Perspectives of ASEAN-European Security Cooperation

Ralph D. Thiele

June 2017

Summary

This and their consequences to include in future countering hybrid security challenges, resilience paper proposes expanding the significant role ASEAN has taken in dealing with crises, disasters building and cooperating on these issues with the European Union and NATO. To this end three key themes are recommended:

- Building persistence in resilience
- Engage partners
- Expanding networked education, experimentation and exercises

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 ever more 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 worked – in some cases for decades – in executive positions and have at their disposal 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. Hybrid Challenges

While more people have access to highly sophisticated technologies than ever, vulnerabilities and threats have grown, stress and shock have become permanent companions of security considerations. Hybrid security challenges have become one of the most prominent security challenges and consequently an important field of security cooperation in Europe. Coercive and subversive activity to confuse, complicate and hinder decision-making processes has increased. Elections have been influenced. During the ongoing migration crisis, we have seen elements of hybrid influencing by both state actors and non-state actors. Perpetrators of hybrid aggression have tried to radicalize vulnerable members of society as their proxy actors.

In particular Russia's employment of a sophisticated hybrid strategy in the Crimea and the Ukraine has been a wake-up call for EU and NATO member nations. It has clearly challenged Western nations and societies - to include governance and norms - despite their economic, technological, intelligence and military superiority. In the Crimea and the Ukraine „*hybrid warfare*" employed disinformation and deniable forces to maintain maximum ambiguity. Armed Forces helped to create political advantages operating via "*proxy*" non-governmental forces in the form of separatists. Throughout the operations Russia displayed the capacity to undermine and seriously weaken their adversary without crossing established thresholds that would trigger a military response. Russian investments, trade, and capital were employed to influence key economic and political elites. Media were involved to support anti-integration and pro-Russian political parties. Forging of links between Russian organised crime and local criminal elements were noticed, also the establishment of ties among religious institutions, exploitation of unresolved ethnic tensions and campaigns for „*minority rights*" and massive coordinated cyber strikes on selected targets.

Already before Russia the so called Islamic State emerged as a hybrid organisation following again the initial Hezbollah model - part terrorist network, part guerrilla army, part proto-state entity. Meanwhile Iran has developed a spectrum of hybrid skills, so have North Korea and China as well. Certainly, also ASEAN will have to deal with hybrid challenges.

As hybrid actors target the cohesion of societies, a society´s collective mind-set the values and principles of the attacked societies become challenged, their resolve weakened and consequently political objectives are abandoned or modified. While hybrid actors strive for producing large scale man-made disasters, they may also take advantage of natural disasters. Hybrid challenges to security have become a driver for national and regional security arrangements on a global scale. Their disruptive nature requires federated, integrated response to include resilience. Although countering hybrid threats is primarily a national responsibility, vulnerabilities to hybrid threats, however, do not limit themselves to national boundaries. They rather require a coordinated response beyond national and even regional levels. Cooperation based on lessons learned and sharing expertise will contribute to aligning national policies, doctrines and concepts.

2. ASEAN - *One Response*

The "Association of Southeast Asian Nations" (ASEAN) region is geographically located in one of the most disaster-prone areas of the world. The region is expected to experience larger movements of people between states or migration of people, increasingly rapid urbanization, strong economic growth, and changes in the natural

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 built-environments. These developments have been reinforcing the need to commonly respond to disasters through concerted national efforts and intensified regional and international co-operation.

At last year's Summit of the ASEAN Leaders and Head of *States of ten Member States signed a declaration on "*One ASEAN One Response: ASEAN responding to disasters as one in the region and outside the region". The objective is to strengthen existing cooperation and coordination mechanisms in responding to disasters to achieve faster response, mobilise greater resources and establish *stronger* coordination. The summit emphasized a shared commitment to maintaining and promoting peace, security and stability in the region.

Last year in November I had the privilege to participate in the 2016 ARDEX exercise – the ASEAN Regional Disaster Emergency Response Simulation - an exercise that has been taking place on a regular basis since 2005. My overall impression was that ASEAN has developed a sense and impressive capabilities for joint approaches in crises and disaster management. That asks for expanding the scope of cooperation to include countering hybrid challenges to security and building improved resilience against such threats.

ARDEX 2016 practiced, evaluated and reviewed the existing Standard Operating Procedure for Regional Standby Arrangements and Coordination of Joint Disaster Relief and Emergency Operations in terms of its facilitation of close and effective collaboration amongst ASEAN member states themselves and with relevant United Nations and international organizations to manage a massive national disaster. I have been thoroughly impressed by the high professional standards of participating nations, organisations and international bodies both

- with view to the well-coordinated political processes, but also
- with view to the practical capabilities of involved first responders their involved overseeing organisations

The Coordinating Centre for Humanitarian Assistance on disaster management – the so-called AHA Centre – has emerged in the past years as the primary ASEAN regional coordinating agency on disaster management and emergency response. In fact, it has already responded to more than 13 disasters in the region since its establishment on 17 November 2011.

The "One ASEAN One Response" vision aims at building upon the collective strength of all stakeholders in ASEAN in coming together when a natural disaster hits, including ASEAN Member States, Civil Society Organizations (CSOs), private sector, Red Cross and Red Crescent societies, ASEAN Dialogue Partners, international organizations, and other ASEAN partners. There are plenty of tools that have been established to

- strengthen ASEAN-Emergency Response,
- strengthen civil-military coordination procedures,
- improve ASEAN Disaster Monitoring and Response, and
- expanding Disaster Emergency Logistics System)

Mechanisms to continuously improve the regional arrangements for disaster relief and emergency response include also military entities such as the

- ASEAN Militaries Ready Group (AMRG),
- ASEAN Centre for Military Medicine (ACMM),
- adoption of ASEAN militaries' Logistic Support Framework, and the
- development of the Joint Operations and Coordination Centre of ASEAN (JOCCA).

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 this point, ASEAN has navigated well within the changing terrain of disaster management. It has learnt from the lessons of jointly responding to large scale disasters such as Typhoon Haiyan. The vision of a resilient ASEAN has been building on a whole-of-government and whole-of-society approach on disaster preparedness and response at the national level, and a cross-sectoral and cross-pillar approach at the regional level. Consequently, countering hybrid threats and promoting resilience building fit excellently into an enhanced ASEAN profile and could serve well as basis for ASEAN and Europe cooperation in security and defense.

3. European responses to hybrid threats

Building resilience includes territorial defense and border security. It concerns developing force structure and improving the defense capabilities to obtain efficient and affordable armed forces. Yet, with view to the nature of hybrid threats and the respective civil center of gravity a focus area has become strengthening the ability to withstand natural and man-made stresses and shocks thus asking for a kind of resilience that offers the creation of conditions that foster greater adaptability and innovation, and enhancing decentralisation, self-organisation and the emergence of adaptive behaviour.

As any successful hybrid attack on targets such as energy supply chains, transport could lead to serious economic or even societal disruption resilience aims at avoiding cascading failures among these critical infrastructure systems. The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by chemical, biological, radiological and nuclear agents. The intentional spreading of animal or plant diseases may seriously affect the food security and have major economic and social effects on crucial areas of the food chain.

The cyber space constitutes the most extreme form of this vulnerability. Broad reliance on cloud computing and big data has increased vulnerability to hybrid threats. Via the cyber space everything is connected to everything else: systems, machines, people. And everything can be damaged, disrupted or put out of service practically from anybody anywhere. Consequently, improving the resilience of communication and information systems is important. Industry needs to be involved. Public-Private Partnership on cyber security could improve protection and also ensure continued research and innovation.

Countering hybrid threats has become a European priority. In mid 2016, the European Commission and the High Representative adopted a Joint Framework to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries. This Joint Communication outlines actions designed to help counter hybrid threats and foster the resilience at the EU and national level, as well as partners.

Actions have been outlined to build resilience in areas such as cyber security, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. In each of these areas, implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation are critical initial steps. Further concrete actions have been put forward to reinforce these efforts. In particular, it is proposed to step up cooperation and coordination between the EU and NATO in common efforts to counter hybrid threats.

Consequently, resilience has become one of the pillars of the EU's Global Strategy. Since the Joint Framework in 2016, the European Union has created an European Union Hybrid Fusion Cell to analyze information on hybrid threats. The Union has also taken steps in strategic communication, protection of critical infrastructure, energy security and other fields, relevant to enhancing our resilience. An important next step is the establish-

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

ment of the European Centre of Excellence for Countering Hybrid Threats that is supposed to take on a major role in promoting strategic level understanding of hybrid influencing and developing European policies.

In December 2016, the European Union and NATO together encouraged their Member States and Allies to participate in the work of the newly established Centre of Excellence for Countering Hybrid Threats. This Centre will serve as a hub of subject matter expertise. It will contribute to a better understanding of hybrid threats and societies' vulnerabilities by analysis and studies. It will also contribute to develop preparedness and civil-military capabilities to counter hybrid threats.

The Centre will engage in strategic-level analysis, consulting and training, and promote cross-sectoral cooperation within thematical networks. The Centre could also serve as a platform for common tabletop exercises of the EU and NATO. The Centre will also have a role to play in bringing practitioners and researchers together to develop a clear conceptual framework for hybrid threats. Obviously, it should be networked and closely cooperate with other Centres of Excellence relevant to countering hybrid threats.

Countering hybrid threats is also a transatlantic priority. Just as the European Union also NATO has understood that only cooperation will enable them to come up with proper resilience. NATO has identified seven baseline requirements to be assessed:

- assured continuity of government and critical government services;
- resilient energy supplies;
- ability to deal effectively with the uncontrolled movement of people;
- resilient food and water resources;
- ability to deal with mass casualties;
- resilient communications systems; and finally
- resilient transportation systems.

A key aspect of resilience is to improve the cooperation with regional partners to enhance border surveillance, intelligence sharing and reconnaissance, improve the armed forces interoperability and foster resilience in the neighborhood. From the European Union and NATO perspective partner nations are key stakeholders. Several partner nations already have fallen victim of hybrid operations. Their experiences and lessons learned can help to better understand the advance and impact of hybrid tactics. Consequently, the European Union and NATO are investing to strengthen partner nations' national capacities in the fight against hybrid threats.[1] To me it appears to be advisable to extent this approach to partner organisations such as ASEAN.

Of particular importance for countering hybrid threats and strengthening resilience has become the cooperation with the private sector.[2] The military has become increasingly dependent on infrastructure and assets in the private sector. For example, today 90 per cent of NATO's supplies and logistics are moved by private companies and 75 per cent of the host nation support for NATO forces forward deployed on the territory of the eastern Allies comes from private sector contracts. A possible disruption of supply chains highlights the present over-reliance on "just-in-time" approaches which may pose grave implications for the military - and as well for

[1] European Union. „*Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy."* Brussels. June 2016. http://europa.eu/globalstrategy/en The European Union Global Strategy states to this end: „*It is in the interests of our citizens to invest in the resilience of states and societies to the east stretching into Central Asia, and to the south down to Central Africa."*

[2] Edward J. Harres. „*Towards a Fourth Offset Strategy*." Small Wars Journal. August 11 2016. http://www.thestrategybridge.com/the-bridge/2016/8/16/a-new-plan-using-complexity-in-the-modern-world

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 civilian population. Similar dependencies exist with view to critical resource and services such as fuel, power and food. Also, when facing distributed denial of service cyber-attacks against its outward-facing networks, military increasingly rely on cooperation from the telecoms sector and the internet security companies to filter and capture data, identify malware and provide extra bandwidth. More than that the private sector has become a key driver of change through technology and innovation. From data mining and drones to 3D printing and sensor systems, many of the most significant technology developments today have both civilian and military applications. ASEAN-European cooperation in countering hybrid challenges and strengthening resilience would thus have a perspective in promoting enhanced cooperation of the respective involved private business.

4. Recommendations

In sum, European Union, NATO and their member states have started getting their act together. Countering hybrid threats and strengthening resilience has the potential to become a rewarding theme for ASAEAN – European security cooperation to include defence.

Networking stakeholders and their respective capabilities is at the core of building resilience. It requires preparedness and a culture of risk awareness. Building resilience demands persistent interconnectedness between the civil, private and military sectors. The requirement is to establish knowledge transfer between key stakeholders; and develop actionable proposals on how multinational organizations such as ASEAN, EU and NATO can collaborate with the nations and other partners to build resilience.

Three key themes to enhancing resilience are recommended:

- **Building persistence in resilience**

  Nations, cities, organizations, and businesses should conduct a critical sensitivity analysis to assess their own strengths and vulnerabilities. An important first step by the nations is providing a realistic assessment of their progress towards achieving Baseline capabilities

- **Engage Partners**

  With view to the potential consequences of not successfully mitigating those vulnerabilities experts and partners are of interest as they may possess relevant knowledge and tools. Knowledge transfer amongst and between partners across all the sectors will provide solutions, especially where mutual trust and understanding have been engendered. To this end information sharing is key. Building trusted and mutually reinforcing relationships and partnerships will, in the long term, encourage transparency and develop a shared perception of relative threats, risks and opportunities.

- **Expanding education, experimentation and exercises**

  Education, experimentation and exercises are fundamental building blocks in achieving resilience. This develops shared awareness and helps better understand risks and required subsequent actions. Whilst educating individual citizens to comprehend the complexity and challenges of today can lead to a more resilient society, at the strategic level education, experimentation and exercises foster skills and shared awareness. Federated (online) education, experimentation and exercises bring together different actors, encourages shared learning, enabling them to embrace and harness different perspectives and realize potential benefits. Expanding education, experimentation, modelling and training is critical to test inter-

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

dependencies with the sectors and build mutual trust. Connectivity between the sectors enables modelling and simulation of risk and critical elements of resilience - the ability to resist and recover.

Resist entails enhancing preparedness and mitigating known risks, whilst recovery requires agility and responsiveness. Identifying, mitigating and managing risks are important factors in achieving resilience, but should not be viewed in isolation. Modelling and simulation could provide useful tools to quantify, potentially monetize and insure against risks. Cyber defense and information security should become core issues. This could include the development of cyber defense and cyber education projects. The collaboration could be expanded to reflect information security and protection of communication networks and infrastructure.

***

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

This paper was presented on the occasion of the joint conference at the 1st Germany-Indonesia Strategic Dialogue in Jakarta, 22-23 May 2017, organized by the office of the Konrad Adenauer Foundation (KAS) in Indonesia and the Centre for Strategic and International Studies (CSIS) in Jakarta.

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

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