere in the world can have an immediate impact on a nations' security. Globalisation has become a source of tensions between those that benefit from it and those that suffer its negative effects. The common main task of the parties involved – both nationally and internationally – is to protect the interconnected societies and their values, such as democracy, respect for human rights and an effective international legal order.

Against this background, transnational developments and supraregional risks increasingly determine the action requirements. Means for an asymmetric conflict resolution are becoming the rule. Actors who do not have well-developed military capabilities at their disposal increasingly shift conflicts to difficult terrain like cities and the information space. Scientific and technological progresses as well as growing networks, globalization and the vulnerability of modern industrialized societies increase their chances of success. States have to find new answers as not only challenges in the area of security policy have changed considerably, but also technical possibilities for both attack and defence.

Within the EU, over the years, a distinctive European approach to security has emerged, which is characterized by a broad, multidimensional and comprehensive notion of security, which starts from the interdependence between all dimensions of security – political, socio-economic, ecologic, cultural and military – rather than just focusing on the latter; hence the need to set objectives and apply instruments in all of these fields. Thus, a comprehensive approach to security has become a particularly characteristic of EU policy with respect to neighbouring States, which it attempts to integrate in an encompassing network of relations. The Commission as an enhanced framework has promoted this approach for relations between the EU and even distant

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

neighbours like Mongolia.[2] This way the EU is striving to achieve a network of shared prosperity and values leading to in-depth economic integration, close political and cultural relations and a joint responsibility for conflict prevention.

NATO's new strategic concept[3] is in line with this approach as the comprehensive and cooperative approach to security has emerged as an important answer to the challenges of the 21st century. Crisis management and prevention must take the form of a combination of political, development-policy, police, in some cases cultural and, where necessary, military measures. A number of implicit strategic assumptions guide EU and NATO policy in this regard. Yet these assumptions need to be substantiated and policy areas need to be integrated in order to arrive at a framework for maximally consistent, coherent and effective foreign, security and defence policy including external action.

III Continued Adaption

The institutions that have guarded Europe's and North America's security during the 20th century were not designed with 21st century threats in mind. Tanks and bombers, ships and missiles are still necessary but no longer sufficient to keep people and societies, nations and alliances safe. The instruments of security policy must also include tools that protect cyber and energy networks, halt the proliferation of weapons of mass destruction, counter the threats of terrorism and destructive ideologies, in part by confronting the political, economic, and social conditions that give rise to such ideologies in the first place.

Holding on to traditional patterns of action without reflection is not a sustainable option against the background of possible damage. In the future, decision-making processes will rely on an even closer integration of political, military, economic, humanitarian, policing and intelligence instruments for conflict prevention and crisis management. This integration 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 national level and, in particular, across borders – necessary in view of the changed security situation.

A three-pronged approach will be required, with measures aimed at

- prevention,
- protection and an
- improvement in the performance of administrations, security, defence and rescue forces.

Building up structures and processes that reflect these tasks is of special importance; this also includes, for instance, setting up clear-cut responsibilities, exchange of information and common planning processes. Even more important, however, is the development of a culture of cooperation between civilian and military actors, between highly different authorities and organizations both nationally and internationally.

[2] European Commission, "Recommendation for a Council Decision Brussels", 2012, accessed October 3, 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0389:FIN:EN:PDF

[3] NATO Heads of State and Government, "Lisbon Summit Declaration. PR/CP(2010)0155," 2010, accessed October 3, 2012 http://www.nato.int/cps/en/natolive/official_texts_68828.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

In times of globalization, innovation, complexity and dynamism require a continued adaptation of security concepts. For example, looking at ground forces existing budget limits call for a balance between the reasonable use of efficient legacy systems – i.e. command and control systems, weapon systems, communication systems, IT systems, and logistic systems of the armed forces that have been in service for some time – on the one hand and new disruptive technologies – i.e. technological innovations, products, or services that are squeezing previously dominating technologies out of the market – on the other hand. Against this background, the overall performance within the system is becoming the decisive factor. Cooperation between users and suppliers, industry and research is not only to handle the complexity of modern system of system solutions, where individual system components, subsystems and/or so-called platforms interact synergistically, but also to optimize them. Therefore, new paths have to be trod.

In the past decade, the volatile environments in which civilian and military security actors operated has allowed senior leaders to ignore such requirements. Fearing reactions of constituencies, strategic communities, public opinion and not at least of employees has kept them from successfully implementing the comprehensive approach. In between change has become indispensable. Traditional toolboxes of states have fallen short of delivering sufficient impact to respond effectively and with adequate agility to the existing multifaceted challenges to security. In all developed industrialized states and beyond, intensifying globalization leads to ever-higher innovation frequencies. This means that former success is no guarantee for continued prosperity or security. This in turn eventually implies that new products and capabilities are being developed in ever-shorter periods of time. Successful organizations and enterprises, societies and states depend on their own courage to change their traditional behavior patterns, i.e. from the currently prevailing incremental innovation to structural innovation.

Solutions to this end very often conflict with the way of common thinking in administrations and industry, armed forces and security forces, and also with well-known, classical solutions. Yet, existing concepts and capabilities have not been capable of meeting the new challenges because:

- the converging tasks related to internal and external security demand a new security architecture;
- the sustainable cooperation of key actors from all societal areas needs to be designed in a purposeful manner;
- modern operational command and control is networked to a much higher degree in all security and business areas;
- decentralized command and control and the synchronization of elements that act autonomously become more and more important;[4]
- the spectrum, performance and types of intelligent sensors and effectors/instruments to be employed are expanding rapidly;
- requirements concerning information requirements, information management and information security are increasing significantly.

[4] David S. Albert and Richard E. Hayes, "Power to the Edge: Command and Control in the Information Age," 2003, accessed October 3, 2012, http://www.dodccrp.org/files/Alberts_Power.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

Implementing a comprehensive approach that meets such requirements begins with a vision and a plan. It ends – in best case – with a culture of active collaboration and transparency among those involved. Getting to respective capabilities though requires a challenging change management featuring the vision of the comprehensive approach as well as addressing people and their mindsets, organization – i.e. processes and architecture - and last but not least technology. Good communication is the biggest carrier of any proposed change.

a) Vision

The comprehensive approach as the principle vision of NATO, the European Union and their member states 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 respectively to terminate hostilities, restore order, commence reconstruction, and begin to address a conflict's root causes. 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, but – of course – also include contributions to reconstruction and stability building.
- Political instruments refer to the use of political power, in particular in the diplomatic arena cooperating with various actors, to influence an adversary or to create advantageous conditions.
- 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 instrument 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 (NGO).

b) People

Because security is inextricably bound to a society's daily political, economic and cultural values, technological innovation cannot fully contribute to security unless it focuses on the human being. Security from a social perspective has three major characteristics:

- it is about people – both as the source and the object of insecurity;
- it is about society – in the knowledge that some threats will target people's identity, culture, and way of life;
- it is about values – and which proactive and reactive measures can protect people while reflecting their values and way of life.

Certain risks cannot be planned for or avoided. Resilient societies are those whose citizens, infrastructures and organisations can face shocks and recover from them. This ability to reduce vulnerability, mitigate effects and recover quickly requires resilience at all levels of society. The cohesion of any society will depend heavily on the strength of its convictions and commitment to its institutions, culture and identity. In times of crisis this

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

requires that individuals work together, based on joint preparation and mutual trust, confidence and support. Such interaction is crucial to societal robustness and resilience.

c) Organization

It is of key importance that sustainable efficient and effective organizational structures and business processes underpin newly developed capabilities. Organizational design needs to define the structure, roles, skills and job descriptions of the instruments of the comprehensive approach. The process of design must be complementary with the objectives as organizational systems exist for only one purpose – to deliver the power of the organization's vision. Every element needs to be examined and designed to make sure that it is fit for purpose – to deliver the vision of the comprehensive approach. Structures and processes need to be shaped to enhancing interoperability, facilitating interaction and synergies in complex engagement spaces among very different organizations.

Structure, as shown on organization charts, needs to define the boundaries of authority and decision-making and to identify the key personnel responsibilities. Once vision and strategy, core work processes and key roles have been identified, the structure should be reviewed and, if necessary, redesigned in order to provide the required support. Within the comprehensive approach the organizational design of civil-military components needs to support:[5]

- command and control – interconnected complex of command and control, communications and information collection and processing as well as intelligence (C4ISR) at the disposal of the political, civilian and military leaders as well as an adequate, comprehensive logistical set-up for all task elements.
- rapid deployment – small modular task groups with a high command and control capability with emphasis on undercover special operations, surveillance, intelligence and cyber warfare, including the necessary situational awareness, access to land-, air- and sea-based active options as well as strategic-operational mobility. Reaction and adaptable forces – as recently has been reported[6] with regard to structural reforms in the British Army – will enable to respond in an emergency while also preparing for longer-term deployment.
- force multipliers and stand-off capabilities – land-, air- and sea-based active systems which ensure that decisions can be brought about in a stand-off manner with or without the support of the forward-based task elements.
- consolidation capabilities – militarily organized and armed police or similar units with components for nation-building, economic and social intervention as well as for countering international criminality/terrorism. These include experts from the areas of administration, social affairs, infrastructure, judiciary, civil defence etc. as well as possibly support from and cooperation with non-governmental organizations.

[5] Ralph Thiele, „Intervention und die Sicherheit zu Hause in Deutschland: Transformation der Sicherheitspolitik unter neuen Vorzeichen," in: *Weniger Souveränität – Mehr Sicherheit: Schutz der Heimat im Informationszeitalter und die Rolle der Streitkräfte*, ed. Heiko Borchert, (Hamburg: Mittler & Sohn, 2004), 95-115.
[6] Kim Sengupta, "Revealed: Plan to Split Army into Two Forces," *The Independent*, June 19, 2012.

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

Work processes need to describe how work gets accomplished within the organizations enabling a comprehensive approach to security. These would range from a few high-level cross-functional integrated core processes down to detailed processes and procedures in units, teams or even for individuals.

To this end, the Allied Command Operations Comprehensive Operations Planning Directive[7] (COPD), dated 25 Feb 2010 constitutes an important milestone. 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 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 analyzed i.e. through a system 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.

Within the COPD 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 of advice and decision making during the planning for and conduct of operations. 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.

d) Technology

Technology has always played a major role in shaping an organization's structure and processes, as well as being one of the major catalysts for organizational change. Until recently, innovation has been relatively slow and the need to adopt new technologies not particularly pressing. Thus, organizations could adopt it incrementally and find ways for it to complement organizational structures and processes by trial and error.

The revolution in the field of information and communication technologies has become part of a greater structural transformation process: high-performance networks and network connections, together with the data streams involved, form the basic infrastructure for a functionally linked global system. This revolution is also an essential factor for the competitiveness and productivity of countries, regions and enterprises all over the world as it introduces a new way of international work sharing. With the creation of a global village, a new communication reality is emerging where messages can be centralized and reception of these messages decentralized. Connection to the global communication system guarantees the participants an increase in importance. Non-participants are being marginalized.

[7] Geza Simon and Muzaffer Duzenli: "The comprehensive operations planning directive," *NRDC-ITA Magazine* 14 (2009), accessed October 3, 2012, http://www.nato.int/nrdc-it/magazine/2009/0914/0914g.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

The information revolution has also exacerbated the vulnerability of modern industrial states to asymmetric attacks. The enormous multiplier effects that are connected to the different uses of information make the state and society extremely dependent on such potentials, which are mostly interconnected. Even the smallest faults within the critical information-oriented infrastructure can have serious consequences. The functional capability of postmodern industrial states depends not least on well-protected databases and other facilities of the information infrastructure.

Telecommunication systems in particular, which are often also used by the military, need to operate without interferences. However, malfunctions can also affect other sensitive areas such as energy and water supply, traffic, public administration, industry, commerce, banks, insurances, the police, security and rescue services as well as political and military command and control on all levels. There are many ways to deliberately cause damage or disturbances with relatively little effort. Even individuals can seriously damage the critical infrastructure of a modern industrial state through deliberate attacks. Preparation and conduct of such attacks can hardly be detected. In information warfare, there are no warning times or advantages for the defender. Countermeasures have to be developed on the basis of anticipations; that is why they are, naturally, full of uncertainties.

As technological innovation in the engagement spaces of security has accelerated, organizations cannot afford to adopt new technology by trial and error or to learn gradually how to make new technology complement the rest of the organization. They must learn fast and the complementarity achieved must be superior to succeed. Technology needs to contribute accomplishing comprehensive missions more efficiently and effectively than in the past, and enable comprehensive avenues that were previously unthinkable. To this end, the accelerating rate of technological change in information technology, biotechnology, nanotechnology, robotics, alternatives to hydro-carbons, and socio-cognitive research requires close monitoring. The ongoing info-bio-nano-robo-hydro-cogno developments will seriously impact chances and risks with regard to making the comprehensive approach work. Consequently, trade and industry need to be well integrated in the development and maintenance of comprehensive capabilities, particularly as the vast majority of the critical infrastructure belongs to or is operated by this sector.

IV Situational Awareness

Situational awareness is the prerequisite of comprehensive security. The purpose of situational awareness is to generate actionable knowledge. Knowledge is the decisive resource of all social processes and social organizations. As society turns into a knowledge society, access to knowledge and the exchange of information are becoming more and more universal: for individuals, social groups, politically and economically relevant actors, states, and alliances. It is also in the fight against security challenges that knowledge becomes more and more important. Rapid changes and spreading biotechnology, for example, also enhance the ability of opposing actors to use biological weapons. Thus, knowledge diffusion and proliferation has become a core problem. Space is a perfect example of this. Due to the knowledge proliferation nowadays, smaller states, non-governmental actors or individuals are already able to use space at relatively low costs.

The comprehensive approach builds on a holistic analysis of the challenges that needs to be addressed. To get there, a system of systems analysis is required, taking account of the knowledge requirements of all stake-

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

holders. In any crisis situation, decision makers and actors must have correct, relevant information in time, in order to be effective. Situational awareness systems enable information integration through network-centric services. Having a good overview of the situation, being able to communicate with each other and use each other's resources can improve knowledge, behaviours, work procedures and skills.

- Imagine the power of being able to track the movements of staffs, convoys, and vehicles and automatically check for their safety and security as they move;
- With regard to sensitive cases, imagine being able to communicate, coordinate and collaborate in real time with globally dispersed decision makers and security actors;
- Imagine being able to upload in near real time videos and photos from operational locations and share a common relevant operational picture with all involved.

Emergencies and security challenges – regardless of their size – need a professional response including data, information, and accurate record keeping. S*ituational awareness* allows seeing wider, deeper and further than ever before. Due to Endsley's definition situational awareness is "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future".[8] The principles of situational awareness are based on

- *perception* of elements, relationships and structure in a given environment,
- *comprehension* of the real-time situation,
- *projection* and anticipation of possible outcomes into the future.

The historical situational awareness paradigm of perception, comprehension and projection is most familiar to military pilots engaged in training and combat based situations. In the recent years well-established situational awareness approaches have been extended to field troops navigating an operational theatre of small networks distributed across remote rural regions and inside challenging urban environments. They have also been embraced by crisis response teams seeking to create an information architecture for relaying real-time information across a temporarily disabled system.

In future situational awareness will contribute to cultivating decision makers capacity for increased awareness, mindfulness, and focus in an age of information distraction. It will force *learners* to expand their collection of inputs, selectively identify their filters used in synthesizing and sense-making. Furthermore, it will help to mainstream system thinking and the imperative of understanding structure, relationships and feedback loops in a globally interdependent world.

Much of this is occurring already today in a broad scope of applications. For example IBM's vision of a Smart City[9] has become a viable concept in Moscow, Amsterdam, Dubai and many other places in the world with tremendous dynamics. As an increasingly instrumented, inter-connected, and intelligent urban system, it has been focusing on positive impacts of Information Communication Technologies on the efficiency and effec-

[8] M.R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors* 37 (1995): 32–64.
[9] Susanne Dirks und Constantin Gurdgiev and Mary Keeling, "Smarter cities for smarter growth. How cities can optimize their systems to the talent-based economy," 2010, accessed October 3, 2012, http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03348usen/GBE03348USEN.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

tiveness of healthcare and security, power and transport, and the practice of commerce and work. The Smart City is viewed as a 'system of systems' with the city realizing benefits through integration and coherence amongst its systems. It is addressing urban performance as a function of the complex interplay between systems composed of infrastructures, capital, assets, behaviours, and cultures, addressing the economic, social, technological, political, and environmental spheres. Particularly situational awareness is important for a smart city as the addressed potentials can only be mobilized, if inhabitants, companies or the administration are aware of the cities' position, knowing the city from the inside but also being aware of the surroundings – including global networks – and the system of cities the city is located in.

Exactly this is the challenge in the security and crisis prevention/management context. Key actors need to be analyzed and understood from various perspectives, with particular attention paid to political, military, economic and social, information and infrastructure aspects. Consequently holistic approaches addressing issues such as border security, maritime domain security and the protection of critical infrastructure or disaster relief operations as the Haiti earthquake[10] in 2010 with its catastrophic magnitude. All of these concepts build on system of systems analysis and situational awareness as core functions to manage complex, dynamic and time critical challenges, i.e. in Brazil[11], in Qatar, in Saudi Arabia and Singapore.

For an inter-agency approach to work it must draw together the strengths of the relevant organizations involved in addressing security issues. Much expertise is resident within NGOs. Numerous governmental, military and business organizations already possess valuable inputs into shared situational awareness. These are particular valuable resources when it comes to design action and effects, methods for assessments and interpreting results. Often civilian agencies have presence in crises regions prior to military engagement. They provide continuity during transitions and are focused on long-term solutions. However, no source captures all of the information needed or currently available. In better use of limited resources to address the omnipresent, multi-national security challenges the output would be most valuable for governments, international organizations and the commercial sector as well. The information exchange between these actors, in particular, sharing common databases, is the real power behind situational awareness.[12]

Situational awareness systems have the potential of integrating a wide range of emerging disruptive technologies that include: low cost sensors, IT networks, video, robotic vision, gaming, 3D/geospatial modelling, physical and virtual augmentation, autonomous systems, simulation software, location based service, social web *life streams,* and expert software learning systems. Situational awareness will be generated via platforms, sensors, links, data & sensor fusion, change detection, decision support tools, open source intelligence, knowledge development and C4ISTAR facilities.

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. Lessons learned from many contingencies suggest that some capabilities for each of these missions have much in common, particularly with respect to interoperability and information sharing. Some capabilities for compre-

[10] Kerren Hedlund, "Strengthen in Numbers. A Review of NGO Coordination in the Field – Case Study Haiti 2010," 2010, accessed October 3, 2012, http://www.icva.ch/doc00004599.pdf.
[11] Reuters, "Reuters Report: Brazil to spend $6 bln on border controls," 2011, accessed October 3, 2012, http://www.reuters.com/article/2011/01/09/brazil-borders-idUSN0920148520110109.
[12] Allied Command Transformation, "Maritime Situational awareness, Norfolk. North Atlantic Treaty Organization," 2012, accessed October 3, 2012, https://transnet.act.nato.int/WISE/BRITE/Trifoldsfo/MaritimeSi/file/_WFS/MSA%20Tri-fold.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

hensive approach situations can be developed quickly. Building these capabilities might cost much less than expected by many, partly because of the vast development of commercial capabilities that can be leveraged.

The utility of the common knowledge base depends upon the ability to practically share data in a timely manner – based on a network of governmental and non-governmental expert knowledge and instruments. 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. A role-based approach, rules and workflow modeling 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 are looking at different situational pictures, but all look into the same situation with a common shared situational awareness.

Shared situational awareness 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.

Situational awareness also benefits private industry. A multinational situational awareness program – preferably within the context of NATO and EU – would allow for a plenitude of national and international security, research and business initiatives and foster broad participation of large, medium-sized and even small-sized companies in a transatlantic collaborative approach. As it focuses on optimization at the systems level versus the platform level, it does not favor any particular technology or platform. It enables trades of risk, cost and capability, and it opens competition at multiple work levels, giving small and large companies from around the world equal opportunity to compete. In doing so, it encourages, indeed demands, best of industry solutions and innovation.

V Civil-Military Teamwork

At the very core of comprehensive capabilities is the teamwork of military and civilian capabilities. Both of these distinct but related asset pools are indispensable for successful effects based operations within an overall comprehensive approach to security. Armed forces are not the only – often not even the most important – security instrument available to the state. In the past, society was mobilized in order to support the military in case of attack. Today, it is the other way round: the armed forces are part of the forces a community uses to react to attacks. In the field of internal security and hazard prevention, it is the police, the fire brigade, disaster control and other first responders that are mainly required. There is no doubt, however, that the manifold capabilities armed forces have at hand – partly as the only organization with these capabilities – should become part of a comprehensive security system. This system must integrate all authorities responsible for public security, including the state and police, medical services, fire brigades, intelligence services etc.

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

Military forces will have two essential tasks in the future: One is to win a given conflict militarily in a rapid and decisive manner – even from a distance. The other is to consolidate the military success on the ground. Both tasks support the political purpose. There is no imperative sequence for them, so the focus of action between decision and consolidation can always shift in the course of an operation. Besides a small number of major nations, there will be few states left which are capable of waging an interstate war with any prospect of success. This is in stark contrast to the emergence of more and more new and non-governmental protagonists prepared to wage war. This is the rationale of warfare: While modern industrial states are interested in preventing war out of self-interest, there are states and non-governmental protagonists which use war as an economic or ideological factor leading to another cost-benefit calculation. Furthermore, cyber warfare offers the possibility to considerably affect especially those protagonists who depend on command and control systems and employ them hierarchically.

Military organizations at all levels must be able to conduct integrated military-civil missions, including through well-balanced organizational interfaces. This requires pre-established information sharing, comprehensive planning methods, role integration and ultimately operational support. While private contractors have been increasingly supporting military missions on the other side military support to civil agencies can be extensive. Generally it requires resources, including vehicles, shelter, communications, security, supplies, etc. in excess of the kit required by the military unit alone.

Civilian capabilities come mostly from national assets. These include capabilities such as interagency departments of member governments. Contractor support has also become a large factor in national support. If this is indeed to be the primary and most dependable source for embodiment of a comprehensive approach, there is reason to consider establishing a modest capacity to coordinate national contribution and planning efforts. Beyond governmental task forces of involved nations civilian support comes from a host of international organizations, both nongovernmental and multinational, many with specialized and highly desirable skills. Key organizational partners are the UN, OSCE, regional organizations or major NGOs such as the Red Cross.

Unfortunately, unlike military capabilities, civilian resources are rarely available and ready on the massive scale required for deployment to current crises. It can take considerable time to identify and deploy necessary civilian resources. Nations should consider organizing a standing civilian corps for international crisis response. Merely compiling a list of volunteers and skills is not sufficient. These resources should be afforded specialized education and exercise opportunities that expose them to the operational environment they will have to manage.

In consolidation missions, where the military and civilians will integrate closely, the challenge is in particular to

- provide a secure environment for the conduct of civilian stability operations,
- protect the victims of conflict as much as they seek to neutralize perpetrators of unlawful violence,
- provide both physical security and logistical support to deployed civilians, and
- conduct humanitarian or reconstruction operations.

Once consolidation becomes the primary mission, military commands must determine the military resources necessary to achieve initial stability and the return of essential services in the immediate wake of military operations. These are assets such as military police, CIMIC (Civil Military Cooperation), construction engineers

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

and military medical personnel. These forces have the mission to move into areas in the wake of conflict and work with combat forces that are still securing the area. They must provide public security, temporary governance and the most basic of services. These forces must be culturally aware and accustomed to working with both traumatized populations and civilian actors, including NGOs that may already be in the conflict area.

All available instruments must be able to participate in a coordinated, integrated, sometimes even synchronized manner in a multinational framework. This requires establishing policies, technologies, and procedures to enable synergies among the very different actors. Joint pre-mission exercises and training are of particular importance to ensuring common understanding of the different organizations' approaches, cultures and objectives.

Military missions have expanded with the developing challenges to security – an ever-growing array of tasks, adding new to traditional missions: nation building, stabilizing fragile states, counterinsurgency, and strengthening the security capacities of other countries. The capabilities of civilian agencies have not kept pace, which have caused an imbalance in the tools of statecraft and a resultant inability to meet strategic objectives. For example, despite the European Union's claim to approach security comprehensively, it has until now primarily built military institutions, improved military planning, and generated military capabilities with the civilian institutional counterparts lagging behind and with relatively little attention devoted to civilian personnel and equipment. It has taken more than a decade since the launch of European Security and Defence Policy to recognize that this lopsided situation needs to be remedied.[13]

Any comprehensive approach in need of civil-military cooperation must address the justice, rule of law and governance sector. Without a systematic effort in this field, securing a sustainable transition to post-conflict development and reconstruction has proven to be extremely difficult. Critical to this is addressing the problem of organized crime that often fills the gaps in governance in the immediate aftermath of major combat. That requires specialized advanced intelligence planning and continued access to information both from international law enforcement and from local governments. In turn the military must be tied closely to the information flow on criminal activity and enforcement actions in their operational area. Another critical civilian task in crises resolution is police training. Here again, close coherence of civil and military efforts is key to operational effectiveness.

Just as many militaries have cultural differences, also each civilian organization has a unique culture. Operations in Afghanistan and Kosovo experienced hard communication stovepipes among organizations that proved difficult to breech. For civilian organizations working with a strong, large and ever-present military organization, individuality is important. NGOs are special organizations with cultures of strict impartiality that are essential to self-protection and effectiveness. The military should do nothing to compromise NGOs' impartiality. To break down barriers between military and civilian partners, integrated training, educating, exercising, and planning for military and civilian personnel who may be operating together is indispensable. Furthermore, the priority of sharing information laterally as well as vertically across the network has to be emphasized. With that in mind, organizations like NATO and EU should re-double their efforts to move beyond the current limited ad hoc arrangements, and take another step to ensure that the comprehensive approach initiative moves closer to a comprehensive capability.

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

VI Conclusion: Getting Started

The financial crisis hit Europe at a time when all countries have undergone major reductions in their force structures. It has put public budgets under additional severe pressure. The fact that the post cold war threat was significantly lower already had led to a continuous reduction in funds over the last two decades. Today, most European states are either in midst or even only in early stages of transforming their armed forces with the primary goal to increase the proportion of capable and sustainable forces that can be deployed in international operations.

Now, as security challenges broaden and resources shrink in the West the requirement for synergy-led partnerships both between states and across non-governmental organizations will grow. The strategic shift towards Asia/Pacific, but also the requirement to address new challenges such as cyber, ballistic missile defence, and space will require allocation of additional resources for security and defence. All these initiatives will have to be found within the given financial framework and will gradually consume a greater proportion of ever more scarce resources.

Countering Somali-based piracy in the Gulf of Aden has set an example how the EU – NATO – Asia/Pacific cooperation could evolve in future. 26 participating nations from the Asia/Pacific region, the Mediterranean, NATO and the EU have coordinated their operations in this mission under the Shared Awareness and De-confliction (SHADE) forum for maritime security, in 2012 with additional Chinese participation. Of course, the scope of cooperation needs to go far beyond piracy in the Gulf of Aden. Assuring access to the global commons, dealing with climate change and proliferation, managing the global economic crisis, building common situational awareness, developing international institutions and decision-making processes – there are plenty of challenges to security that require close and effective cooperation among nations.

Situational awareness needs to and should be instrumental in providing valid orientation to this process of dealing with globally connected security issues in a comprehensive fashion. Building situational awareness would constitute a systemic, networked response to symmetric and asymmetric, traditional and networked security challenges. As a mixing console it would support partners and allies collaborating effectively together thus supporting global and regional contributions to the issue of interconnected security which may take the form of international organizations and regimes, joint task forces, confidence building measures, peacekeeping and so forth. Situational awareness would bring together different types and generations of people, organizations and equipment through a common connector and promote a culture of information sharing. Inherent architectures, processes, and tools would provide for informed, responsive decisions in an interagency and international security environment that includes the services of government actors and private business.

EU, NATO and the Asia/Pacific nations have a responsibility in managing challenges to regional and global security through comprehensive capabilities. The future of international stability and security will largely depend on their ability and willingness to manage their respective growth without major conflicts and on their decision to share responsibility with regard to the challenges coming up.

***

[13] Margiet Drient, "The EU's Comprehensive Approach to Security. A Culture of Coordination," *Studia Diplomatixa* LXIV (2011), 5-7.

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

Remarks:

Opinions expressed in this contribution are those of the author.

This analysis has been published firstly in: KAS Journal on Contemporary Korean Affairs 1(2013)2, p. 45-68, ISBN 978-89-93324-53-2 93360.

About the Author of this Issue

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

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 enter-prises 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