7TH EAST ASIA SECURITY OUTLOOK

SEMINAR MONOGRAPH • 5 March 2015

SULTAN HAJI HASSANAL BOLKIAH
INSTITUTE OF DEFENCE AND STRATEGIC STUDIES
(SHHBIDSS)

EAST ASIA SECURITY OUTLOOK 2015

Edited by:

Research Division, SHHBIDSS

Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies
Brunei Darussalam

Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies

Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS) was formally formed in April 2007 as the Brunei Darussalam Ministry of Defence's Policy Research Institute. SHHBIDSS mission is to study, discuss and disseminate defence, security and strategic issues relevant to Brunei Darussalam and its surrounding environment.

SHHBIDSS invites internationally renowned academicians and practitioners to present and write on the different issues surrounding the East Asia Security Outlook. This publication is based on presentations delivered by SHHBIDSS's invited speakers on the 5 March 2015.

© Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies, 2009.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without prior permission from SHHBIDSS.

First published: *2017*
ISBN: *978-9997-36-69-3*

Printed and bound by:
Brunei Press Sdn Bhd, Brunei Darussalam

All correspondence should be addressed to:

Library and Publication Section
Support Services Division
Sultan Haji Hassanal Bolkiah
Institute of Defence and Strategic Studies
Ministry of Defence
Bolkiah Garrison
Bandar Seri Begawan BB3510
Negara Brunei Darussalam

Tel: +673 2386693
Fax: +673 2381424
Email: library.shhbidss@mindef.gov.bn

CONTENTS

Preface i
List of Acronyms ii

1. **Keynote Speech**
   Dato Seri Laila Jasa Tan Sri Rastam Mohammad Isa

2. **Prospects of Cooperation in Non-Traditional Security Threats**
   Dr. Alistair Cook

3. **Challenges and responses in Cybersecurity**
   Lieutenant Colonel (Retired) Sazali bin Sukardi

4. **Future High Technology Weaponary in East Asia: Strategic Drivers, Issues And Debates**
   Dr. Michael Raska

5. **Implications of Disruptive and/or New Technologies: Managing Potentially Disruptive Military Technologies in the Context of East Asian Security**
   James Hasik and Byron Callan

Contributors

Preface

This publication is the outcome of the 8th East Asia Security Outlook (EASO) seminar conducted on the 24 November 2015 by the Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS).

The East Asia Security Outlook Seminar in 2015 continues to look into trends that have an important bearing on the strategic and security environment of the region. The contributors in this publication have provided important insights and perspectives on the current security dynamics including major power strategic relations, managing maritime tensions in the South China Sea and Northeast Asia as well as emerging trends on violent extremism and terrorism. This year's EASO seminar also discussed on developments in preventive diplomacy initiatives and ASEAN's role in post 2015 as confidence builder and peace promoter, convener of dialogue and cooperation process as well as community builder.

SHHBIDSS would like to thank the contributors, its staff and all others who are involved in making our EASO this year a success.

Muhammad Shahrul Nizzam Umar
Director
Sultan Haji Hassanal Bolkiah
Institute of Defence and Strategic Studies

List of Acronyms

AADMER	ASEAN Agreement on Disaster Management and Emergency Response
ACDM	ASEAN Committee for Disaster Management
ADMM	ASEAN Defence Ministers' Meeting
AHA	ASEAN Coordinating Center for Humanitarian Assistance
ALNAP	Active Learning Network for Accountability and Performance
APCERT	Asia-Pacific Computer Emergency Response Team
APSC	ASEAN Political-Security Community
APT	Advanced Persistent Threats
ARF	ASEAN Regional Forum
ASB	Air-Sea Battle
ASEAN	Association of South East Asian Nations
ASEAN-ERAT	ASEAN Emergency Response Assessment Team
ASEAN-ISIS	ASEAN Institutes of Strategic and International Studies
A2/AD	Anti-Access and Area Denial
BDS	Beidou Defense System
BYOD	Bring Your Own Device
CALT	China Academy of Launch Technology
CBRN	Chemical Biological Radiological and Nuclear
CCIS	Command and Control Information System
CC2C	Changi Command and Control Centre
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CNSS	Compass Navigation Satellite System
CSCAP	Council for Security Cooperation in the Asia-Pacific
CSIRT	Computer Security Incident Response Team
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
DoD	Department of Defense
EU	European Union
GPS	Global Positioning System
HADR	Humanitarian Assistance and Disaster Relief
HCV	Hypersonic cruise vehicles
ICF	Inertial Confinement Fusion
ICRC	International Committee of the Red Crescent

ICT	Information Communications and Technology
IDRL	Guidelines for the Domestic Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance
IFE	Inertial Fusion Energy
IFRC	International Federation of the Red Cross
JAM-GC	Joint Access Maneuver in the Global Commons
JICA	Japan International Coordination Agency
JOAC	Joint operational Access Concept
MCDA	Military and Civil Defence Assistance
MLP	Medium to Long-Term Plan
MRAP	Mine Resistant Ambush Protected
NADI	Network of ASEAN Defence Institutions
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCA	Norwegian Church Aid
NEAT	Network of East Asian Think Tanks
NTS	Non-Traditional Security
NGO	Non Governmental Organization
NZDF	New Zealand Defence Force
OIC-CERT	Organization for Islamic Cooperation Computer Emergency Response Team
PLA	People's Liberation Army
PLAAF	People's Liberation Army Air Force
PLAN	People's Liberation Army Navy
RHCC	Regional Humanitarian Assistance and Disaster Relief Coordination Committee
RMA	Revolution in Military Affairs
RMB	Renminbi, unit of China's currency
R&D	Research and Development
SCS	South China Sea
SCADA	Supervisory Control and Data Analysis
SEED	Swift Emergency Evaluation Deployment
SLOC	Sea Lines of Communication
UN	United Nations
UNFPA	United Nations Populations Fund
UNHRD	United Nations Humanitarian Response Depot

UN OCHA	United Nations Office for the Coordination of Humanitarian Affairs
US	United States
USAF	United States Air Force
WFP	World Food Programme
WHO	World Health Organisation

Keynote Speech by Dato Seri Laila Jasa Rastam Mohd Isa
Chairman and Chief Executive
Institute of Strategic and International Studies (ISIS) Malaysia
at the 7th East Asia Security Outlook Seminar

Mr Shahrul Nizzam Umar
Director
Sultan Haji Hassanal Bolkiah Institute of Defence and Strategic Studies (SHHBIDSS),

Distinguished guests, ladies and gentlemen,

I would like to begin by expressing my sincere thanks and appreciation to Mr Shahrul Nizzam and SHHBIDSS for inviting me to speak at this seminar. It is always a pleasure for me, as a former diplomat and current head of a think tank, to interact with people who share a similar interest in issues relating to international relations, diplomacy, security and strategic studies.

I must commend the organisers on their choice of topics and speakers. The issues that have been identified are important and relevant to the current situation and changing dynamics not just in East Asia and the wider Asian region, but also all over the world. We are living in a world so interconnected that we cannot afford to ignore anything that happens anywhere in the world, without thinking of the possible implications and ramifications upon us. What happens in East Asia would be of interest and concern to others just as we would and should have an interest in events and developments occurring in other parts of the world.

We are now seeing a somewhat different global strategic scenario unfolding. The major power balance in the Asia-Pacific is undergoing a shift with the rise of China, albeit with the US pledging its commitment towards maintaining a continued presence in the region. Developments in Northeast Asia, the ASEAN region and the South China Sea, among others, have begun to pose major challenges to the regional architecture while at the same time presenting ample opportunities for countries in the region to forge wider and deeper cooperation on a plethora of issues, including the emerging non-traditional security issues.

The wide variety and increasing complexity of non-traditional security issues facing us would inevitably have an impact upon all of us in one way or another.

No country or region can afford to isolate itself from those issues and challenges. Examples are abundant, be they related to terrorism, extremism and militancy, pandemic diseases, cyber security or climate change. This then heightens the urgent need for efforts to be intensified to lessen tension, prevent conflict and increase cooperation among countries.

Another important issue that requires attention is the ongoing and future military expansion and modernisation programmes undertaken by various countries, in particular the impact of those programmes on the overall regional security situation. There are many related key issues and scenarios in this regard that could affect the regional security outlook over the next decade. These could be anything ranging from either positive or disconcerting developments in the South China Sea to possible deterioration of the situation in the Korean Peninsula.

The world has undergone a tremendous strategic shift in the last decade. The events in the Middle East, Europe and Asia attest to this. As we move forward, we find ourselves facing new problems and having to grapple with greater challenges. While some old problems persist, many have evolved into more difficult and complicated ones. The wonder of an initially successful venture into regional integration known as the European Union has run into a number of political and economic problems and now lost quite a bit of its appeal and glamour. The recent EU experience certainly has provided many lessons for others, in particular ASEAN which would soon declare itself as a community.

The move to democratise the countries in the Middle East and North Africa, beginning with the invasion of Iraq in 2003 has turned out to be much more than a walk in the park for everyone; the proponents and initiators, the key players, the rest of us who may be far away from the scene but would still feel the impact, and, most tragically, the hundreds of thousands of victims. It is undeniable that the situation has worsened. Indeed it has spawned new issues and bigger problems, not least being the rise of the Islamic State (IS), which has created another nightmare of different proportions, imposing a new dimension of security threat upon nations and societies, including ours.

New and emerging issues, once discussed as hypothetical "what ifs" and mere "probabilities", have now morphed into causes for concern for many. Such is the outlook for our world.

It is only natural that we should remain concerned over the traditional military-security issues. Therefore, the actions of the major powers, our neighbours and even others situated far away from us, related to defence and security, would raise

our curiosity and interest. Fortunately there are already in place various bilateral, regional and international structures and mechanisms that provide the avenues for countries to consult, discuss, clarify and forge cooperation. The architecture in East Asia is functioning well although it can be argued that it could be improved, such as in the case of the East Asia Summit.

The increasing number and intensity of non-traditional security issues such as transnational crime, terrorism, cyber security threats, disaster relief, impact of climate change, resource security and public health epidemics and the threats they pose are increasingly becoming major security challenges to Asian states. East Asia has been, is and will be dealing with the fallout from the evolution of non-traditional security threats.

The last few years have seen the region having to deal with the adverse impact and significant damage brought about by natural disasters. If one looks further back, there was also the impact of SARS on the region. We are now confronted with the new threat of other pandemic diseases such as Ebola and MERS, which this region needs to be prepared for given the increased global connectivity. We cannot pretend to be immune from such threats. Thus the current efforts at promoting cooperation need to be intensified and we have to look into the prospects of greater cooperation and better coordination to effectively manage and counter those issues.

The question of cooperation in the face of non-traditional threats would necessarily present new challenges for the evolving regional security architecture. What are the issues than can be truly considered as non-traditional security threats and how do we respond to them? Do these threats warrant a similar response such as envisaged or planned for traditional security threats? How can the military and security forces adapt to respond to non-traditional threats while maintaining their main functions and traditional roles? While the state should play the leading role in responding to these threats, what could be the roles of other actors – international organisations, NGOs and even the private sector, and what would be the scope and limits of those roles? How do all these stakeholders cooperate in creating a proper balance among their various their roles and responsibilities? A good example to examine would be the still ongoing effort to find the missing MH370 aircraft. I am certain this seminar will be looking at these very questions and seek to find the appropriate answers.

The good news is that the need for better cooperation has long been recognized and that numerous multilateral fora already exist for security cooperation in East Asia. The ASEAN Regional Forum (ARF), ASEAN Defence Ministers Meeting (ADMM) and ADMM Plus and the East Asia Summit can and is being used to

build up a more effective basis for cooperation on an entire range of security challenges, including non-traditional ones. As I have mentioned earlier, there are other arrangements. All these complement one another. One major hurdle to overcome is the tendency for duplication, thus also giving rise to uneconomical use and deployment of resources which, we have to admit, cannot be completely eliminated. These efforts can be further bolstered by Track 2 security processes which can provide helpful policy advice and recommendations. In this regard, CSCAP, for example has played a useful role.

There is a growing awareness – and an increasing sense of urgency – that the worst-case forecasts for the region's non-traditional security environment will inevitably have a spillover effect into the traditional security areas. If these non-traditional challenges can be effectively and jointly addressed today, before they have a chance to evolve into more serious problems, it will not only lead to better management of such threats when they occur in the future. Indeed, it may even inspire solutions and innovative pathways for tackling some of the region's long-standing traditional security problems.

Terrorism continues to remain a clear and present danger to the world. We, in this region, are not immune from it. While there have been concerted efforts to deal with the scourge of terrorism, with varying degrees of success, the last couple of years have indicated a disconcerting evolution in the threat posed by terrorism.

As seen in the Middle East, North Africa, Nigeria and Europe, terrorists have increasingly set their eyes on soft targets and changed tactics so as to cause maximum carnage to advance their cause. They resort to challenging and taunting governments and societies through social media. Such an extraordinary situation would require extraordinary responses. The international community obviously has not been able to figure those out. But it has to be done and done fast, lest more young men and women will be attracted to the distorted and deviant ideologies if the likes of IS or Boko Haram.

As the world becomes ever more digitally connected, the cyber security threats faced by states, organisations and even individuals become more diverse, sophisticated and dangerous. Cyber security issues are increasingly relevant for not just developed large countries but also developing countries here in Asia. There is a need for third parties, especially specialist institutes and think tanks, working with governments, to push and seek answers to questions that would positively influence policy on cyber security.

Unfortunately, while cyber security has become more and more important in the realm of international security, there are still governments grappling with such issues as to what this exactly means and its impact on national and regional security and interests.

The situation gets murkier when it comes to the question of cyber warfare. There are different types of cyber-attacks – by individuals, groups and states on each other. The growing involvement of non-state actors in acts of cybercrime and cyber warfare further complicates matters. What are the criteria to regard one type of cyber-attack over another as an act of cyber warfare? Acts carried out in cyber space could see repercussions in the physical world – leading to serious consequences. In Europe, some states are beginning to discuss, both internally and internationally, what would constitute an "armed attack" over cyberspace and what could the possible responses be.

There have already been public allegations by some states that rival states have used their cyber capabilities to intimidate states and organisations, conduct espionage or even unleash viruses designed to cripple certain systems. Some analysts have even speculated that we are heading into an era of a 'cyber Cold War' where the playing field in cyberspace is more levelled between states than in the real world. In dealing with the challenges and responses of cyber security, public-private partnerships remain at the core of good cyber security practice and the development of cyber defence capabilities. Hence, there is the obvious need for cooperation. The flow of information must go both ways blurring traditional approaches to matters of national security. This is something that both governments and their partners must learn to work out. Additionally, the time has also come to move towards transparent regional dialogues involving all stakeholders in the Asian region – perhaps through the ARF or EAS – on establishing international norms for cyberspace and cooperation in cyber confidence-building measures.

For decades, the military establishments in Asia, especially Southeast Asia, have focused on domestic insurgencies, border security and, in some cases, maintaining political control. In such threat scenarios, large land armies were the principal requirement. These days however, governments in the region are increasingly concerned about securing air and sea space so that they can exercise sovereignty over marine and seabed resources, contest overlapping claims and monitor the movement of vessels. Hence the increase of investment in naval and air power has become something that has come to characterise Asian defence planning over the last decade.

As longstanding sovereignty disputes flare up, regional states are increasingly focusing their defence spending on newer, more high tech platforms in order to gain an edge over a competitor. This has led to assessments of the growing number and quality of capabilities like submarines, armed drones and anti-ship cruise missiles in East Asia. For the major powers, these assessments extend to the development of anti-ballistic missile systems and satellite- destroying capabilities.

Some regional navies are building large "flat-top" ships that can carry anti-submarine helicopters or quickly land troops on outlying islands or oil platforms. Japan has set the trend. South Korea, Australia and even Singapore are following suite. Several regional states are also acquiring fifth-generation fighter planes with flight-and weapons-control characteristics far in advance of any military aircraft in service. The introduction of these fighters will be a game changer in the region.

As part of the US "rebalance to Asia," there have been reports that US forces stationed in the Pacific theatre will get the newest weapons systems first. As it stands, the US is giving out ambiguous signals about deploying its advanced Terminal High Altitude Area Defence (Thaad) batteries to South Korea. This has ruffled feathers in Beijing with China indicating its unhappiness over the potential move.

For its part, China is also investing heavily in the development and purchase of anti-ship missiles, stealth fighter jets, hypersonic vehicles and other high-tech weaponry. Latest reports seem to indicate that China may be prepared to increase its defence budget by ten percent this year.

While it is understandable for states to continue to invest in defensive military capabilities, the impact of the rapid introduction of such high tech weaponry in East Asia and beyond needs to be carefully examined. Are the introduction of such weapons and platforms even warranted? Do such weapons and platforms further destabilise the region, instead of stabilising existing conflicts?

When discussing the impact of high-tech weaponry in East Asia, it is inescapable for us to mention the contesting claims in the South China Sea. For the most part, the capabilities that have been brought to bear by the various claimants have been decidedly low-tech. Even at the height of the HD-981 oil-rig standoff between China and Vietnam in 2014, both sides can be said to have shown a degree of restraint. Neither side sought to deploy their latest air and naval capabilities, preferring to mostly use their maritime law-enforcement vessels instead. In short, there seemed to be an implicit recognition by both sides to avoid crossing a certain threshold in the use of high-tech military equipment.

But how certain can we be, that a dangerous escalation can always be avoided? The construction and reclamation activities in the South China Sea present a challenge in this regard. These man-made islands can potentially allow some of the claimants to station their forces on a more persistent basis in or near areas where there are competing claims. In turn, this could encourage an action-reaction dynamic, which may well include the introduction of more lethal military platforms in these areas, including land-based anti-ship cruise missiles. It took nine years of negotiation for ASEAN and China to agree on the Guidelines on the Implementation of the DOC in the South China Sea in 2011. Yet, it has taken less than a year for China to transform Fiery Cross Reef from a tiny maritime feature into an island that is about 3- kilometres long. There is therefore an urgent need for the diplomatic process to keep up with the strategic realities on the ground, which is changing day-by-day, month-by-month. The realisation of a COC in the South China Sea and an enhanced discussion between ASEAN and China on the overlapping claims need to be a matter of priority for all countries involved.

Before I conclude, ladies and gentlemen, let me to briefly mention the advent of new capabilities brought about by the social media revolution, which now allows information to be shared almost instantly with anyone who is connected. This brings in a new element of "the masses" into the relationship between states and how it impacts regional security. As we have seen in East and Southeast Asia, perceived diplomatic slights or disputes of sovereignty have gained traction of their own in the social media sphere with nationalists whipping up sentiments and sometimes, indirectly influencing governments to take a harder stance on diplomacy. How will such developments impact the regional security and diplomatic outlook? While some may be dismissive of such influence, one should never discount the impact and influence of social media in influencing both the citizenry and their leaders.

These, in a nutshell, are some of the issues, in my view, that the region will face moving forward. Are we currently equipped to face these issues and are we moving to prepare for them? Do we even recognise what the issues are and the impact that they will have in the region? Given the globalised world today and the important role that Asia plays in the world economy, it is unlikely that problems affecting this region can be contained here for long and vice versa. There is a need to address the challenges of non-traditional security and military expansion and modernisation, to cooperate in solving current issues and to prepare for foreseeable ones. This must be done with tact and foresight. We need to wage an intelligent struggle to identify and address these challenges.

PROSPECTS OF COOPERATION IN NON-TRADITIONAL SECURITY CHALLENGES: HUMANITARIAN ASSISTANCE AND DISASTER RELIEF IN THE ASIA-PACIFIC

Alistair D. B. Cook

Introduction

As 2014 drew to a close, the Philippines confronted Typhoon Hagupit when it made landfall on 4th-5th December. Initial reports made by the Joint Typhoon Warning Centre predicted it would reach the intensity of Typhoon Haiyan. Yet, while the devastating impact of Typhoon Haiyan in 2013 was averted, a reported 18 people were dead, 916 injured, close to one million displaced, and an estimated US$75 million in damages by mid-December 2014. As we reflect on Typhoon Haiyan and Typhoon Hagupit in the Philippines, it is important to assess the recent and several advances made in humanitarian assistance and disaster relief (HADR) and how better preparedness and awareness channeled limited resources to where they were needed. As the scale of Super Typhoon Haiyan became clear at the beginning of 2014 – killing 6,300 people, affecting 11 million people and costing an estimated US$10 billion – many lessons were observed as government agencies and militaries, international and regional organisations, non- governmental organisations, the Red Cross and Red Crescent Movement took stock of the international response. One year later, while Typhoon Hagupit was much less intense, the humanitarian response had improved with better warnings around storm surges, advanced placement of food stocks, managed evacuation and medical teams to minimise casualties.

These two super typhoons were not isolated incidents. Many communities across the Asia- Pacific face more frequent and larger disasters. The region is highly exposed to natural hazards such as storms, floods, drought, earthquakes, landslides, volcanic eruptions, wildfire, and epidemics. Indeed all these events account for 14% of the total number of worldwide disasters in the period 2001 – 2009 in ASEAN which is home to 9% of the global population or approximately 584 million people. Furthermore, the Asia – Pacific accounts for 40% of global casualties as a result of natural hazards, which means that countries in the region are disproportionately affected when the events occur.

Why is the Asia-Pacific to a disproportionate number of casualties as a result of natural hazards? How are countries and societies developing their responses in this region? What levels of cooperation occur across and between different levels

of government and non-government actors? What approaches are best suited to such scenarios? What role does technology have to play in HADR?

In addition to more extreme weather events is an increasingly diverse range of international humanitarian responders. One of the core challenges we face today is the absence of appropriate governance mechanisms to make sure efforts are not duplicated, harm is not done, and needs are met. The 1994 Oslo Guidelines are the foundational document, subsequently updated in 2003 as the MCDA Guidelines[1] to coordinate international humanitarian responses. Yet twenty years on since the Oslo Guidelines, there is a need to revisit the guidelines to reflect the current humanitarian landscape and establish an effective coordination and cooperation mechanism.

The challenge the global community faces today is how to formulate such an inclusive framework that draws on the strengths of different stakeholders. The Sphere standards[2] were designed to provide universal minimum standards for humanitarian assistance. However, these standards are criticised for their overly technical focus and saw some humanitarian responders withdraw from the project. Yet many civilian agencies and academics argue that they remain the most important benchmark for quality assurance in HADR.[3] The international humanitarian system is now a crowded field with a diversity and rising number of non-state actors in addition to traditional state actors like militaries and international organisations providing humanitarian assistance. As a result, there is a need for a revised, inclusive and comprehensive framework for humanitarian assistance and disaster relief in the Asia-Pacific as a site of frequent disasters and draws global attention and responses. Indeed, while some ASEAN member states are more vulnerable than others, disasters affect the whole ASEAN Community because these events influence the region's economic competitiveness, its food security, political stability, and quality of life.

Realising Change?

Today's humanitarian landscape sees non-state actors providing the majority of civilian assistance. Alongside NGOs, the UN and Red Cross account for a quarter of the response each, as calculated by the Active Learning Network for Accountability and Performance (ALNAP).[4] At the same time, the types of disasters communities and states face have diversified and some have collided to create complex humanitarian emergencies. There is an increasing risk of technological disasters including chemical, biological, radiological and nuclear (CBRN) hazards where countries adversely affected by financial crises are unwilling to replace or unable to maintain aging infrastructure or are built in harm's way of extreme

weather events, pre-existing social tensions or conflicts. Further, the international community faces a multitude of factors such as urbanisation, rapid population growth, climate change, and water shortages which impact how communities and states respond. In essence, non-traditional security threats have grown; the responses needed have become more complex but are faced with glacial changes in approach.

While the humanitarian landscape continues to evolve, it is essential that the principles of humanitarian assistance remain intact to ensure civilian protection but new modes of interacting have never been more pressing. The principles of neutrality, impartiality, independence and a commitment to humanity need to form the bedrock of humanitarian assistance the world over.[5] That is why in 2014 the United Nations Secretary-General Ban Ki- moon started an initiative to improve humanitarian action, which will culminate in the Global Humanitarian Summit in 2016. In the lead up to the world summit, the UN Secretary-General aims 'to build a more inclusive and diverse humanitarian system by bringing all key stakeholders together to share best practices and find innovative ways to make humanitarian action more effective'.[6] The 2016 summit will convene a space for the key actors to create pathways forward to address the humanitarian challenges related to natural hazards and conflicts.

Regional Organisations

Regional organisations are widely regarded as the 'building blocks' for global governance and constitutive parts of the global multilateral order.[7] At the 2005 World Summit of the United Nations, the membership of the global body attached a key role to regional and sub-regional organisations through General Assembly Resolution 60/1 for the management of global peace and security. The same year saw the highest level of national military involvement to a disaster scenario in the global response to the Pakistan earthquake. While a strong and well-equipped military response can bring benefits, the principles of humanitarianism are at odds with military culture. Resolving or reducing the tension between these two organising principles is key to building trust between civilian and military actors in HADR activities. Many relationships are built in the field in response to a particular event. In the 2005 Pakistan earthquake many practitioners noted that coordination and response had measurably improved since the Boxing Day Tsunami. However, it was not clear whether these lessons learnt were individual or institutional. Therefore a key area for improvement is building of institutional memory to ensure that lessons learnt from one HADR response to the next is not lost when personnel move on to new roles and responsibilities.

As the world becomes more aware of interconnectivity and the importance of the different levels that make up global system governance, regional organisations are increasingly observed to carry important weight in responding to issues of international peace and security. In the Asia-Pacific, the development of ASEAN albeit with its own constraints has supported further interaction amongst its members, and notably other partner countries to respond to a raft of policy issues. Many of these issues have been in non-traditional security as defined by Southeast Asian nation-states, as states need to respond to transnational security threats including disasters, pandemics and climate change. It is clear that with the saliency and transnational nature of non-traditional security issues such as pandemics, climate change, terrorism, and disasters today, regional organisations are understood as an avenue to overcome collective action problems when the slow pace of negotiations around global agreements are taken into account.

While the function and form of regional organisations have often been characterised by local norms, the emergence of non-traditional security issues as seen by policymakers has offered a new and clear-cut role for regional organisations. Some academics argue that cooperation on non-traditional security threats that lead to a wider array of initiatives at the regional level will compete and overcome apprehension and opposition to collective action over traditional security concerns such as territorial integrity, political independence and state sovereignty.[8] Cooperation has built trust and reduced tensions between countries on NTS issues yet it remains unclear whether cooperation on HADR for example will trickle into other issue areas or if it is an end in itself.

The explicit policy recognition of security threats beyond interstate warfare has a longer history in Southeast Asia. Prior to the Asian Financial Crisis in 1997 the concept of comprehensive security was a mainstay of policy elites in Southeast Asia. While the concept recognised non- traditional security threats the notion placed the nation-state as the main referent. In the aftermath of the Asian Financial Crisis and the terrorist attack in Bali, ASEAN member states ramped up their efforts to collaborate and coordinate at the regional level, which saw the signing of the Bali Concord II and the emergence of the ASEAN Political-Security Community. However, the APSC notably included reference to trans-boundary nature of security threats and the need to address these in a holistic, integrated and comprehensive way and attempted to strengthen regional as well as national capacities through activating multilevel governance.[9] This approach was reaffirmed in the 2008 ASEAN Charter and provides the regional organisation with legal status, new powers and an institutional framework and a shift away from the state as the main security referent towards a multidimensional and problem-solving approach to non-traditional security threats in Southeast Asia.[10]

Indeed, as analysts have observed non-traditional security issues are often interlinked, and their impact on the well-being and security of both states and societies can be as severe as those that result from military conflicts and violence. Through the multidimensional and problem-solving approach taken by ASEAN, the concept of non-traditional security identifies the referent as both state and society.[11]

Humanitarianism in the Asia - Pacific

Across the Asia-Pacific, governments and communities are trying to grapple with extreme weather patterns and conflicts. It has been evident for a long time that a coordinated humanitarian response is difficult, and will remain a challenge particularly between civilian and military actors. Within the region, ASEAN has been at the forefront of bringing together key humanitarian responders to develop an effective and coordinated response. Through the development of the ASEAN Agreement on Disaster Management and Emergency Relief, the ASEAN Coordinating Centre for Humanitarian Assistance on disaster management or AHA Centre for short was established as a regional body to facilitate linkages between national governments, the United Nations and international organisations in times of need. Established in November 2011, the AHA Centre most recently sent its emergency response team and the ASEAN Emergency Response Assessment Team (ASEAN-ERAT) a day before Typhoon Hagupit landed in the Philippines to monitor developments, provide emergency telecommunication support, assist in rapid assessment of the Philippines national disaster council, and provide logistical support for relief item deployment from ASEAN's emergency stockpile in Subang, Malaysia, and coordinate with other ASEAN member states and regional non-state or private sector actors like the Corporate Citizen Foundation's Swift Emergency Evaluation Deployment (SEED) team.

With the difficulties faced to deliver aid where it was needed most in the aftermath of Typhoon Haiyan, there was recognition that the surge capacity of donor militaries played an important role and was a key stakeholder in the humanitarian landscape. The launch of Singapore's Changi Regional Humanitarian Assistance and Disaster Relief Command and Control Centre (RHCC) in September 2014 is to coordinate such a military response with an affected country when they do not have the bandwidth themselves. However, while the offer of a mobile Command and Control unit was in place during Typhoon Hagupit, the devastation seen by Typhoon Haiyan a year earlier was averted.

As a result of these two significant developments, Southeast Asia is now home to two regional coordinating institutions for humanitarian assistance and disaster

relief – the AHA Centre and Changi RHCC. It is therefore of critical importance that these two regional institutions work together to build towards an inclusive and coordinated response in the aftermath of a disaster in the Asia – Pacific. One of the greatest challenges these institutions face will be for effective communication between militaries, national governments, regional organisations and civilian agencies. However, the emergence of these two regional bodies signals a clear commitment by governments in Southeast Asia to build capacity to respond to humanitarian emergencies. These regional institutions will face more complex disasters ahead and so while the seeds of cooperation and coordination have been planted, the forthcoming year will provide the opportunity to continue to develop disaster preparedness and response in the region.

Like in other policy areas, disaster response will be supported by a network of non-official diplomacy with the emergence of unofficial diplomats from epistemic communities as well as "track 2" networks across Southeast Asia[12] – such as the ASEAN-ISIS (ASEAN Institutes of Strategic and International Studies), CSCAP (Council for Security Cooperation in the Asia- Pacific), NTS-Asia (Consortium of Non-Traditional Security Studies in Asia), NADI (Network of ASEAN Defence and Security Institutions) and NEAT (Network of East Asian Think Tanks) to name the most prominent. However, the development of track 2 initiatives on HADR remain in an embryonic level of development particularly regarding the coordination between military and civilian stakeholders, which will continue to be a challenge for the region.

United Nations Framework

At the global level, there are a series of non-binding agreements regulating HADR between states including the 1991 UN Resolution on strengthening of the coordination of humanitarian emergency assistance of the United Nations, which called for the establishment of the Inter- Agency Standing Committee supported by a strengthened UN Disaster Relief Coordinator[13], the IDRL Guidelines[14] supported by a 2008 UN Resolution calling for member states to uphold them, and the World Customs Organization 2011 Resolution of the Customs Co-operation Council on the Role of Customs in Natural Disaster Relief.[15]

In addition to the global frameworks established to further HADR coordination, UN agencies have provided a lead role since the humanitarian reforms in 2005, which established the cluster approach. The cluster approach and the UN OCHA are bridging mechanisms which link the actors in an effort to establish an interdependent humanitarian system. There are also national coordinators and global level mechanisms – the inter-agency standing committee and emergency

relief coordinator. The cluster approach pool government and non-government agencies into sectors to enhance the coordination of the relief effort and these clusters work hand-in-hand with line ministries. Before the activation of the UN cluster approach, Red Cross national societies are generally the first points of contact for Governments requesting additional support from IFRC (in natural disasters) and ICRC (in situations of armed conflict). Once activated, the UN Cluster approach identifies a lead agency for the relief effort based on the below designation:

Humanitarian & Emergency Relief Cluster Leads	
Food Security	WFP and FAO
Health	WHO
Logistics	WFP
Nutrition	UNICE
Protection	UNHCR
Shelter	IFRC / UNHCR
Water, sanitation and hygiene	UNICEF
Camp coordination and camp management	IOM / UNHCR
Early recovery	UNDP
Education	UNICEF & Save the Children
Emergency Telecommunications	WFP

However, while in theory the cluster approach is inclusive there are those non-state humanitarian actors who work outside these global norms such as some radical faith-based organisations using disasters as a recruitment means, or states who fund a particular organisation to leverage or reach particular populations – best understood on a spectrum from extreme to mainstream. Some relief agencies may well be unaware or unequipped to buy-into the cluster system, which remains an ongoing challenge to the broader relief effort.

UN Humanitarian Response Depot

In 2010, the World Food Program signed an agreement with the Malaysian government to establish a UN Humanitarian Response Depot for the region in Subang and was built in 2012. By 2014, partners using UNHRD's Subang depot included the AHA Centre, Care, Irish Aid, JICA, Mercy Corps, Mercy Malaysia, NCA, Swiss Red Cross, UNFPA, WFP, WHO and World Vision International. The depot also facilitates specialized humanitarian operations trainings, emergency drills and other practical exercises with governments, UN agencies and non-governmental organisations. The training centre caters for a maximum of 50

participants and is fully equipped. In 2013, the Subang depot dispatched 40 consignments on behalf of 13 partners, supporting humanitarian interventions in 14 countries.[16] With the establishment of the UN logistical hub in Malaysia, it is clear that in 2015 we are now in a period of extensive development of cooperation mechanisms between stakeholders in relief assistance and protection. It is therefore essential that a culture of cooperation between the different stakeholders takes root to ensure humanitarian effectiveness.

Regional Agreements

There is political will in ASEAN to address the shortcomings in HADR. The 2004 Boxing Day Tsunami was the turning point for member states in realising the need for significant improvements in HADR cooperation across the Asia-Pacific. Since then we have seen an increasing effort to respond to HADR as it affects the political stability of countries in the region as they experience dysfunctional institutions, poorest affected the most, destruction of life, infrastructure, and food supplies. However, since the founding of ASEAN there has been recognition of the need for mutual assistance on natural disasters and was explicitly contained in the 1976 ASEAN Concord I.[17] In 2000 there was recognition within ASEAN to elevate cooperation on disaster management to a higher level, which saw the ASEAN Committee on Disaster Management (ACDM) established in 2003 with the goal of attaining 'disaster resilient' member states.

In the immediate aftermath of the Boxing Day Tsunami, ASEAN member states came together at an emergency meeting to strengthen relief, rehabilitation, reconstruction and prevention.[18] The following year member states signed the 2005 Agreement on Disaster Management and Emergency Response (AADMER), which came into legal force once it was ratified by all ASEAN member states on 24 December 2009. The AADMER is a proactive regional framework for cooperation, coordination, technical assistance, and resource mobilisation in all aspects of disaster management. It also affirms ASEAN's commitment to the Hyogo Framework of Action (HFA)[19] and is the first legally-binding HFA-related instrument in the world. Finally in 2011 the ASEAN Coordinating Centre for Humanitarian Assistance on Disaster Management (AHA Centre) based in Jakarta was established.

AHA Centre

The establishment of the AHA Centre which opened in 2011 was a significant milestone in regional HADR Cooperation and institutionalisation of AADMER and a clear indication of the implementation of the ADDMER Work Programme 2010 – 2015 and ASEAN Working Group on HADR. The Work Programme seeks

to translate AADMER's spirit and intent into concrete actions and initiatives to be implemented from 2010 to 2015 in order to attain the ASEAN vision of disaster resilient nations and safe communities by 2015 and beyond. It essentially seeks to reassert the role of the state back into humanitarian action where much work is now carried out by NGOs and CSOs.

The partnership strategies developed stronger cooperation within the Hyogo Framework for Action (HFA) with governments engaging a multi-sectoral approach and implemented the priority areas of action by different stakeholders, including civil society (i.e., NGOs, CBOs, and volunteers), the scientific community, and the private sector. This essentially generated support for AADMER and was one avenue to work towards a 'whole of society' approach. The work plan established the AADMER fund, which receives voluntary contributions, commits member states to raise awareness amongst the public and encourages member states to develop and implement national and local level plans for AADMER.[20] Natural phenomena such as typhoons and earthquakes need not translate to disaster, or their human impact can be minimised, if states and societies are equipped to deal with them. The AHA Centre was established to be vocal point for this and the communication hub in all humanitarian assistance missions in the region. Establishing the AHA Centre as a premier provider of information and communication services supporting humanitarian assistance missions and disaster risk reduction principles will help ensure the success of AADMER and support the well-being of the people, communities, and economies of Southeast Asia.

To conclude, the AHA Executive Director, Said Faisal, said recently that the past 3 years have been about getting the AHA Centre up-and-running. "It is no longer a concept, there is an AHA Centre." The executive director foresees the AHA Centre developing in four key ways in the years ahead, which he refers to as AHA Centre 1.0, 2.0, 3.0 and X.0. In the first phase, the AHA Centre experienced teething problems notably in 2012 around its response to Typhoon Haiyan and got "visibility damage", because it focused its efforts on working with the Philippines national disaster management office and was not seen as an active player in the field. This year, the AHA Centre enters AHA Centre 2.0 which launches with the ASEAN Community "One ASEAN, One Response" and bring together stakeholders to move forward in the same direction. The third wave will be AHA Centre 3.0, which will see the AHA Centre making connections with the rest of the world through organisations like the ASEAN Regional Forum and the East Asian Summit to further develop partnerships with UN OHCA for the centre to be the main coordination centre in the region. Finally, in a future iteration the AHA Centre X.0 will be for the centre to coordinate an ASEAN response outside of its region to build the sense of 'we' with complementary cultures of organisations to respond to disasters.[21]

Changi Regional Humanitarian Assistance and Disaster Relief Coordination Centre (RHCC)

The Changi RHCC is based at the Changi Command and Control Centre (CC2C) in Singapore and draws on the facilities available at the CC2C for large-scale multinational operations and exercises as demonstrated through the Information Fusion Centre (IFC) which is also housed there. The RHCC will focus on supporting a disaster affected state's military in coordinating assistance provided by foreign militaries, and support and complement other existing mechanisms like the AHA Centre in Jakarta as part of an overall HADR effort. The RHCC is able to fuse information from regional disaster and early warning centre, distribute the situation picture to partner militaries through its OPERA Command and Control Information System (CCIS) web-portal. Then in collaboration and agreement from the affected state, the RHCC can also concurrently conduct initial planning and scale up for a potential multinational military relief effort. If for example an extreme weather event occurs then the RHCC can assist in minimising duplication and identify gaps in military assistance, and deploy a mobile coordination unit to support the affected state's military in coordination efforts on the ground until an affected state's military is able to coordinate the foreign military assistance without external support.[22]

Civil-military relations

The establishment of the RHCC and AHA Centre illustrate a significant turning point in HADR in the Asia-Pacific. They are also the coordinating mechanisms for military and civilian responses respectively. One of the greatest challenges yet to be overcome is the effective development of communication and coordination between these two significant types of stakeholders and it will become ever more important in the coming years. One of the significant points of departure between practitioners is over the use of military assets in HADR particularly in countries affected by armed conflict or other violence. Civilian agencies argue that military assets in such circumstances should be a last resort, whereas military practitioners recognize that the surge capacity of the military makes their response rapid and effective to alleviate suffering. The emergent middle ground between these two positions is that the use of military assets can only be justified by the serious and urgent need for life-saving humanitarian action and when there is no alternative means of taking that action. In other words, the use of the military should be prompted by needs rather than availability.

Within the Asia-Pacific, the capacity of states to respond to disasters remains varied. However, those states most susceptible to disasters like Bangladesh, Myanmar and

Nepal are the same countries without national guidelines and remain the least prepared for the sudden onset of an extreme weather event. Within the region, Thailand is seen as a leader in developing national guidelines, and developing a coordination plan with civilian actors including an effort to address issues like the need to set up a pre-registration system for humanitarian actors. It is important to build understandings between military and civilian actors on the ground and to maintain these professional relationships. Drawing on the latest technology is one avenue to bridge the divide to create the conditions to share information on early warning, coordinate planning and produce effective relief delivery. As such, crowdsourcing technology can help with interoperability to bring humanitarian aid to where it is needed most.

Further the institutionalisation of capacity is central to connecting actors in a formalised and structured way to ensure institutional memory, which has been lost time-and-again after a disaster with similar recommendations identified after subsequent disasters including the need to understand operational context, the different roles and ways of working for involved actors, promoting better working relationships between actors, the importance of personal relationships, better coordination for operational planning between military and civilian actors, streamlining communications, and information sharing. A way forward would be for greater institutionalisation of capacity and include the establishment of policies, strategies, systems and structures, designation of resources, and annual assessment, planning and implementation. Ultimately, clear roles and responsibilities of key actors, clear terms of references for entries and exits, optimisation of surge capacity, and disaster management is everybody's business.[23]

One key example of how to overcome these stakeholder differences was during the Christchurch Earthquake in 2011. The NZDF Liaison Officers built personal relationships between military and civilian agencies, which minimised bureaucracies and misunderstandings. Liaison Officers also advised civilian agencies of the military capabilities, and tasks not suited to the military were re-directed to more appropriate agencies.[24] However, at first, a certain level of trust needed to be developed between the various information sharing partners. This willingness to share does not come easy, as most continue to operate on a 'need to share' basis," and a key recommendation was to develop trust-building exercises to lower these barriers.[25] A second recommendation was on the "interoperability between countries which can be impeded due to equipment limitations. In such cases, capacity building is key to enabling all partners to be able to share on an equal footing."[26]

Traditionally militaries have been associated with protecting sovereignty and territorial integrity, but now militaries amidst changes in geo-politics are called upon for Peacekeeping Operations and HADR. For militaries, working alongside United Nations agencies and Non- Government Organisations is the new norm in Complex Humanitarian Emergencies. There is a need to harmonise, manage and coordinate the amount of assistance on the ground to ensure smooth transition from military to civilian control where militaries were used as a last resort. This new architecture will dominate the global discussions to update global guidelines to reflect the new geo-strategic realities and actors. There is space for cooperation in the Asia-Pacific region for civil-military disaster response but challenges remain. These challenges include the different cultures of decision-making, with a need to see them as positive engagement; the transfer of responsibility from emergency response to longer-term recovery; the appropriate use of information and technology. These challenges will require proactive commitment from both military and civilian actors because the bottom line is that trust-building is about engagement during peacetime and outside of disaster scenarios. Up until today, there remain many lessons observed rather than learnt which identifies two challenges. In the first instance, it means that there are difficulties present with institutional memories within military and civilian institutions, and in the second, the failure to establish durable communication channels between military and civilian organisations. It is therefore a notable development that the RHCC provides a platform for military liaison officers to develop such communication and coordination mechanisms with civilian agencies through the AHA Centre.

A New Reality?

This policy paper has sought to not only conceptualise non-traditional security in terms of levels of governance and sites of legitimacy and insecurity, it also provides an introduction to policies that seek to address HADR in the Asia-Pacific. In the first instance, activity at each level of governance can be envisioned in three broad constituencies. This paper has sought to identify key developments in HADR and advance the necessity for a multidimensional and holistic approach to HADR in an effort to recognise the changing nature of state-society relations affecting how effective HADR responses are put in place.

The building of bridges between these different stakeholders is underway although at a glacial pace but does offer an avenue for further research and study, and that the structure dominant in ASEAN is being mitigated by the institutionalisation of 'interstate cooperative patterns.'[27] Through the visioning of the regional level of

governance through civilian agencies, militaries and of non-state influencers like track 2 epistemic communities and civil society organisations, the complex web of interactions which determine the level of engagement in HADR and understanding the ways and means of improving responses becomes clearer to see.

A multidimensional and holistic approach to HADR attempts to address concerns that states in the Asia-Pacific moves beyond rhetorical commitments to policies that substantively address HADR to ensure a sustainable pathway ahead. With more frequent disasters occurring in the Asia – Pacific and the emergence of new actors in the humanitarian landscape, the system of governance in place for humanitarian assistance is no longer fit for purpose as there is a need to engage actors across and between local, national, regional and global levels. In the absence of an appropriate system of governance, coordination and cooperation will remain a key challenge and eyes will be on the World Humanitarian Summit in 2016 to address these concerns.

CHALLENGES AND RESPONSES IN CYBERSECURITY

Lieutenant Colonel (Retired) Sazali Sukardi

Digital Age has provided unprecedented opportunities for states to utilise information and communication technology (ICT) to progress and prosper. It is expected that by 2015, five billion people would be connected in a global community brought closer together by voice and, increasingly data communications.[28] There are more than 2.8 billion people using the Internet and over 10 billion Internet-facing devices in existence. More than 40% of global Internet users are now based in Asia Pacific with 644 million users. Southeast Asian markets account for approximately 10% of the Asia Pacific Internet population.[29] As the global centre of gravity shifts from Europe and North America, the Asia Pacific region is becoming the most important political, economic, strategic and socially diverse and dynamic region in the world. The major factor driving this change is the development of the capabilities offered by ICT, and the ability of the region to exploit the resultant opportunities to both national and regional advantage.

The widespread use of ICT, however has introduced new cyber security challenges. The world has witnessed the rapidly-changing world of cyber threats and how they are encroaching into every sphere of human activities. Current cyber security landscape is worsened by the users' ignorance, technical incompetency, and ineffective cyber security measures by states and organizations. Increasing dependency on cyber space by states has exposed them to a significant risk and their well-being is dependent on the security across cyber space. Hence, ensuring the secure, resilient and trusted operating environment is essential to sustain the states' progress and prosperity.

Most states have already put in place a domestic cyber security, however it is not sufficient. Individual states should also establish common collective measures of cooperation with others to enhance cyber security to the mutual benefit of the global community. This paper describes the current cyber security landscape, the various cyber security challenges, and how to respond to such challenges.

Current Cyber Security Landscape

The exploitation of ICT has introduced various technical threats such as hacking, phishing, web defacement, botnet and malware infection. Content-related threats may refer to abusive contents such as hate speeches, radical, and offensive statements, seditious and defamatory contents although being committed in the

name of freedom of speech. The trends of computing such as cloud computing, mobile devices, Big Data, Bring Your Own Device (BYOD), Internet of Things and social media were created for convenience with limited security functions, hence posing new security challenges.

Cyber threats today are geared towards Advanced Persistent Threats (APT) targeting critical systems or specific targets that will result in high impacts on an organization. Cyber criminals are exploiting technology vulnerabilities and users' ignorance to intrude computer systems using a combination of technical sophistication, exploitation and social engineering.

International Organized Crimes

Opportunities for cybercrime have increased with the continued advancements of Internet. While businesses are weighing the benefits of new technologies, criminals are also using the same innovations to refine their areas of expertise. It is not an exaggeration to say that cybercrimes are fast becoming the crime of choice and gradually replacing traditional crimes. Today, most states are facing a lot more threats posed by international organized crimes namely drug and human trafficking, financial fraud, scams and money laundering. Criminals exploit Internet to facilitate their cross-border criminal activities. Both cyber and traditional crimes include conduct whether by act or omission, cause the breach of the laws. With the advancement and availability of ICT, cybercrimes are on the rise making today's crimes become more problematic.

Cyber crime is a growth industry as it is profitable and the risks are low. In 2014, the report from the Center for Strategic and International Studies and sponsored by McAfee estimates that the likely annual cost to the global economy from cybercrime is more than $445 billion, including both the gains to criminals and the costs to companies for recovery and defense. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion.[30] The report also concludes that cybercrime causes an impact on approximately 200,000 jobs in the U.S. and 150,000 jobs in the European Union.

Internet Underground Economy

Today's cyber crime has its own supply chain structure that reflects how all serious crimes will be organized in the future. ICT experts are continuously driving the innovation of tools and some of them provide their services to criminals who are lacking the skills or capabilities. Criminals use the service-based nature of the cybercrime market to carry out more sophisticated crimes. Internet underground market provides cyber criminals with a connection for the trade of goods and services using web currency creating an organized set of criminal relationships.

Such situation creates challenges for law enforcement especially in regards to tracing the sources of criminal activity.[31] Not only could the experts make profit from selling their services, but also they could make equal profit by performing the crimes for themselves.[32]

Cyber Attacks on Critical Systems

Critical infrastructure encompasses among others, telecommunications, banking and finance, transport, energy, and water sectors that enable any government to function and deliver critical services to the people. The trend of cyber attacks targeting critical infrastructures has become national security concern and it is growing. The act of cyber attack is understood as a targeted attempt to destroy or temporarily interrupt the critical infrastructure. According to McAfee Virtual Criminology Report 2007, 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.[33] Most states have declared critical infrastructure as a strategic national asset as any disruption on any sector within the critical infrastructure can affect the states' operations and functions. To date, most states have already formulated various security measures to protect their national critical infrastructures.

Connecting the industrial Supervisory Control and Data Acquisition (SCADA) systems to the corporate IT network gives organisations the ability to connect systems that provide new opportunities for supporting manufacturing and automation systems remotely. However, this new degree of connectivity means that industrial control systems are exposed to cyber security threats similar to those faced by corporate networks. Energy companies especially in the Middle East have already been subjected to a series of cyber attacks. Operation Night Dragon is an example of cyber attack targeting the energy sector, which employs a combination of social engineering, exploitation, and coordinated plan.[34] The Middle East region also cannot forget Shamoon, spyware with a destructive module that caused huge impacts on the operations of oil companies.

At national level, it is imperative for individual states to establish an effective public-private cooperation. At the international level, states should promote a robust cyber security culture that can be derived through various regional and international resolutions. If a state is attacked, the impact will not only be confined to that state, but it can also spread to other parts of the globe. At this juncture, there have been significant efforts amongst states in having collaborative initiatives to protect their common critical interests.

Hostile Activities and Conflict in Cyber Space

Cyber security experts acknowledge the existence of hostile activities and act of aggression conducted by states, state-sponsored and non-state actors. Such activities can refer to anything from cyber espionage, malicious software (malware) infection and system intrusion to high- scale cyber attacks conducted with technical complexity and sophistication. Such activities are committed with diverse political and economic motives to achieve dominance in cyber space. New techniques and methods of cyber attacks have emerged, and the traditional ones become obsolete. As such, in today's digital age the attitude towards war has also evolved and innovated.

There are evidences indicating that cyber space is utilized by states, state-sponsored, non state actors to wage war. As a result, the trend of cyber security now is seen becoming more aggressive. As the matter of fact, every state now organizes itself to face the possible occurrence of conflict in cyber space using both offensive and defensive approaches. This situation has increased tension in cyber space and if it is not addressed adequately, the world will face cyber war as the trend of future conflict. This is not rhetoric as several states have already developed their cyber war strategies and acquired related capabilities. The demand for cyber warfare capabilities will grow as states continue to invest heavily to protect their government systems and critical services from cyber attacks.

Cyber Espionage

Cyber space can be categorized as part of hostile activities and acts of exploitation. According to the research firm SANS Institute, cyber espionage was ranked as third on its Top Ten Cyber Menaces for 2008, after web site attacks exploiting browser vulnerabilities and botnets.[35] In 2008, PC Word Business Center Economic warned that cyber espionage would be a major concern as states employ cyber theft of data to gain economic advantage in multinational deals.[36] Cyber espionage already widespread, not only suggests criminal involvement but also state intelligence and military services. Cyber espionage has becomes more aggressive nowadays, as states, states-sponsored, and organized crime groups have been conducting large- scale act of cyber espionage campaign targeting government and industrial computer networks. It was reported that NetTraveler espionage campaign made 350 high-profile victims in 40 countries. According to Kaspersky, most of the targets were from the diplomatic sector (32%), followed by governments, military and private organizations. The espionage group's most recent domains of interest are energy production, nanotechnology, space exploration, nuclear power, lasers, communications and medicine.[37]

It comes as no surprise that global cyber espionage activities often involve world's superpowers namely the United States and China. The Asian School of Cyber Laws, India, stated that in March 2009 covert network using servers mainly based in China, tapped into classified documents from government and private organizations in more than 100 countries.[38] It is also claimed that U.S. computer networks have become under series of attacks since 2003 that were attributed to the Chinese hackers known as Titan Rain.[39] The hackers allegedly gained access to many United States defense contractors' computer networks that were targeted for their sensitive information, including those at Lockheed Martin, Pentagon and The National Aeronautics and Space Administration (NASA).[40] However, it is difficult to prove such allegations as the Chinese government has been denying involvement in most cases.

The Edward Snowden's leaks have captured global attention.[41] The leaks revealed important things about the spying activities of the United States and its allies that targeted amongst others high-profile individuals, major organizations and governments. Spying activities by the world's superpowers have set a serious precedent with other states are likely to catch up, hence posing the risks of undermining global Internet freedom. The Snowden's leaks also indicate that no state is safe in cyber space, hence potentially eroding users' trust in digital technologies. Cyber espionage is not adequately addressed as there are national sensitivities, political, military and other, that must be recognized; hence, there will be obstacles to future cooperation if confronted.

Cyber espionage has long been part of national and military doctrines. With regard to this, most states seem reluctant to talk about their surveillance programs, making the world far from being transparent about spying issue. Within ASEAN Regional Forum (ARF), ASEAN is yet to derive a more suitable approach to deal with its partners namely the United States and China as cyber espionage will continue to be a pressing issue in many more years to come.

On the contrary, Snowden's leaks have prompted outrage within European Union (EU). Some of EU leaders have even suggested that talks for a free trade agreement between Washington and Europe should be postponed until further clarification from the United States. EU has also considered more transparency and less influence of the United States over the institutions controlling the mechanics of the Internet. EU has also demanded the multi-stakeholder approach as the way forward to Internet governance.[42] With regard to this, the United States needs to recognize that EU is serious when it comes to privacy and the individual freedoms

of European peoples. The United States may have to incorporate privacy into its future transatlantic policy as the way to rebuild its relationships with EU.

Hacktivism

The explosion of Internet has also created the phenomenon towards "digital hacktivism". "Anonymous" has claimed responsibility over the past years for cyber-attacks against governments and major multi-national companies. The "Anonymous" hacktivist group is said to have thousands of operatives and has no set rules or membership. It is regarded by experts as politically-motivated, high profile and sophisticated. Anonymous has attacked several established organisations that include the U.S. Central Intelligence Agency (CIA) and U.S Congress, MasterCard, Visa, Sony Playstation network, Turkish Government websites, North Atlantic Treaty Organizations (NATO), and many others. In June 2010, Malaysia has witnessed cyber attacks via codename "Operation Malaysia" by Internet-based hacktivism known as "Anonymous".[43] It was noted that Malaysian hackers had teamed up with "Anonymous" group during the attacks in response to the government's decision to block a number of websites. Although, there was a warning for a second cyber attack codename "Red October" but it was not realized.

On another occasion, a Facebook site believed to support Anonymous has called for Anonymous, Wiki-Leaks, the Pirate Party, Occupy and Oath Keepers to defend humanity. The site also posted a warning that reads "Remember who your enemies are: Billionaires who own banks and corporations who corrupt politicians who enslave the people in injustice".[44] Hacktivism will continue to pose global threats claimed to be done in the name of Internet freedom and justice.

Sophistication of Malware

Modern malware today is complex, intelligent and disastrous. The world has seen how Stuxnet targeted the operations of industrial systems that run nuclear facilities.[45] Duqu was designed to gather intelligence data and to set a pre-cursor for a future attack.[46] The world also witnessed the emergence of Flame, a sophisticated spyware believed to be part of a well-coordinated cyber espionage operation committed at a level of state.[47] These malware are evolutionary and they provide an insight into the future state of the ever-changing cyber threat landscape. Protecting against such malware attacks is a key challenge as states continue to invest heavily on ICT and digital economy. In most cases, malware serve as the initial step to cyber attacks. Computers infected by malware will become part of botnet which can be taken control and subsequently used as a springboard to launch cyber attacks. The situation is alarming when botnet services can be acquired from the Internet underground economy.

Misuse of Social Media

Internet users today are spending more time on social networks, hence exposing themselves to various risks. Internet namely social media nowadays is fast becoming the medium of choice for social interaction. Some states view that cyber threats are also in the forms of malicious contents. On-line news, discussion forums, chat rooms, blog and web sites, and social networking sites are accessible to all and they can be effectively used as propaganda tools in threatening people's safety and national security.

The use of cyber media should not be overlooked as it can influence the perception of the population. Inter-active websites and blogs, social networking sites and discussion forums have been extensively used for illegitimate purposes by insurgent, radical and extremist groups to spread their ideas. As a result, out of frustration, anger and hatred being triggered by seditious and provocative contents may escalate to road protests and civil unrest.

The 2013 statistics show that there are about 1.056 billion Facebook users worldwide.[48] States especially in the Asian region have to do more to protect their populations to protect their cultural values that can be different from the West. As written by many literature and news, social media was extensively used during Arab Springs to bring down several government leaders in the Middle East.[49] No doubt that social media is a powerful tool to promote peace and stability, while, at the same time, it can also be misused by irresponsible groups to undermine national security. The misuse of Internet as a propaganda tool can corrupt the minds and transform the moderates into radicals and extremists. Many of the actors in foiled plots have been discovered among others, to launch anti-government propaganda in the name of freedom of speech that is protected under human rights.

Shadi Hamid of Brookings Doha Center states, "People are using social media for cyber warfare. That's what we are going to see – governments or non-state actors are going to try to find ways to use the Internet and social media to gain an advantage in their own battle".[50] It is expected that the subject of social media will remain as a major security concern in many more years to come because it is an effective tool for Psychological Operation (PsyOps) that can undermine national security.

Coherent Response to Evolving Cyber Threats

The rapid development of ICT in all parts of the globe has resulted in enhanced prosperity amongst the states. Cyber security that ensures a secure, trusted and resilient ICT domain is a critical factor in underwriting that prosperity. While measures to tackle cyber security challenges are an ongoing effort, the types of cyber threats do not remain static. New cyber threats regularly emerge and they are becoming more sophisticated. In this regard, most states recognize the need to establish a coherent response to cyber security challenges. International community needs a trusted cyber environment to enable it to interact with each other with trust and confidence.

Most states have a great concern about the security of critical sectors, including that relating to telecommunications, banking and finance, transport, energy, water, essential government services and the media, in the delivery of national advantage. Therefore, the priority for each state to implement an effective domestic cyber security strategy and policies to protect their respective critical sectors, and to extend all possible supports to the other states in their legitimate requests for cyber security cooperation. In this context, the formulation and implementation of a more effective international cooperation in cyber security, therefore, is an urgent requirement.

ASEAN Regional Forum (ARF)

In July 1993, the 26th ASEAN Ministerial Meeting and Post Ministerial Conference have agreed to establish the ASEAN Regional Forum (ARF).[51] The following year in July 1994, the 27th ASEAN Ministerial Meeting stated, "The ARF could become an effective consultative Asia- Pacific Forum for promoting open dialogue on political and security cooperation in the region. In this context, ASEAN should work with its ARF partners to bring about a more predictable and constructive pattern of relations in the Asia Pacific. Despite the great diversity of its membership, ARF has attained a record of achievements that have contributed to the maintenance of peace, security and cooperation in the region."

ARF member states are already embracing digital transformation, the opportunity offered by the convergence of new digital technologies. In this context, the success of ARF efforts to foster constructive dialogue and consultation on political and security issues can be seen to be dependent on cyber security. ARF has served as an important inter-governmental platform in addressing several cyber security issues. Therefore, there are several cyber security issues addressed through the ARF statements as well as in the various meetings and activities. Such ARF

events demonstrated the commitment and seriousness of ARF to provide ample opportunities for its members to share their views and best practices on cyber security.

To achieve better mutual understanding in cyber security, ARF has adopted "The Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space" in July 2006 and "The Statement by the Ministers of Foreign Affairs on Cooperation in Cyber Security" in July 2012. ARF has implemented several events to demonstrate its commitment and seriousness in responding to cyber security in the region.

The development of ARF Work Plan on "Cyber Security in the Use of ICT" is an initiative by ARF to address the norms of responsible behaviours in cyberspace. The work plan is aimed at promoting a peaceful, secure, open and cooperative cyber environment by developing thrust, confidence and assurance between ARF participants. The work plan, however, is yet to be deliberated amongst ARF participants before it can be implemented. ARF has also been working on Cyber Confidence Building Measures intended to promote the importance of confidence building and transparency measures in promoting stability in cyber space. The initiative is still on-going and addressing several practical issues such as the importance of having Points of Contact in each member state for managing cyber issues.

Although, states in the region recognize the urgent necessity of prohibiting hostile activities such as cyber espionage by state actors, but they are of the view that this issue should be elaborated within appropriate forums. In this context, ASEAN prefers to work with its ARF partners that bring about a more predictable and constructive pattern of relations in the Asia Pacific. The way ahead, therefore, is to identify those areas of mutual concern that will enable collective cooperation, the setting and measuring goals and action within those areas, and related priorities.

The Council for Security Cooperation in the Asia-Pacific (CSCAP)

In June 2010, the CSCAP Steering Committee established the CSCAP Study Group aimed at examining the various cyber security issues and challenges facing the Asia Pacific region, and their likely security risks. Based on the findings, CSCAP has proposed a more effective cyber security strategy being submitted to the ASEAN Regional Forum (ARF) for its further consideration.[52] Its findings among others propose that concurrent with the development of national strategies and policies, it is vital that states in the region cooperate in establishing effective collective measures to ensure that cyber security across the whole region meets their mutual interests.

Cyber threats are revolutionary and we have seen how they are growing in sophistication, hence regional approaches towards cyber security must be equally evolutionary. Amongst such measures include regional cooperation that further increase regional abilities to effectively address cyber threats as highlighted by CSCAP Study Group on Cyber Security are described in this part.[53]

Cyber Security Awareness and Education

Human aspect should be given a great emphasis in cyber security. ARF promotes a robust culture of cyber security and cyber safety awareness and education to build confidence in the domestic and international digital environment, and create the knowledge and tools with which to protect themselves and respond to threats. No doubt that the positive use of the Internet infused with security acculturation and education amongst Internet users will promote stability, social well being and wealth creation.

Sharing of Information and Experience

A suitable system needs to be established to facilitate the sharing of information and experiences about cyber threats. Ultimately, states (potentially through their CERT) should be able to share threat information in real time to enable them at ARF level to anticipate and collectively mitigate cyber threats.

Capacity Building and Technical Assistance

It is in the mutual interests of all states in ARF to implement as a matter of priority, a program of advice, training and technical assistance that develops the cyber security capacity of all states where required. A suitable work plan on cyber security should be formulated to better promote capacity building efforts within the region because some states may not have the required level of cyber capabilities. Adequate technical expertise and capabilities among states are needed in order to strengthen international collaborative efforts in mitigating cyber threats.

Computer Emergency Response Team (CERT)

Recognizing cyber threats as trans-border issues, there are several organizations that ARF states can engage to strengthen their domestic and collaborative cyber security. It is recommended that where a state does not already have CERT, it is to be established. CERT may be either a government or non-government organisation, depending on national preference. The role of the CERT would be to facilitate coordination for the provision of information and advice amongst all domestic stakeholders, and to facilitate regional and global cooperation. A very practical activity to undertake would be to initiate a program where those nations with a CERT capacity would assist those without to establish this function.

International community should explore whether CERT that are established in various countries can be further developed as the coordination centre for the distribution of information and advice about cyber threats, vulnerabilities, and protective and mitigation measures. Amongst them are the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) and the Asia Pacific - Computer Emergency Response Team (APCERT). APCERT currently has 26 Operational Members from 19 economies, whereas OIC-CERT has 33 members from 19 states. In this regard, Malaysia was the Co-founder and the Chair for APCERT in the year 2007 to 2008. Malaysia is now a member of APCERT Steering Committee. Malaysia was also the Co-Founder and the Chair for OIC-CERT in the year 2009 to 2011 and 2011 to 2013. Currently it serves as a permanent scretariat to OIC-CERT. CERT cooperation such as via OIC-CERT and APCERT has already established links with other regional CERT and Computer Security Incident Response Teams (CSIRT).

Legal Approach

CSCAP recommends that all states in ARF review their criminal laws and, wherever practical, implement changes to harmonise laws to protect their society and promote international legal cooperation against cybercrime. They should also enable legal cooperation with investigations, the collection of evidence and other related forms of legal mutual support. Any form of study or review of laws pertaining to cyber activities is to take into account the correlation between the phase of development of technology and growth and prevalence of cyber crime. In the absence of effective laws, a state will likely become a prime target in cyber crimes, and also be made as a springboard to launch cyber attacks on other states.

ARF Cyber Security Action Task Force

It is recommended that a regional action task force be established to liaise with all key stakeholders to develop recommended standards, mechanisms, and policies to assist in the harmonization of laws to combat cybercrime.

Challenges in Cyber Security

It is a great challenge for international community to strengthen communication, enhance mutual trust, and promote cooperation to build a peaceful, secure, open and cooperative cyberspace. The various challenges in cyber security are due to various factors, which are described in this part.

Cultural and Religious Diversity

International community, namely within Asia Pacific region, presents a great historical, cultural, and ethnic diversity as well as a variety of stages of political evolution and economic development. Therefore, basic approach to enhancing regional cyber security may have to consider the cultural aspect. This includes the notion of cyber culture, the necessity to recognize the cultural elements behind the Internet policies and to promote international cooperation in the spirit of mutual respect and inclusiveness. The regional approach also implies that the principles of national sovereignty and non-interference in other's internal affairs should be safeguarded. To achieve the desired cyber security situation, it may require the combined roles of central and local governments at a domestic level. It also includes the participation of private sector and non-governmental organizations (NGOs) that are increasingly playing more significant roles to support domestic cyber security. At the regional level, such situation should be further strengthened through various discussions and cooperative efforts.

Internet Rules

Some Asian states view that Internet rules are necessary to restrain provocative and offensive behaviours in cyber space that may lead to the breach of national security and public order. For example, the misuse of social media may raise the risk of an overreaction from the public when sensitive and contentious incidents occur in the multi-ethnic and multi-religious states. Therefore, some Asian states believe that it is their rights to repudiate such unacceptable acts. In this regard, Internet rules maybe necessary to establish some basis on what can be done in cyber space. The move to restrain malicious behaviour in social media, however, may be controversial, as it may be seen by other states as limiting the freedom of expression and protection of basic human rights. Some states are of the view that the focus of cyber security should be on safeguarding the technology and infrastructure and not on controlling the flow of content or information. The move to regulate Internet contents and restrict the free flow of information may be a subject of a special attention amongst states, NGOs and human right activists.

Establishing the Norms of Behaviour in Cyber Space

It is understood that states may have different adaptability to cyber security acculturation. Some states namely in ARF emphasise the importance of guarding, protecting, preserving, and promoting national identities. We have seen how certain contents that are posted online may be seen as sedition and defamation, hence violating a state's laws. On the contrary, the same contents may be considered as the act of freedom of speech that is protected under human rights, hence acceptable for other states. The challenge faced by ARF is to establish the norms of behaviour in cyberspace as a non-legal approach towards ensuring a

secure cyber space. More regional efforts are needed to reduce cultural gaps and mitigate conflicts in cyberspace as well as strengthening legal measures and cyber ethics that are suitable for local practices while at the same time in consistent with international norms.

In view of this, behavioural norms in cyberspace are about the acceptance of common best practices and they should be based on mutual understandings rather than legal process. Some states recognize the great importance of promoting cultural diversity to build an inclusive information society, and that the national identity and values should be respected and safeguarded.

Trend of Cyber Space Conflict and Protection

We have seen how the trend of cyber space protection is growing in sophistication and changing over times. The trend is becoming more subtle, flexible, and even offensive in character, often using legal regulations to supplement or legitimize covert activities. Today, many states are becoming more aggressive and more overt in strengthening their cyber defences and they are investing heavily to protect their critical infrastructures via proactive and responsive approaches. Many states have already extensive networks for gathering information and conducting surveillance and highly sophisticated capabilities to monitor communications.

Cyber space protection has also served as credible deterrent that includes pre-emptive cyber attack on imminent threats. We should also note that any major cyber attack on networks linking states and organizations would have grave implications, hence leading towards destabilization of the region.

The CSCAP acknowledges the existence of cyber threats arising from hostile activities by states and state-sponsored actors. It recommended that states in the region should recognize the urgent necessity of establishing regional and international regimes, which prohibit such hostile activities in cyber space. The CSCAP notes the importance of state-related hostile activities as potential cyber security threats to all states, and this could be the subject for separate consideration. The challenge to the regional community is to elaborate these issues in an appropriate format, and failure to do so, may lead to the rise of cyber war as the trend of future conflict.

Cross-Border Jurisdictional Matters

Different laws among states causing cross-border cyber incidents can be difficult to deal with. Laws are to protect national security interests within well-defined geographical boundaries. As such, most current laws are of limited effectiveness in addressing transnational cyber crimes. This explains why cross-border

jurisdictional matters deserve a special attention by international community in order to effectively address cyber security.

There is no specific sovereignty that controls cyber space. Although many regulations pertaining to cyber space have been passed in several jurisdictions, the open and sometimes unregulated nature of the Internet and the irrelevance of geography may lead to the cyber space being a safe haven for potentially criminal activities. Cyber space can be exploited by international organized crimes without fearing of getting caught. Apart from it, rapid technological advancements exacerbate the difficulty in apprehension of criminals, if not rendering it impossible altogether.

International Laws on Cyber Crimes

Harmonization of laws is still far from being a reality as most states are not ready yet to go for it. Every state has its own security interests as well as having diverse perception towards cyber crimes. Therefore, most laws are created mainly to protect national security interests within national borders. Cross-border crimes and jurisdictional issues will remain as a major cyber security challenge. Any relevant efforts to harmonize laws will take a long process due to various bureaucratic and tedious procedures that exist among states in the region.

The Budapest Convention on Cybercrime is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among states. The Convention opened for signature on 23 November 2001 and it entered into force on 1 July 2004. As at December 2012, 58 states are parties/are committed to become parties. Many other states are also believed to use Budapest Convention as a guideline for domestic legislation. In view of this, Malaysia recognizes the cross-border jurisdictional and legal issues, and the possibility of common legal approaches to address them. Despite certain common cyber threats, the differences in legislation between states remain significant. Due to legal complexities involved, Malaysia has taken some time to sign any multilateral treaties, including the Budapest Convention. Malaysia is to ensure that such treaties should not be in conflict with national interests and sovereignty. To date, Malaysia is still studying the Budapest Convention while preparing itself towards complying with the Convention.[54]

Conclusions

Cyber threats are growing in sophistication in parallel with ICT revolution and they would remain as the global security concerns in years to come. Most states have already expressed great concern about the rise of cyber crimes and the trend of cyber attacks geared at attacking critical infrastructure as well as their impacts on national security interests. In view of this, all states should adopt a more coherent and holistic approach to respond to various cyber challenges in order to protect their common security interests. International cooperation is an essential requirement for ensuring that all states, individually and collectively, are able to operate within and benefit from the advantages of a secure and trusted cyber environment.

FUTURE HIGH TECHNOLOGY WEAPONRY IN EAST ASIA: STRATEGIC DRIVERS, ISSUES, AND DEBATES

Michael Raska

East Asia's Changing Security Paradigm

East Asia's strategic assessments and debates currently focus on three broad issues: the pace, character, and direction of China's military modernization, the struggle for dominance by the region's two great powers (China and Japan), and perhaps most importantly, the contours of long-term regional strategic competition and rivalry between China and the U.S. The key question driving the debates is whether, how, and why may conflicts occur in the future East Asian strategic landscape? These questions reflect the East Asia's changing strategic realities, shaped by contending trajectories of unresolved historical legacies and emerging security challenges.

One of the key factors driving the debate is China's ongoing qualitative military modernization. The economic, political, and military rise of China, reflected in three decades of relentless Chinese economic growth, has propelled progressive modernization of the Chinese military with major improvements in virtually every capability domain: land, air, naval, missile, space, cyber, and electronic warfare.[55] The cumulative effects of these developments are substantial as China's catalogues of air, land, and naval platforms are gradually catching-up in terms of both qualitative sophistication and operational effectiveness.[56] In March 2014, China announced $131 billion defense budget, up 12.2 percent from the 2013 budget of $119 billion – marking 17 straight years of near-double digit increases in defense spending.[57] As China expands its national interests in the broader context of "new historic missions", it seeks to regain a great power status and reassert its geopolitical role in the region. China's People's Liberation Army (PLA) is gradually pursuing capabilities for force projection into China's 'near seas' or an area defined by the 'first island chain' consisting of the Kuril Islands, Japan, Taiwan, and the South China Sea. In this context, China's PLA Navy (PLAN) is gradually transforming toward a "regional [blue water] defensive and offensive type navy with extended so-called anti- access/area-denial (A2/AD) capabilities, limited expeditionary capabilities, and corresponding defensive and offensive air power."[58]

China's terms its comprehensive A2/AD strategy in terms of "active defense" or "counter- intervention", which is interpreted in the U.S. strategic thought as denying U.S. forces the freedom of action in China's 'near seas' by restricting deployments of U.S. forces into theatre (anti-access) and denying the freedom

of movement of U.S. forces already there (area denial).[59] In the long term, China envisions capabilities that would extend its strategic reach into the 'second island chain', which includes U.S. bases on Guam. In this context, Chinese air power doctrine, for example, envisions the PLA Air Force by 2030 conducting independent air campaigns within 3000 km radius of China's periphery – shifting its primary missions from traditional land-based air defense, interdiction, and close air support operations, toward deterrence and strategic strike at sea.[60]

East Asia's strategic template is thus shifting toward a mix of asymmetric anti-access/area- denial (A2/AD) threats, low-high intensity conventional conflicts in traditional flashpoints such as the Taiwan Strait or the Korean Peninsula, and a range of non-traditional security challenges such as energy security, cyber security, and intra-regional competition in territorial disputes in East China and South China Seas. East Asia's "hybrid" security challenges coupled with the diffusion of advanced defense technologies in nearly every battlefield domain is also widening operational requirements and compels states to adopt and adapt military capabilities and innovations of their existing or potential rivals.

The United States, Japan, South Korea, and to a lesser degree Taiwan are acquiring new power projection capabilities – from reduced-signature fifth-generation air platforms, standoff precision weapons, ballistic and cruise missiles, early warning, intelligence, surveillance and reconnaissance assets to naval assets, including maritime patrol, anti-submarine warfare, and submarines. At the same time, they are demonstrating the political willingness to use these assets for different strategic reasons. Japan seeks to overcome the limitations posed by its pacifist postwar constitution and the Yoshida Doctrine to exercise greater strategic adaptability and operational flexibility in responding to regional contingencies. Tokyo is rethinking its national defense posture and its overall security role in the region. In November 2013, Japan's cabinet under Prime Minister Shinzo Abe launched the country's first National Security Council, followed by the approval of the first National Security Strategy, and increased efforts to reinterpret Japan's pacifist constitution.[61] Meanwhile, South Korea's ongoing defense reforms and acquisition programs have aimed not only at strengthening capabilities vis-à-vis North Korean asymmetric threats, but also developing joint air and naval capabilities that would complement long-term U.S. strategic interests in East Asia.[62] The United States, with its policy of Strategic Rebalancing toward the Asia-Pacific, seeks to remain a "Pacific Power" through economic, diplomatic, cultural, and military presence and influence.[63]

These trends are also altering the strategic context in contested areas in Southeast Asia, particularly in the South China Sea. Smaller and medium-sized states in

Southeast Asia are gradually modernizing their naval and air forces to keep their vital sea lanes open, conduct intelligence missions, and perhaps most importantly, provide credible asymmetric "force multipliers" in deterring and potentially disrupting China's naval forces from seizing disputed islands in the South China Sea. While there are different political, strategic, and technological drivers shaping regional military modernization trajectories, including long-standing intraregional rivalries and competition over borders, resources, and history, most of Southeast Asian countries share concerns about China's military capabilities and future aspirations in the region. As a result of China's "coercive diplomacy" since mid-2010, Southeast Asian countries are responding by revamping their force modernization priorities, alliances, and overall strategic choices. The result is not a regional "arms race" per se (i.e. action-reaction cycle of arms acquisitions based on mutually adversarial relationships, explicit tit-for-tat arms acquisitions, the intention of seeking dominance over one's rivals through arming and intimidation), but rather a gradual "arms competition" or "arms dynamic" characterized by a mix of cooperative and competitive pressures, continued purchases of advanced weapon platforms, including the introduction of new types of arms and, therefore, unprecedented military capabilities.[64]

Emerging "Domains of Military Rivalry"

As the character and range of changes in the East Asian security dynamics becomes progressively more complex and multifaceted with the confluence of hard and soft security challenges, the prevailing strategic assessments tend to focus on projecting the varying political, strategic and technological trajectories. In this context, however, strategic intelligence is becoming increasingly difficult for the sheer number of variables, both objective and subjective, and their interactions that yield contending assessments of economic development growth-tracks, magnitudes of resources available, technological, manpower, and military advances and constraints, threat perceptions, and the nature and source of military force postures and scales. In other words, recognizing the linkages between the past, present and long-term futures, identifying key tipping points, and assessing key policy implications for optimum deployment and allocation of resources is increasingly a challenging task.

The predominant analytical spotlight is on China's increasing technological capabilities and defense production, which yield into significantly robust and visible power projection capabilities. As China's security and capabilities increase, the range of its strategic choices and options increases as well. Traditionally, China's primary strategic interests, influence, and military modernization initiatives have aimed at prevailing in any future conflict over the status of Taiwan.

While Taiwan scenarios remain the baseline for the PLA defense planning, China's military is gradually developing asymmetric warfare strategies and technologies designed to constrain U.S. freedom of action in East Asia. China's asymmetric counter-intervention strategies are backed by accelerating R&D in four mutually-reinforcing domains of "new military rivalry" – (1) outer space, (2) near space, (3) cyber space & (4) underwater. In the next five years, China will likely transfer select new weapons platforms and technologies in these domains from experimental stages into production, including next generation of ballistic missiles, nuclear and conventional, long-range precision-strike assets such as hypersonic vehicles, offensive and defensive cyber capabilities, new classes of submarines, supported by a variety of high-tech directional rocket rising sea mines with accurate control and guidance capacity .

A closer look on China's long-term strategic military programs yields evidence of deep integration with China's advancing civilian science and technology base, which in turn is increasingly linked to global commercial and scientific networks. Technology transfers, foreign R&D investment, and training of Chinese scientists and engineers at research institutes and corporations overseas are part of China's "indigenous innovation" drive to (1) identify, (2) digest, (3) absorb, and (4) reinvent select technological capabilities, both in civil and military domains.[65] In the process, China is benchmarking emerging technologies and similar high-tech defense- related programs in the United States, Russia, India, Japan, Israel and other countries.[66] Most notably, China's *"indigenous innovation"* strategy is embedded in the 2006 National Medium to Long-term Plan (MLP) for the Development of Science and Technology (2005-2020).67 The MLP is Beijing's most ambitious science and technology plan to date with special long-term total funding estimated at 500 billion RMB (US$75 billion). The plan is as a follow-up to the highly acclaimed National High Technology Program ("863") launched in March 1986 - the most important China's civilian-military R&D program next to the *"Two Weapons, and One Satellite"* science and technology development plan of 1956-67.[68] The 863 Program featured a concurrent development of dual-use technologies applicable in both civilian and military domains. The program had initially focused on developing seven strategic priority areas: laser technology, space, biotechnology, information technology, automation and manufacturing technology, energy, and advanced materials. In the mid-1990s, China expanded these areas in size, scope, and importance, shifting its trajectory toward cutting-edge technological products and processes.[69] The 863 Program is ongoing, funding projects such as the Tianhe-1A and Tianhe-2 supercomputers.[70]

Central to the MLP are 16 National Megaprojects – vanguard S&T programs – "priorities of priorities" – designed to transform China's science & technology

capabilities in areas such as electronics, semiconductors, telecommunications, aerospace, manufacturing, pharmaceuticals, clean energy, and oil and gas exploration. The megaprojects include both civilian and military areas, with 13 listed and three "unannounced" areas classified. Indeed, the 16 Megaprojects have been a source of considerable controversy and debates both in China and abroad, given the continuing structural, technological, and manufacturing challenges that inhibit disruptive innovation in Chinese defense science & technology system. The debate has also focused on the three classified megaprojects. Recent analysis suggests three prime candidates for the military megaprojects:[71]

Shenguang Laser Project for Inertial Confinement Fusion

The Shenguang (Divine Light) laser project explores the inertial confinement fusion (ICF) as an alternative approach to attain inertial fusion energy (IFE) – a controllable, sustained nuclear fusion reaction aided by an array of high-powered lasers. The lasers essentially heat and compress pellet-sized targets typically containing two hydrogen isotopes, deuterium and tritium, sending shock waves into the center and releasing energy that heats the surrounding fuel, which may also undergo fusion. Shenguang aims to achieve such "burn" – fusion ignition and plasma burning by 2020, while advancing research in solving the complex technological challenges associated with controlling the nuclear reaction.[72] Shenguang's target physics, theory and experimentation, began as early as 1993. By 2012, China completed the Shenguang 3 (Divine Light 3), a high-powered super laser facility based in the Research Center of Laser Fusion at the China Academy of Engineering Physics – the research and manufacturing center of China's nuclear weapons located in Mianyang. In this context, Shenguang has two strategic implications: it may accelerate China's next-generation thermo-nuclear weapons development, and advance China's directed- energy laser weapons programs.[73]

Second Generation Beidou Satellite Navigation System

The second prime candidate for China's 'unlisted' megaprojects is likely the Beidou-2 Satellite System (BDS), formerly known as the Compass Navigation Satellite System (CNSS). According to HIS Jane's, by the end of 2012, China had 16 operational Beidou satellites in orbit – six geostationary satellites, five Medium Earth Orbit spacecraft, and five satellites in Inclined GeoStationary Orbits covering the Asia-Pacific region. By 2020, Beidou 2 envisions a full-scale system of at least five geostationary and 30 non-geostationary satellites providing a global coverage in two modes: free "open" services available to commercial customers with 10-meter location- tracking accuracy, and restricted "authorized" services providing positioning, velocity and timing communications estimated at 10 centimeter accuracy for the Chinese government and military.[74] Beidou 2 satellites, developed by the China Academy of Space Technology, are also designed with effective

protection against electromagnetic interference and attack. Notwithstanding its wide commercial utility, the BDS will enable the PLA to significantly enhance its global navigation, tracking, targeting capabilities, providing guidance for military vehicles, ballistic and cruise missiles, precision-guided munitions, as well as unmanned aerial vehicles. Most importantly, the BDS eliminates China's dependency on the US GPS and Russia's GLONASS satellite navigation systems that could be deactivated in select areas in times of conflict.[75]

Hypersonic Vehicle Technology Project

While data on China's hypersonic research remains scarce, there are signs that China is developing conceptual and experimental hypersonic flight vehicle technologies such as hypersonic cruise vehicles (HCV) capable of maneuvering at Mach 5 speeds (6,150+ km/h), and flying in near-space altitudes. Andrew Erickson and Gabe Collins analyzed China's Shenlong (Divine Dragon) spaceplane project, including its apparent test flight in 2011 and noted subsequent profusion of Chinese research articles on the subject.[76] Similarly, Mark Stokes from the Project 2049 Institute identified new research institutes focusing exclusively on the design and development of hypersonic test flight vehicles, including the 10th Research Institute (also known as the Near Space Flight Vehicle Research Institute) under the China Academy of Launch Technology (CALT) – China's largest entity involved in the development and manufacturing of space launch vehicles and related ballistic missile systems. The Qian Xuesen National Engineering Science Experiment Base in Beijing's Huairou district is also one of China's key HCV research centers.[77]

Taken together, the above examples of China's long-term DSTI programs reflect not only Beijing's scientific aspirations, but also changing strategic priorities and PLA's long-term operational requirements embedded in the concept of "diversified missions" (The Diversified Employment of China's Armed Forces) that are vital to China's "core interests." Ever since the late 1990's, the PLA has been selectively upgrading its existing weapons systems and platforms, while experimenting with the next generation of design concepts. These can be seen in the gradual modernization of China's nuclear and conventional ballistic missiles, integrated air, missile, and early warning defense systems, electronic and cyberwarfare capabilities, submarines, surface combat vessels and the introduction of fourth/fifth generation of multi-role combat aircraft.[78] With the qualitative shifts in "hardware", the PLA has been also revamping its "software" - military doctrine, organizational force structure, and operational concepts that are now focused on "local, limited wars under informatization."[79] In particular, the prevailing emphasis in Chinese strategic thought is on "integrated networked attack and defense" air, sea, land, cyber and space operations that would amplify PLA's capabilities in terms of early warning, intelligence, and information superiority, firepower,

mobility, and operational reach. By 2030, for example, Chinese air power doctrine envisions conducting independent air campaigns within 3000 km radius of China's periphery – shifting its primary missions from traditional land-based air defense, interdiction, and close air support operations, toward deterrence and strategic strike at sea. In this context, PLAAF's concept of "integrated attack and defense" – joint counter-air strike campaigns in conjunction with the Second Artillery's anti-ship ballistic missile (ASBM) capabilities are seen as vital in defending China's territorial and sovereignty claims, as well as in limiting potential adversaries (U.S) strike, access options, and maneuver capabilities. Consequently, in potential future conflict flashpoints such as the Taiwan Strait, Korean Peninsula, East and South China Seas, selected PLA units may be able to mitigate, at least to a limited extend, the traditional operational advantages and unrivaled freedom of action of U.S. forces in East Asia.

The JAM-GC (Air Sea Battle) Debate

The growing importance and complexity of East Asia's security challenges, including the strategic and operational consequences of China's ongoing military modernization, is increasingly shifting U.S. strategic focus and debates. In September 2009, the US Navy and Air Force signed a classified memo to initiate an inter-service effort to develop a new joint operational concept: the Air-Sea Battle (ASB). Emulating intellectual transitions in military doctrine along the lines of the AirLand Battle developed in the early 1980s to counter advances in Soviet operational art, the ASB has been designed at the strategic level to preserve stability and sustain U.S. power projection and freedom of action in the western Pacific, and at the operational level to offset current and anticipated A2/AD asymmetric challenges. At the declaratory level, the ASB as such, does not specifically target China as an adversary, but is inherently designed to limit China's emerging A2/AD systems and capabilities. Since its inception, however, the ASB has been hindered by strategic ambiguity and uncertain operational consequences. Notwithstanding two semi-official reports published by the Center for Strategic and Budgetary Assessments and the recent Joint Staff publication entitled 'Joint Operational Access Concept' (JOAC), the US Department of Defense (DoD) has not articulated in detail the purpose, end or degree to which the ASB concept is necessary. Instead, the DoD has attempted to convey a broader strategic rationale behind the ASB in the context of restoring and sustaining a stable military balance in the western Pacific by strengthening deterrence vis- à-vis China, and providing US allies with security assurances. In February 2015, the DoD renamed the ASB concept into Joint Concept for Access and Maneuver in the Global Commons (JAM-GC).

U.S. allies in East Asia, however, have not fully embraced the concept nor the rationale behind it. Indeed, South Korea, Japan, Australia and other U.S. partners in the region have been relatively quiet on the implications of the JAM-GC, largely because they do not share the full extent of the planned operational details, which are classified. Such hesitance is also attributable to concerns, from the allied perspective, over the extent to which the JAM-GC provides strategic reassurance as opposed to representing abandonment by the US. Indeed, the U.S. has not clarified the link between the JAM-GC concept and its 'rebalancing strategy' in the Asia-Pacific region, nor what particular aspects of the JAM-GC will be relevant for future allied interoperability requirements and involvement. Moreover, at the operational level, U.S. allies question whether implementing the JAM-GC concept would actually mitigate military effectiveness and the defense of proximate U.S. allied bases in the region.

In a hypothetical crisis scenario or future conflict in which China could use its increasingly sophisticated A2/AD capabilities, the JAM-GC envisions a pre-emptive, standoff, precision strike – or 'Networked, Integrated Attack-in-Depth' – initiated and carried out by U.S. forces alone, in three distinct phases. First, by striking the PLA's intelligence, surveillance and reconnaissance (ISR) assets from afar through a 'Blinding Campaign' in order to deny their situational awareness: by reducing the PLA's ability to 'see deep', U.S. aircraft carrier groups would thereby gain access to the battlespace. Secondly, by carrying out a 'Missile Suppression Campaign' to disrupt PLA air-defence networks, using stealthy long-range platforms, supported by submarine-launched weapons and sensors. Through this destruction or degradation of Chinese critical air-defence assets and the consequent achievement of air superiority, U.S. forces would be able to attack PLA land-based missile launchers, surface-to-surface missiles and their supporting infrastructure. Thirdly, by conducting diverse follow-on operations, such as 'distant blockades' to seize the operational initiative and ensure protracted US freedom of action in the region.

In this context, U.S. allies in the region question whether and to what extent the JAM-GC foresees active allied participation in the envisioned 'deep-strike missions' targeting China's surveillance systems and the long-range missiles dispersed across the mainland. This operational uncertainty in turn translates into broader strategic uncertainty, in which future alliance credibility may be compromised. Consequently, if the JAM-GC indeed comes to shape U.S. operational conduct, U.S. allies in the region may feel the need to devise alternative defense strategies, and rethink the pace, direction and character of their military modernization, including their resource allocation and weapons acquisition priorities.

However, with the prevailing emphasis in the media, think-tanks and ultimately the military services on decoding the JAM-GC itself, there has been a lack of awareness of the recent emergence of critical responses to the JAM-GC and the evolution of alternative strategies and innovative concepts within the US military. Opponents of the JAM-GC point to the high escalatory risks resulting from projected deep-strike operations against China, including the possibility of a nuclear response. Critics also point to the fact that implementing the JAM-GC would require substantial investment in the next generation of networked C4ISR systems (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), submarines, long-range conventional strike systems (including stealth bombers and anti-satellite weapons), strike fighters and innovative unmanned technologies, which the U.S. defense establishment may not be able to afford.

The emergence of conceptual alternatives to the JAM-GC is also propelling inter-service debates within the US military. One of the key alternative concepts is the "Offshore Control" strategy currently emerging within the National Defense University. Offshore control refrains from initiating deep precision-strike campaign against China to gain access to the battlefield. Instead, it reverses the JAM-GC concept by relying on the U.S.'s maritime superiority to threaten to limit the freedom of action of Chinese warships and commercial ships in the contested areas vital to China's sea lines of communications (SLOCs). The office of the chief of naval operations is also considering a scaled-down JAM-GC alternative that envisions relying less on expensive stealth platforms; instead utilizing higher sortie rates from both proximate allied bases and the U.S. Navy's aircraft carriers deployed in the region. The U.S. Army, meanwhile, has been critical to the initial ASB concept, given its neglect for U.S. expeditionary and ground forces. With the renaming to JAM-GC, the US Army is integrating its own 'Joint Concept for Entry Operations' into the JAM-GC that envisions amphibious, airborne and air-assault operations to gain and maintain inland access to the adversary's territory.

Notwithstanding the ongoing inter-service debates within the U.S. military, the JAM-GC concept will be tested and calibrated with changing strategic realities, available defense resources, and the operational experience of U.S. forces. While it is unclear whether or when the concept will be fully implemented amid varying institutional and organizational support, technological and budgetary requirements and operational uncertainties, its adaptation trajectory will have significant policy implications for U.S. allies not only in East Asia, but also in Europe. Indeed, the emergence of contending operational concepts provides an important background for the projection of potential paths and patterns of future warfare. This is because the JAM-GC debate challenges not only the established

interoperability roles and missions of U.S. allies at the operational level but, more importantly, it outlines the contours of the next Revolution in Military Affairs (RMA), which will shape the defense planning and operational conduct of other advanced militaries. In this context, the emerging strategic competition in East Asia will inevitably drive U.S. strategy toward the Asia-Pacific, and accelerate the diffusion of military innovation that will provide greater lethality, precision, range and an overall increase in power-projection capabilities.

Conclusion

The implications of the JAM-GC as an emerging concept, process and debate are not confined to the U.S. or China alone; indeed, U.S. allies and partners in East Asia should explore, benchmark and debate the applicability and implications of these debates in terms of their own evolving strategic narratives and military innovation paths. Detecting, predicting and responding to military innovation or new approaches to combat in different geostrategic settings is vital to ensuring strategic and operational adaptability in advanced military establishments. Comparative perspectives and studies of military innovation trajectories, whether in terms of 'hardware' or 'software', in different geostrategic settings can help defense policy-makers to detect changes in approaches to combat; and in doing so, prompt a new debate on the validity of their countries' established strategic paradigms and operational art. In this context, the character of Sino-U.S. strategic competition will therefore gradually shape not only the political processes but the manner how both states use military power, and subsequently accelerate the development of new weapons, technologies and concomitant strategies and operational concepts. The resulting new capabilities will drastically change the functioning and effectiveness of military forces on both sides of any future major conflict. As new strategic realities create new powers, new types of future conflicts emerge. Select military technologies and capabilities will also diffuse to other major and many minor military powers, reshaping the paths and patterns of military innovation. In short, the confluence of new strategies, technologies, organizations, and doctrines in the broader context of global power transitions will shape the direction, pace, character, and outcome of military change in East Asia.

DISRUPT OR BE DISRUPTED: MANAGING POTENTIALLY DISRUPTIVE MILITARY TECHNOLOGIES IN THE CONTEXT OF EAST ASIAN SECURITY

James Hasik and Byron Callan

Abstract

Just what makes a military technology disruptive? How does one know who will disrupt, and who will be disrupted? How can we aim to develop disruptive technologies, and how can spot them before others use to them disrupt our security? Recent studies suggest that five factors matter most in developing those technologies into real military capabilities: financial resources, industrial readiness, systems integration, cultural receptivity, and organizational capacity.

While East Asian states face many common security problems, their internal situations vary widely. But even with relatively circumscribed abilities, prototyping and field experimentation can focus the powers of the available inputs, and help make the potentially disruptive ultimately decisive in keeping peace or winning wars.

Defining Disruption

A *disruptive* technology changes the dynamics of competition in ways that are both profound and unexpected. The concept comes from business competition, as first proposed by Clayton Christensen of Harvard Business School in his 1997 book *The Innovator's Dilemma*.[80] The alternative is a *sustaining* technology, whose development reinforces existing patterns of competition. Today, citing Christensen's work on disruption in business has become popular amongst almost everyone studying military innovation.[81] But defining disruption is important, lest pundits abscond with the term in the same manner as *transformation*—applied to anything fashionable in the Rumsfeld era. In the military context, a disruptive technology radically alters the strategic balance. Cases from the turbulent hundred years after 1850 readily come to mind: railroads, steamships, machine guns, aircraft, and nuclear weapons.

In each instance, another military technology was supplanted, and by technologies that initially offered seemingly unimpressive performance. But the disruption induced can extend well beyond armaments, bringing unforeseen alternations to the very makeup of society.[82] This is because disruptive technology "offers

capabilities that were not available— and were in many ways unimaginable—a generation earlier, and in so doing provokes deep questions whose answers are not readily available."[83] The historical narrative is familiar: the stirrup increased the social importance of horse-owning nobility, the longbow checked it, and the power of cannons finally killed it in favor of the centralized state.

Spotting and Mastering a Coming Disruption

Even the powerful and resourceful United States has struggled with foreseeing disruptive change, and most assuredly in its campaigns in Asia. As former Secretary of Defense Robert Gates observed in his recent memoir, "in the forty years since Vietnam, our record in predicting where we will be militarily engaged next, even six months out, is perfect: we have never once gotten it right."[84] Finding the weapons needed for those wars may be scarcely less challenging. A framework can help, and a host of recent studies suggest five factors:

Financial resources are essential. More expensive technologies advantage wealthier countries, or those with less costly strategies.[85] The threat of disruption is thus less when militaries have simpler tasks, or fewer constraints on resources. Consider the lagging British response to unrestricted submarine warfare in the First World War. The U-boats derived cover from the German High Seas Fleet, even as a mere fleet-in-being. Counterfactually, had the Royal Navy more money, it might have maintained its lead in dreadnoughts and built enough destroyers to protect both the battle line and merchant shipping.[86]

Money can also be spent strategically to induce unaffordable reactions by potential opponents. Consider one Cold War argument over intercontinental bombers and ballistic missiles. Alain Enthoven, the economist, calculated that the entire nuclear mission could be most cost- effectively undertaken with ballistic missiles. Glenn Kent, the Air Force general, argued that aircraft would greatly complicate the defense of the huge expanse of the Soviet Union, forcing Moscow to spend money it did not have.[87] More revolutionary technologies would later induce greater trepidation. As the Economist noted in its memorable 1995 survey of military technology, "Russia had neither the resources nor the technology to realize all of Marshal Ogarkov's ideas. America has."[88]

Of course, more money is not strictly better. Disruption often comes from firms whose products Dill a market need below the performance of products from the established militaries or firms. It's an old dynamic: in the fourteenth century, longbows had to be cheaper than plate mail and horses, as Medieval England was never as wealthy as France. Honda's motorcycles are a recent and classic

commercial example. Today, Apple spends far less proportionately on research and development than Microsoft, but is scarcely less innovative. But citing that legendary firm also establishes the size of the problem for modern militaries with constrained budgets. Apple's $6 billion in annual spending is only somewhat less than the $8.5 billion that the US Army spends on all its research and development. That is a great deal of lot of money for dreaming up new gadgets, and there is no live-fire testing to pay for.[89]

Industrial readiness forges latent technologies into actual weapons. Consider how France was a leader in aircraft design during the First World War. France's industry was ravaged by the Depression, but Germany's literally started from scratch after Versailles. Yet France poured most of its postwar resources into its army, never catching up in aviation, even though it had access to the same technologies as Britain and Germany. Resource allocation and poor industrial organization contributed to its defeat.[90] Later, Germany invested heavily in potentially disruptive technologies: cruise missiles, ballistic missiles, and jet- powered fighters. But German industry could not produce those bleeding-edge weapons in sufficient quantities, and was hampered by too-close supervision by military and political authorities, who imposed too- frequent design changes. The result was chaos, craft production, and stunted capacity.[91]

When military-industrial readiness is not enough, governments may look to commercial technologies for disruptive options. Aircraft design was a commercial business before the First World War, and military designs drew on commercial advances in the Interwar period. Today, improvisation of Afghan explosives draws from Pakistani fertilizer plants. Even in the United States, a range of new weapons has derived from technologies of commercial provenance: the first Predator drones flew with snowmobile engines, and the Navy's Spearhead-class transports are militarized catamaran car ferries.[92] Of course, not all commercial analogs to military technologies will be battle-ready, as military needs are often more demanding.[93] The key is ascertaining which requirements can be reasonably relaxed.

Systems integration fuses discrete technologies, which are rarely war-winners in their own right. Proximity fuses, radar and heavy bomber engines may be counter-examples from the Second World War, in that they added important capabilities without requiring years of integration to mate them to existing systems. Atomic weapons were important in winning the war against Japan, they were not the sole reason for victory. Furthermore, the history of atomic weapons is a reminder that monopolies can be fleeting. The US monopoly lasted just four years—until 1949, when the Soviets exploded their own weapon. Overall, what mattered much more in the Cold War was the superior Western capacity to combine multiple

technologies— particularly in electronic systems—into integrated war-fighting systems.[94]

With many recent weapon programs, integrating the electronic hardware and software has often required a decade or more. In development, time is money, but around NATO, member states' military budgets have been at best flat. Defense production seems to be globalizing, so tapping into skills and capacity around the world is appealing.[95] This broader supply base is yet to motivate weapons buyers in the Pentagon, but it may provide less wealthy actors greater access to advanced technologies.[96] If so, the advantage of the first movers may be fleeting.

Cultural receptivity brings the flexibility for organizational thinking about disruption.[97] Given their culture, military forces generally can 'be all they want to be'—their past organizational experiences help determine which strategic and technological opportunities they pursue.[98] Thus, even as culture opens some avenues for change, culture closes others.[99] A service's culture "screens out some parts of 'reality' while magnifying others".[100] For cultural and other institutional reasons, military organizations sometimes persist with old priorities and programs well after previously secondary missions have risen in importance.[101] Different military services within a single nation can have quite different cultural outlooks.[102] Consider the difference between the US Air Force's reluctant acceptance of armed drones and the US Navy's embrace of cruise missiles. The Navy's surface admirals wanted an offensive weapon, and after overcoming resistance from the aviation admirals, got the Tomahawk and Harpoon.[103] The USAF's fighter generals, however, dominated the culture of their service after the Cold War, and were not interested in flying missions from a cubicle. The military leadership of the Air Force thus resisted expanding the Predator force even as it was being heavily employed over Afghanistan and Iraq.[104] Serious adoption took direction from Defense Secretary Gates and his appointment of Norton Schwartz, a transport pilot, as chief of staff.[105]

Cultural dispositions can affect not just rates of adoption, but even fundamental interest in change.[106] Consider how Ottoman Turkey and Manchu China totally failed to adopt the innovations of the nineteenth century, while Meiji Japan "spectacularly made the transition."[107] Willingness to tolerate social change may account for the difference. The Ottomans rejected Western practice as they feared Christian influence on Islamic society— until Ataturk rejected the Ottomans.[108] Like Napoleon's early opponents, the samurai couldn't imagine arming peasants, but reformers in France and Japan alike embraced the idea as modernity.[109] Instead, the security policies of the anciens régimes were focused internally, in forlorn efforts to shore up their existing orders.[110] This is why, even in the modern context, disruptive

innovations may be best disguised as sustaining ones lest they encounter too much political resistance.[111]

Organizational capacity is the human analog to systems integration. Troops must be trained, tactics devised, and procedures mastered before a new technology can be employed effectively. The likelihood of successful adoption varies strongly with the operational complexity of the weapon system. For example, proliferation of ballistic missiles is threatening in part because it is administratively simple. Organizing, training, and equipping a Scud brigade is a task that even Iraq managed before 1990, despite a Stalinist approach to personnel management that crippled much of the rest of its military.[112] In contrast, despite the huge surplus of carriers after the Second World War, only a handful of countries have ever convincingly operated them with fixed-wing aircraft. The choreography of flying, deck, and hangar bay operations is truly difficult to master.[113] In this context, the difference in the pace of development in the Chinese Second Artillery and the Chinese Navy's carrier force may be stark, but it is understandable.

Wealthy countries do have greater resources to bring to challenges, but they sometimes fail to force the necessary changes on military bureaucracies.[114] The question encompasses not just technologies, but how they are applied. Consider the tanks in the 1930s: the British organized all-tank armored brigades, the French penny-packeted them as infantry support, but the Germans created combined arms panzer divisions. British and French tanks were actually better than the German models of 1940, but they were organized badly, as interwar British and French doctrine permitted nothing better.

Thus, "successful military innovators must master the art of bureaucracy even as they attempt to circumvent its most anti-reformist tendencies."[115] Leaders can help them by organizing intellectual conduits for identifying, prototyping, acquiring, and experimenting with candidate technologies. Leveraging a formal process for internal dissemination of lessons learned can help immensely. Until the 1990s, this had been largely missing from the US armed forces, but great progress has been made since.[116]

Evaluating Technologies in the East Asian Context

The modern problem with identifying possibilities is that the host of technologies can be bewildering. Should military leaders thus dread becoming a modern-day shogunate? For East Asian actors, a brief review of the evolving security situation indicates where to focus concern. Throughout the region, distances are formidable, populations are urbanizing, and hinterlands remain relatively inaccessible. With

a few exceptions, interstate disputes are primarily maritime, and the quotidian security concerns remain the constant threat of extremist terrorism and the rapidly developing realm of cyber conflict.

Countries in the region possess widely varying financial resources, military-industrial capacity, and systems integration capability. These last three factors are difficult to change in the short run. But the greater powers may reasonably worry that the diffusion of inexpensive communications technologies—Internet multimedia, wireless phones, commercial encryption, big data, GPS, etc.,—is indeed leveling the military playing field.[117] Regardless of size, some of the armed forces in the region have considerable organizational capacity. The question is whether they can inculcate in their hierarchies the cultural receptivity to change that is needed to meet new challenges. Even the United States and the United Kingdom struggled during their campaigns in Iraq and Afghanistan to learn or relearn the tactics of counterinsurgency, and to procure its tools, in systems like the MRAP and the Predator drone.[118]

The list of usual suspects is then easily recounted, but who is advantaged with each is not always clear. Additive manufacturing could dramatically lower the minimum efficient scale of production operations, and provide a new basis for military-industrial competition and cooperation. The US Navy can put 3D printers on its carriers, but the Chinese can get their own printers too. Cyberattacks are now practiced by several states, and electronic espionage has become easier in that globally integrated economy. That is, if American forces seem much better networked, Chinese penetrations of those networks have been at least deeply troubling. Robotics have burgeoned in the US arsenal since the 1990s, but the Iranian Shahed drones over Damascus today are looking a lot like American Reapers, and by sheer numbers, the largest drone maker in the world is China's DJI.[119]

Indeed, the competition between the two largest actors in East Asian security is in some technological flux. Stealth has endured as a US monopoly for thirty years, though largely for the economic inability of the Soviet Union and, later, Russia to compete. As Moore's Law marches on, at least for now, the near-invulnerability of stealth aircraft is increasingly called into question.[120] Directed energy may someday permit robust defenses against ballistic missiles, but this may also allow well-funded enemies to decimate waves of strike aircraft. Rail guns could render long-range bombardment a trivial expense on the margin, but the futility of intercepting hypersonic solid slugs would make worries over China's DFThe United States, then, may encounter some danger if Pentagon strategists choose to invest simply in tomorrow's war-winning technologies, rather than in those

technologies in which they can maintain an advantage over time. If money is the matter, the Chinese, unlike the old Soviets, have plenty. But the situation for the long-standing guarantor of East Asian security is not hopeless—not just yet is cyber-stealing Chinese plans somehow a better investment. Quite the contrary—China's armed forces still suffer from serious shortcomings in human capital and organizational development, some two decades after serious modernization supposedly began.[121] The United States has remarkable leads in many areas of technology and knowledge, and in hard-to-duplicate know-how like logistics. No one military can so easily project power on its scale around the world. It is simply to say that if that lead is to be extended with selective investments, those investments must be chosen carefully, with a clear eye to the competition.[122]

Disrupting, Before Being Disrupted

War is a matter of life and death, so innovations should naturally diffuse as a matter of survival, and the speed of emulation should depend strongly on the severity of the threat.[123] Eventually, the weapons and strategies of competing powers might converge around the world.[124] But the process is not automatic: even successful militaries occasionally need external motivation for action, and institutional reinforcement of change, for bureaucracies are designed to be hard to change.[125] In wartime, that threat may be specter of defeat or the trauma of a high casualty count. In peacetime, the impetus can be harder to summon, as staff need a conviction that the leadership will stand by its reforms.[126] One could emphasize organizational capacity, which is foremost for building the flexibility needed to respond in crisis, but the long gestation period of some weapon systems makes this a problematic way of mitigating technological surprise.[127] Technical intelligence and cooperation with sophisticated allies like the United States can help, but someone must ultimately invest and build capacity. In particular, national security leaders around the region should consider two under-appreciated steps:

Prototyping builds the needed industrial readiness and tests the possibility for systems integration. Science-fair experiments spur thinking, but ultimately only real weapons help the troops. The contractors supplying those weapons also need the prospect of earning a return on their investments. Defense ministries thus need to spend vigorously on not just research, but development. Applying monies at what the Pentagon calls the 6.4 (advanced component development and prototyping) and 6.5 (systems development and demonstration) levels is important, for these are where actual prototypes are funded. Full prototyping is admittedly more challenging for states without well-established armaments industries. But two other approaches can help economize with scarce funds. In the near term, devoting some of research budgets to modification of off-the-shelf

purchases can provide an easy entry into leading-edge development. In the longer run, the promise of additive manufacturing may reduce the minimum effective scale of participation in the global competition for new and better systems.

Field experimentation is then needed to test the new systems and the ideas behind them. While this happens to some extent in the cyber realm, it is largely adhocracy elsewhere. One option would be to establish permanent, small-scale "opfors" (opposing forces) equipped with potentially disruptive systems. The US and Australian Armies have named OpFors and several air forces maintain similar 'aggressor squadrons,' but these are largely intended to train regular forces in potential adversaries' tactics. An experimental opfor would specifically test theories about future combat, and develop the accompanying tactics and procedures, through the use of prototype equipment. Actively working out the details in the field builds organizational capacity for not just one technology, but in a repeatable fashion for future systems. Demonstrating the art of the possible helps bake new ideas into operating concepts and ultimately military culture.

Enough prototyping and experimentation might just make the operationally disruptive strategically decisive. But the game does not end there. Without a lasting occupation or an acceptable armistice, defeated powers can return to fight another day, or another decade, with the disruptive weapons they copy from the victors.[128] The globalized economy and its information flows have made many technologies and tactics available to enemies around the world. Advantage remains with actors who work to integrate new technologies into broad war fighting systems, but only if they work.

Endnotes

[1] Guidelines on The Use of Foreign Military and Civil Defence Assets in Disaster Relief ("Oslo Guidelines") have been updated based on the layout of the 2003 "Guidelines on the Use of Military and Civil Defence Assets to
Support United Nations Humanitarian Activities in Complex Emergencies" ("MCDA Guidelines") several times. For more information on the guidelines, see UN OCHA: www.unocha.org

[2] For more information on the Sphere Standards, see the Sphere Project: www.sphereproject.org/

[3] Lulf, Charlotte and Katharina Behmer. 2015. Deconstructing Fortresses: The Protection of People Fleeing Armed Conflict in Human Rights and Migration Laws. Paper presented at the International Studies Association Annual Convention, New Orleans, LA, USA, 18th February.

[4] For more information on ALNAP, see www.alnap.org/

[5] For more detail on humanitarian principles, see UNOCHA: https://docs.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf

[6] World Humanitarian Summit website. 2015. See: http://www.worldhumanitariansummit.org/whs_about

[7] Ruland, J. 2011. Southeast Asian Regionalism and Global Governance: "Multilateral Utility" or "Hedging Utility"? Contemporary Southeast Asia, 32(1), 83-112.

[8] Pennisi di Floristella, A. 2013. Are non-traditional security challenges leading regional organizations towards greater convergence? Asia Europe Journal, 11(1), 21-38.

[9] Ibid.

[10] Caballero-Anthony, M. 2010. Non-Traditional Security Challenges, Regional Governance, and the ASEAN Political Security Community (APSC). Asia Security Initiative Policy Series, 7.

[11] Caballero-Anthony, M. 2008. Non-traditional security and infectious diseases in ASEAN: going beyond the rhetoric of securitization to deeper institutionalization. The Pacific Review, 21(4), 507-525.

[12] Tan, S. S. 2005. Non-official Diplomacy in Southeast Asia: "Civil Society" or "Civil Service"? Contemporary Southeast Asia, 27(3), 370-387.

[13] United Nations General Assembly resolution 46/182, available here: http://www.un.org/documents/ga/res/46/a46r182.htm

[14] The guidelines for the International Federation of the Red Cross Red Crescent Societies' (IFRC) International Disaster Response Laws, Rules and Principles (IDRL) on the Domestic Facilitation and Regulation of International Disaster Relief and Initial Recovery Assistance are available here: http://www.ifrc.org/en/what-we-do/idrl/idrl-guidelines/

[15] The WCA 2011 Resolution is available here: http://www.wcoomd.org/en/about-us/legal-instruments/~/media/A0C1DEE96F944E08BCD48FFDD1A7D4B7.ashx

[16] For more information on UN Humanitarian Response Depot in Subang, see here: http://

www.unhrd.org/?page_id=102

[17] The full agreement title is 1976 Declaration of ASEAN Concord I and ASEAN Declaration on Mutual Assistance on Natural Disasters, 2003 Declaration of ASEAN Concord II.

[18] The full title is Declaration on Action to Strengthen Emergency Relief, Rehabilitation, Reconstruction and Prevention in the Aftermath of the Earthquake and Tsunami Disaster of 26 December 2004.

[19] The full title of the action plan is the Hyogo Framework for Action 2005 – 2015: Building the Resilience of Nations and Communities to Disasters. More information is available: http://www.unisdr.org/we/coordinate/hfa

[20] The ASEAN Agreement on Disaster Management and Emergency Response: Work Programme 2010 – 2015 is available here: http://www.asean.org/resources/publications/asean-publications/item/asean-agreement-on-disaster-management-and-emergency-response-aadmer-work-programme-2010-2015-4th-reprint

[21] Remarks by Said Faisal at Building Civil-Military Capacity for Disaster Relief Operations conference, Singapore, 11 – 12 September 2014.

[22] The RHCC Fact Sheet is available here: http://www.mindef.gov.sg/imindef/press_room/official_releases/nr/2014/sep/12sep14_nr2/12sep14_fs.html#.VPeR0vmUeLE

[23] Martinez, Gloria. 2014. 'Lessons Learnt from Recent Disaster Relief Operations – a conceptual approach'. Presented at Building Civil-Military Capacity for Disaster Relief Operations conference, Singapore, 11 September.

[24] Ong, Melvin. 2014. 'Enhancing civil-military coordination – perspectives from Christchurch'. Presented at Building Civil-Military Capacity for Disaster Relief Operations conference, Singapore, 11 – 12 September.

[25] Ibid.

[26] Ibid.

[27] Quayle, L. 2012. Bridging the gap: an 'English School' perspective on ASEAN and regional civil society. The Pacific Review, 25(2), 199-222.

[28] Nokia Siemens Network, Internet For Next Billion, www.nokiasiemensnetworks.com

[29] INSIGHTS, 2013 Southeast Asia Digital Future in Focus, 25 July 2013, https://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Southeast_Asia_Digital_Future_in_Focus

[30] The Center for Strategic and International Studies, June 2014, Net Losses: Estimating the Global Cost of Cyber Crimes – Economic Impact of Cyber Crime II [5] McAfee Virtual Criminology Report 2007.

[31] EUROPOL, The Internet Organised Crimes Threats Assessment (iOCTA) 2014.

[32] DELL SecureWorks: Underground Hacker Markets Report 2014.

[33] McAfee Virtual Criminology Report 2007.

[34] Global Energy Cyberattacks: "Night Dragon" McAfee® Foundstone® Professional Services and McAfee Labs™ February 10, 2011

[35] SANS Institute, Top Ten Cyber Menaces for 2008.

[36] PC Word Business Center Economic 2008.

[37] Sofpedia, Nettraveler Espionage Campaign Makes 350 High-Profile Victims In 40, Countries, 4 June 2013, http://news.softpedia.com/news/NetTraveler-Cyber-Espionage-Campaign-Compromises-350-High-Profile-Victims-in-40-Countries-358427.shtml

[38] Asian School of Cyber Law, India

[39] Nathan Thornborough, "The Invasion of the Chinese Cyberspies (and the man who tried to stop them): An Exclusive Look at how the Hackers called TITAN RAIN are Stealing U.S. Secrets," Time Magazine, September 5, 2005. http://www.cs.washington.edu/education/courses/csep590/05au/readings/titan.rain.htm

[40] Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0071772499, ISBN 978-0071772495

[41] The Guardian, Edward Snowden: A Whistleblower, Not A Spy, 2 July 2013, http://www.theguardian.com/commentisfree/2013/jul/02/edward-snowden-whistleblower-not-spy.

[42] John O'Donnel, Reuter, EU Commission pushes to dilute U.S. Internet influence, 12 February 2014, http://www.reuters.com/article/2014/02/12/us-eu-internet-idUSBREA1B0WS20140212

[43] Ronald Byrne, The Star News, Hacker Group Tells Why It Wants to Attack Malaysian Govt Portal, 14 June 2011, http://thestar.com.my/news/story.asp

[44] The Business Times, Million Mask March: Anonymous Launches Worldwide Protest On Guy Fawkes Day 2013, 10 February 2014, http://www.ibtimes.com/million-mask-march-anonymous-launches-worldwide-protest-guy-fawkes-day-2013-photos-1456108

[45] BC News Technology, Stuxnet 'Hit' Iran Nuclear Plans, 22 November 2010, http://www.bbc.co.uk/news/technology-11809827

[46] Mathew J. Schwartz, Information Weekly Security, 7 Facts On Duqu Malware Attacks, 16 November 2011, http://www.informationweek.com/security/attacks/

[47] Steve Evans, CBR Computer Business Review, France Accuses US of Flame Malware Attack on Government Computers, 21 November 2012.

[48] Maximilian H. Nierhoff, Facebook Country Stats February 2013 – Top 10 Countries Lose Users Due To The Ongoing Account Cleanup, http://www.quintly.com/blog/2013/02/facebook-country-stats-february-2013-top-10-countries-lose-users/

[49] Jamal R. Nassar, University Technology of Sydney – News Room, The Arab Spring: Root Causes And Implications, 2 July 2012, http://newsroom.uts.edu.au/events/2012/07/the-arab-spring-root-causes-and-implications

[50] Ahmed El-Bayouk, Peoples Movement: The dangers of social media, 24 April 2011, http://peoplesmovement.weebly.com/the-dangers-of-social-media.html

[51] ASEAN Regional Forum, http://aseanregionalforum.asean.org/about.html

[52] Council for Security Cooperation in Asia Pacific (CSCAP) Study Group on Cyber Security, http://www.cscap.org/index.php?page=study-group-on-cyber-security-as-a-central-strategy-for-securing-the-cyber-environment-in-the-asia-pacific-region

[53] CSCAP Memorandum No.20, Cybersecurity as a Central Strategy For Securing The Cyber Environment In The Asia Pacific Region.

[54] Council of Europe, European Treaty Series No 185, Convention on Cyber Crime, Budapest.23.XI.2001

[56] Tellis, Ashley. 2012. "Uphill Challenges: China's Military Modernization and Asian Security." In Strategic Asia 2012-13: China's Military Challenge, by Ashley Tellis and Travis Tanner (eds.), 3-24. Washington D.C.: The National Bureau of Asian Research.

[57] Erickson, Andrew. 2012. "China's Modernization of its Naval and Air Power Capabilities." In Strategic Asia 2012-13: China's Military Challenge, by Ashley Tellis and Travis Tanner (eds.), 60-125. Washington D.C.: The National Bureau of Asian Research.

[58] Minnick, Wendell. 2014. "China Mixing Military Modernization with Tailored Coercion" Defense News, April 14, p.11.

[59] Li, Nan. 2009. "The Evolution of China's Naval Strategy and Capabilities: From 'Near Coast' and 'Near Seas' to 'Far Seas'." Asian Security 5(2): 168.

[60] Schreer, Benjamin. 2013. Planning the Unthinkable War: 'AirSea Battle' and its Implications for Australia. Barton: Australian Strategic Policy Institute. p. 8.

[61] Mastro, Oriana Skylar and Stokes, Mark. 2011. "Air Power Trends in Northeast Asia: Implications for Japan and the U.S.-Japan Alliance." Project2049 Institute Occasional Papers. p.4

[62] Hardy, James. 2014. "Strong Constitution: Japan Looks to Reset its Policy on Self-Defence." IHS Jane's Intelligence Feview, May 14.

[63] Lee, Chung Min. 2003. "East Asia's Awakening from Strategic Hibernation and the Role of Air Power." Korean Journal of Defense Analysis 15(1): 219-274.

[64] Ratner, Ely. 2013. "Rebalancing to Asia with an Insecure China." The Washington Quarterly 36(2): 21-38.

[65] Bitzinger, Richard. 2010. "A New Arms Race? Explaining Recent Southeast Asian Military Acquisitions." Contemporary Southeast Asia 32(1): 50–69.

[66] Cheung, Tai Ming, "The Chinese Defense Economy's Long March from Imitation to Innovation," pp. 343-344.

[67] DOD Defense Science Board, Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013).

[68] Xinhua, "China Issues S&T Development Guidelines," (February 9, 2006). Available at: http://english.gov.cn/2006-02/09/content_183426.htm

[69] Ministry of Science and Technology of the PRC, "National High-tech R&D Program (863 Program)," Available at: http://www.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm

[70] Tai Ming Cheung, Fortifying China: The Struggle to Build a Modern Defense Economy (Ithaca, NY: Cornell University Press, 2008).p.193-196.

[71] Brian Tsay, "The Tianhe-2 Supercomputer: Less than Meets the Eye?" SITC Bulletin Analysis (July 2013). Available at: http://igcc.ucsd.edu/assets/001/504798.pdf

[72] Andrew Erickson and Gabe Collins, "Spaceplane Development Becomes a New Dimension of Emerging U.S.-China Space Competition," China SignPost, No. 62 (16 August 2012).

[73] Michael Raska, "Scientific Innovation and China's Military Modernization," The Diplomat (September 3, 2013).
[74] Ibid.
[75] Jon Grevatt, "China Outlines Satellite Navigation System Plans," IHS Jane's Defense Industry (October 20, 2013).
[76] Mark Stokes and Dean Cheng, "China's Evolving Space Capabilities: Implications for U.S. Interests," Report Prepared for: The U.S.-China Economic and Security Review Commission (April 26, 2012). Available at: http://origin.www.uscc.gov/sites/default/files/Research/USCC_China-Space-Program-Report_April-2012.pdf
[77] Andrew Erickson and Gabe Collins, "Spaceplane Development Becomes a New Dimension of Emerging U.S.-China Space Competition," China SignPost, No. 62 (August 16 2012).
[78] Mark Stokes and Dean Cheng, "China's Evolving Space Capabilities: Implications for U.S. Interests,"p.17-23.
[79] Anthony H. Cordesman, Ashley Hess, Nicholas S. Yarosh, Chinese Military Modernization and Force Development, (Washington DC: Center for Strategic and International Studies, 2013).
[80] Andrew Erickson and Michael S Chase, "Informatization and the Chinese People's Liberation Army Navy," In: Phillip Saunders, Christopher Yung, Michael Swaine, and Andrew Nien-Dzu Yang, The Chinese Navy: Expanding Capabilities, Evolving Roles (Washington DC: Institute for National Strategic Studies, 2011).p.247-287
[80] Clayton Christensen, The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail (Boston: Harvard Business Review Press, 1997). Christensen's work built on Henderson and Clark's work on architectural product innovations. See Rebecca M. Henderson and Kim B. Clark, "Architectural Innovation: The Reconfiguring of Existing Product Technologies and The Failure of Established Firms," Administrative Science Quarterly, vol. 35, no. 1, 1990, pp. 9–30. Note also that Joseph Schumpeter's concept of creative destruction may have been the earliest forerunner to the idea.
[81] Michael Horowitz, The Diffusion of Military Power: Causes and Consequences for International Politics (Princeton: Princeton University Press, 2010), p. 45. See also Peter Dombrowski and Eugene Gholz, Buying Military Transformation: Technological Innovation and the Defense Industry (New York: Columbia University Press, 2006), pp. 18, 26–29; and Terry C. Pierce, WarIighting and Disruptive Technologies: Disguising Innovation (London: Frank Cass, 2004).
[82] John Ellis, The Social History of the Machine Gun (Baltimore: Johns Hopkins University Press, 1986).
[83] Peter W. Singer, "Foreword," in Shawn Brimley, Ben FitzGerald and Kelley Sayler, Game Changers: Disruptive Technology and US Defense Strategy, (Washington, DC: Center for a New American Security, September 2013).
[84] Robert M. Gates, Duty: Memoirs of a Secretary at War (New York: Alfred A. Knopf, 2014), p. 590.

[85] Horowitz, The Diffusion of Military Power.
[86] Mukunda, "We Cannot Go On," p. 158
[87] Glenn A. Kent, Thinking about America's Defense: An Analytical Memoir (Santa Monica: RAND, 2008), pp. 153–158. We thank John Pinder and W. Alex Vacca of Northrop Grumman for suggesting this example. In 1973, Defense Secretary Eliot Richardson made a similar argument during the defense appropriations hearings in favor of submarine-launched cruise missiles: every ship would become a potential launch platform, and the Soviets would likely deflect investments from offensive to defensive systems. See Ronald Huisken, The Origin of the Strategic Cruise Missile (New York: Praeger Publishers, 1981), p. 41
[88] The Softwar Revolution," Economist, June 10, 1995
[89] James Hasik, "Getting Faster at Revolutionary: the bureaucratic and technological challenges in speeding up weapons development," The Defense Industrialist, January 30, 2015.
[90] Robin Higham, Two Roads to War: The French and British Air Arms from Versailles to Dunkirk (Annapolis: Naval Institute Press, 2012).
[91] Daniel Uziel, Arming the Luftwaffe: The German Aviation Industry in World War II (Jefferson, North Carolina: McFarland, 2011); Richard Overy, Why the Allies Won (New York: W.W. Norton & Company, 1995
[92] James Hasik, Arms and Innovation: Entrepreneurship and Alliance in the Twenty-First-Century Defense Industry (Chicago: University of Chicago Press, 2008), chapters 3 and 5.
[93] Dombrowski and Gholz, Buying Military Transformation.
[94] Thomas P. Hughes, Rescuing Prometheus: Four Monumental Projects That Changed the Modern World (New York: Pantheon, 1998).
[95] Stephen G. Brooks, "The Globalization of Production and the Changing Benefits of Conquest," Journal of Conflict Resolution, vol. 43, no. 5, 1999, pp. 646–670
[96] Eugene Gholz, "Globalization, Systems Integration, and the Future of Great Power War," Security Studies, vol. 16, no. 4, 2007, pp. 615–636; Eugene Gholz and Daryl G. Press, "The Effects of Wars on Neutral Countries: Why It Doesn't Pay to Preserve the Peace," Security Studies, vol. 10, no. 4, 2001, pp. 4–22.
[97] Mukunda, "We Cannot Go On."
[98] Adam Grissom, "The Future of Military Innovation Studies," Journal of Strategic Studies, vol. 29, no. 5, October 2006, p. 916; Theo Farrell, The Norms of War: Cultural Beliefs and Modern Conflict (London: Lynne Reiner Publishers, 2005).
[99] Theo G. Farrell and Terry Terriff, "The Sources of Military Change," in idem, The Sources of Military Change: Culture, Politics, Technology (Boulder: Lynne Rienner, 2002), pp. 12–17.
[100] Elizabeth Kier, Imagining War: French and British Military Doctrine between the Wars (Princeton: Princeton University Press, 1997), p. 28.
[101] Mukunda, "We Cannot Go On", p. 115. For more on the analogy to submarine warfare in the recent context of counterinsurgency, see Robert W. Sadowski, Joint Improvised Explosive Device Defeat Organization: Anomaly or Future Roadmap (Carlisle Barracks: US Army War College, 2008).

[102] See Carl H. Builder, The Masks of War: American Military Styles in Strategy and Analysis (Baltimore and London: Johns Hopkins University Press, 1989).
[103] See Gregory A. Engel, "Cruise Missiles and the Tomahawk," in Bradd C. Hayes and Douglas V. Smith, eds., The Politics of Naval Innovation (Newport: US Naval War College, 1994), pp. 16–42.
[104] For the early history of the aircraft's development, see Richard Whittle, Predator: the Secret History of the Drone Revolution (Henry Holt, 2014).
[105] See again Robert M. Gates, Duty: Memoirs of a Secretary at War.
[106] See Dima Adamsky, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in
[107] Emily O. Goldman and Richard B. Andres, "Systemic Effects of Military Innovation and Diffusion," Security Studies, vol. 8, no. 4, 1999, p. 80.
[108] David B. Ralston, Importing the European Army: the Introduction of European Military Techniques and Institutions into the Extra-European World, 1600-1914 (Chicago and London: University of Chicago Press, 1990), p. 48.
[109] William H. McNeill, The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000 (Chicago: University of Chicago Press, 1982), pp. 220-221.
[110] Emily O. Goldman, "Cultural Foundations of Military Diffusion," Review of International Studies, vol. 32, no. 1, 2006, pp. 70-71.
[111] Pierce, WarIighting and Disruptive Technologies.
[112] Stephen Biddle and Robert Zirkle, "Technology, Civil-Military Relations, and Warfare in the Developing World," Journal of Strategic Studies, vol. 19, no. 2, June 1996, pp. 176–190.
[113] Horowitz, The Diffusion of Military Power, chapters 3 and 4.
[114] Horowitz, op. cit.
[115] Stephen J. Cimbala, "Forward," in Brett Steele, Military Reengineering between the World Wars (Santa Monica: RAND, 2005), p. xi.
[116] Janine Davidson, Lifting the Fog of Peace: How Americans Learned to Fight Modern War (Ann Arbor: University of Michigan Press, 2010).
[117] Paul K. Davis and Peter A. Wilson, Looming Discontinuities in U.S. Military Strategy and Defense Planning: Colliding RMAs Necessitate a New Strategy (Santa Monica: RAND, 2011). See also Michael R. Rip and James Hasik, The Precision Revolution: GPS and the Future of Aerial Warfare (Annapolis: Naval Institute Press, 2002); and the more recent James Hasik and Mark Revor, Democratized Destruction: Global Security in the Hacker Era (Washington DC: Atlantic Council, 2014).
[118] Andrew Smith, Improvised Explosive Devices in Iraq, 2003-09: A Case of Operational Surprise and Institutional Response (Carlisle Barracks, Penn.: US Army War College, 2011); and Sharon Weiner, "Organizational Interests versus Battlefield Needs: The US Military and Mine-Resistant Ambush Protected Vehicles in Iraq," Polity, vol. 42, no. 4, October 2010.
[119] Dave Cenciotti, "Iranian Shahed 129 Drone Appears over Damascus," The Aviationist, April 10, 2014.
[120] For the tactical implications, see James Hasik, "Hauling Concrete with Cadillacs: the

gradual decline of stealth may call for a high-low mix in airpower strategy," The Defense Industrialist, February 5, 2015.

[121] Michael S. Chase, et al., China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (Santa Monica: RAND, 2015).

[122] James Hasik and Alex Ward, "Third Offset Strategy, Second Adversary: What worked on the Soviets may not work on the Chinese," The Defense Industrialist, November 18, 2014.

[123] John A. Lynn, "The Evolution of Army Style in the Modern West, 800-2000," International History Review, vol. 18, no. 3, 1996, p. 509; Joã o Resende-Santos, "Anarchy and the Emulation of Military Systems: Military Organization and Technology in South America, 1870–1930," Security Studies, vol. 5, no. 3, 1996, pp. 193–260.

[124] Kenneth N. Waltz, Theory of International Politics (Reading: Addison-Wesley, 1979), p. 127.

[125] Barry Posen, The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars (Ithaca and London: Cornell University Press, 1984), p. 226; Stephen P. Rosen, Winning the Next War: Innovation and the Modern Military (Ithaca and London: Cornell University Press, 1994), p. 2.

[126] Conrad Peter Schmidt, Changing Bureaucratic Behavior: Acquisition Reform in the United States Army (Santa Monica: RAND, 2000).

[127] Meir Finkel, On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield (Redwood City: Stanford University Press, 2011).

[128] Michael Howard, "When Are Wars decisive?" Survival, vol. 41, no. 1, 1999; and Howard, "The Transformation of Strategy," RUSI Journal, vol. 156, no. 4, 2011, p. 16.

CONTRIBUTORS

Dato Seri Laila Jasa Tan Sri Rastam Mohammad Isa

Dato Seri Laila Jasa Tan Sri Rastam Mohammad Isa was appointed Chairman of the Institute of Strategic and International Studies (ISIS) Malaysia on 9 January 2015. Since 1 January 2014, he has also served as Chief Executive of ISIS Malaysia. He holds a Bachelor of Social Science (hons) egree from Universiti Sains Malaysia, a Master of Arts degree in International Relations and Strategic Studies from the University of Lancaster and a Certificate of Diplomacy from the University of Oxford.

Dato Rastam has received Federal and State awards, namely the Panglima Setia Mahkota (PSM), SSAP, PJN, SIMP, DIMP, KMN and AMN. In August 2014, he was conferred the Darjah Paduka Seri Laila Jasa Yang Amat Berjasa Second Class, D.S.L.J by His Majesty Sultan Haji Hassanal Bolkiah Mu'izzaddin Waddaulah, Sultan and Yang Di-Pertuan of Brunei Darussalam.

Dato Rastam spent more than 36 years in the Malaysian diplomatic service. He served in various capacities at the Ministry of Foreign Affairs and Malaysian diplomatic missions abroad, including as High Commissioner of Malaysia to Pakistan, Ambassador of Malaysia to Bosnia Herzegovina, Ambassador of Malaysia to the Republic of Indonesia and Permanent Representative of Malaysia to the United Nations in New York. He was Secretary-General of the Ministry of Foreign Affairs from 8 January 2006 until he officially retired from public service on 2 September 2010. Prior to his appointment as Chief Executive of ISIS Malaysia, he was Advisor at the Chief Minister's Department in Sarawak. He serves as chairman of the board of directors of one Malaysian public listed company. He also sits as director on the board of two other companies.

Dato Rastam is Chairman of the Malaysian National Committee for the Pacific Economic Cooperation Council (PECC) and Chairman of the Malaysian National Committee of the Council for Security Cooperation in the Asia-Pacific. (CSCAP).

Alistair D. B. Cook

Dr Alistair D. B. Cook is a Research fellow at the Centre for Non-Traditional Security (NTS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) in Singapore. His research interests are in non-traditional security and human security in the Asia-Pacific including peace and conflict studies, humanitarian assistance and disaster relief (HADR), foreign policy and regional cooperation, and domestic politics in Myanmar.

In 2012-2013, he was a visiting research fellow at the East Asian Institute of the National University of Singapore. Prior to his visiting research fellowship, he was Research Fellow at the Centre for Non-Traditional Security (NTS) Studies from 2009.

He has taught a variety of international relations and political science courses at both the undergraduate and graduate level at Purdue University, University of Melbourne, Deakin University, Nanyang Technological University and Australian National University. He also lectures to visiting student groups to Southeast Asia from U.S. universities. Alongside university teaching, he also lectures at SAFTI and the Civil Service College in Singapore.

He has recently co-edited a book titled Irregular Migration and Human Security in East Asia (Routledge, 2015) and Non-Traditional Security in Asia: Issues, Challenges and Framework for Action (ISEAS 2013). He has published in a variety of journals including International Politics, Journal of International Peacekeeping, China Report among others. He has also published opinion pieces in The Straits Times (Singapore), The Nation (Thailand), The Jakarta Post (Indonesia), and The Brunei Times (Brunei) as well as current affairs magazines.

Born in Cardiff, Wales, Alistair Cook was educated at Malvern College, England, graduated with a B.A. (Hons) from St. Andrews University, Scotland in 2002; Masters from Purdue University, USA in 2004, and a PhD from the University of Melbourne, Australia in 2008.

Lieutenant Colonel (Retired) Sazali bin Sukardi

Lieutenant-Colonel (Retired) Sazali bin Sukardi is the Vice-President of Strategic Research, CyberSecurity Malaysia, an agency under the Ministry of Sceince, technology and Innovation, Malaysia. He holds Master of Science in Information Security from Royal Holloway, University of London, Master of Arts in Defence Studies from King's College, University of London, Post-Graduate Diploma in System Analysis from Universiti Teknologi MARA, and Bachelor of Science in Civil Engineering from University of Hartford, Connecticut USA. He was also a Joint Warfare graduate from the Joint Services Command and Staff College, Shrivenham, United Kingdom.

His current post deals with strategic cybersecurity research works as well as exploration of new cybersecurity initiatives and policies. He was the Leading Co-Chair of the Council for Security Cooperation in Asia-Pacific Study Group on Cyber Security (2010-2012). To date, he has been representing Malaysia in several ASEAN Regional Forums and ASEAN Senior Official Roundtables. Currently, he is a part-time lecturer at Universiti Kebangsan Malaysia in MSc Cyber Security and the Malaysian Armed Forces Staff College under Executive Programme by Universiti Pertahanan Nasional Malaysia. He is also a regular guest lecturer at the Malaysian Armed Forces Defence College. He used to be a part-time lecturer in MSc Information Security at Universiti Teknologi Malaysia (2009).

Dr Michael Raska

Dr Michael Raska's research interests focus on East Asian strategic and defense issues in two aspects: technology futures and military futures. With regard to technology futures, he is interested in how certain types of technologies may affect future military capabilities and geopolitics. This includes dual-use/advanced commercial technologies; robotics and automation, cyber, new materials, and propulsion technologies. With regard to military futures, he explores how technology developments could affect future warfare in East Asia.

He has published on these issues in journals such as the Korea Journal of Defense Analysis, Pointer-Journal of Singapore Armed Forces, and Asian Journal of Public Affairs. He has contributed chapters to edited volumes for the Norwegian Institute of Defense Studies; and the Project on the Study of Innovation and Technology in China at the Institute on Global Conflict and Cooperation, University of California San Diego. His strategic assessments have been published by the Project Syndicate, Defense News, The Diplomat, East Asia Forum, RUSI Newsbrief, and many newspapers around the world. He is a frequent commentator on East Asian security issues for the CNBC, BBC World News, Al-Jazeera News, Bloomberg, Channel News Asia, and other networks.

Dr Raska has taught at the Goh Keng Swee Command and Staff College (SAF Campaign and War Studies Course) and the Lee Kuan Yew School of Public Policy (International Security). His research experiences include visiting fellowships at Yonsei University, Pacific Forum CSIS, and Samsung Economic Research Institute. He is an alumnus of the Columbia / Cornell University Summer Workshop on Analysis of Military Operations and Strategy (SWAMOS 2012), the Philip Merrill Center for Strategic Studies Workshop at Basin Harbor (2013), and the Hertog Summer Study Program (2014). He holds a B.A. in international studies from Missouri Southern State University (2000), an M.A. in international relations from Yonsei University (2002), and a Ph.D. in public policy (2012) from the Lee Kuan Yew School of Public Policy, where he was a recipient of the NUS President's Graduate Fellowship. Born in Germany in 1977, he has lived in six countries.

James Hasik

James Hasik is a Nonresident Senior Fellow for Defense with the Brent Scowcroft Center on International Security at the Atlantic Council. He is concurrently a Clements Graduate Fellow at the Clements Center of History, Strategy, and Statecraft at the University of Texas at Austin, and a William Powers Doctoral Fellow at Texas' Lyndon B. Johnson School of Public Affairs.

Since September 2001, Hasik has been researching and writing about global security challenges and the economic enterprises that provide the tools to address them. As a consultant, he has undertaken studies in operations analysis, supply chain analysis, marketing, product development, competitive analysis, facilities management, strategic planning, policy analysis, merger planning and due diligence, portfolio strategy, business forecasting, privatization planning, organizational design, and antitrust analysis.

Hasik holds an MBA in business economics from Booth School of Business at the University of Chicago, and a BA in history and physics from Duke University.

At the Atlantic Council, he is the primary author of the blog *The Defense Industrialist* (http://www.atlanticcouncil.org/blogs/defense-industrialist). More of this commentaries on technological and industrial issues affecting international security can be found at www.jameshasik.com.