
Cooperation for Security & Peace
2017
SDD
Seoul
Defense
Dialogue

TABLE of CONTENTS

Welcome Message 6
SDD 2016 Sketch 8
SDD 2017 Participants 10

SDD 2017 Overview

Basic Plan 15
Program 16
Floor Plan 22
General Information 24
Tour Plan 26

SDD 2017 Agenda Explanation

Plenary Session 30
Special Session 34

Day 2_September 7 (Thu)

Opening Ceremony 38
Plenary Session 1 39
Plenary Session 2 41
Special Session 1 49
Special Session 2 61

Day 3_September 8 (Fri)

Plenary Session 3 72
Plenary Session 4 80
Closing Ceremony 89

Cyber Working Group

Cyber Working Group 1 / 2 92

Participants

Head of Delegate 96
Official Experts 105
Civilian Security Experts 106
SDD Special Experts Group 124
SDD 2017 Preparation Office 127

모시는 글

대한민국 국방부 차관 **서 주 석**

귀하를 2017 서울안보대화에 정중히 초청합니다.

서울안보대화(SDD: Seoul Defense Dialogue)는 아 · 태지역 다자안보협력과 한반도 평화정착에 기여하기 위해 대한민국 국방부가 2012년 출범시킨 다자안보협의체로서 올해로 6회째를 맞이하게 되었습니다.

올해에는 9월 6일부터 8일까지 46개 국가와 5개 국제기구의 차관급 국방관료 및 민간 안보전문가들을 초청하여, 한반도와 세계가 직면한 안보현안에 대한 회의를 진행할 예정입니다.

본회의에서는「불확실성 시대의 안보협력 비전」이라는 대주제 하에 전세계적으로 이슈가 되고 있는 북한 핵·미사일 위협, 해양 안보, 사이버 안보 및 신종 테러리즘을 다룰 계획입니다. 또한 특별 세션에서는 지구촌 최대 관심사항인 4차 산업혁명을 국방과학기술 및 국방정책 등과 연계하여 논의하는 시간을 가질 예정입니다.

초국가적인 안보위협이 오히려 고조되고 있는 오늘날의 안보현실 속에서, 서울안보대화가 다수 국가 및 국제기구의 고위 관료들과 민간 안보전문가들의 치열한 토의를 통해 실질적 국방협력과 문제해결을 위한 대화의 장(場)이 되기를 기대합니다.

아무쪼록 2017 서울안보대화에 참석하시어 자리를 빛내주시기 바라며, 귀하의 지혜와 고견을 함께 나눔으로써 이번 회의가 보다 알차고 성공적인 결실을 맺을 수 있도록 함께 해주시면 감사하겠습니다.

서 주 석
대한민국 국방부 차관

Welcome Message

I hereby cordially invite you to the 2017 Seoul Defense Dialogue.

A multilateral security consultative body initiated in 2012 by the Republic of Korea Ministry of National Defense, the Seoul Defense Dialogue celebrates its 6th anniversary of aspiring to contribute to multilateral security co-operation in the Asia-Pacific and peace on the Korean Peninsula.

This year, Vice Ministerial defense officials and civilian security experts from 46 countries and 5 international organizations are invited to partake in discussions on security issues of the Korean Peninsula and those faced by the world.

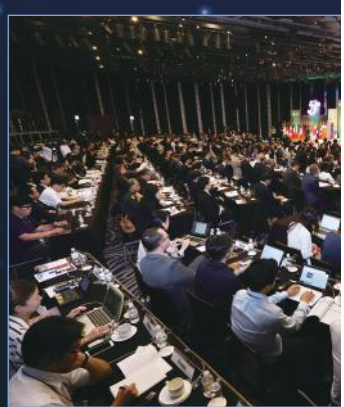
Under the main theme of "Visions for Security Cooperation in an Age of Uncertainty," Plenary Sessions will cover rising global issues including North Korea's nuclear and missile threats, maritime security, cyber security and new forms of terrorism. Moreover, Special Sessions will be utilized for interlocking discussions on the 4th Industrial Revolution - a leading topic of global interest - and defense science & technology and defense policy.

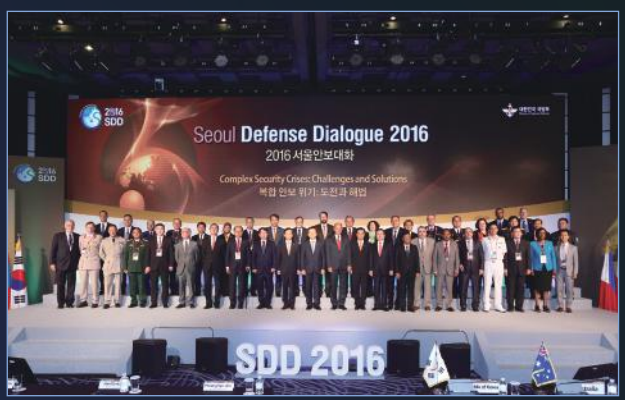
Amidst the current security climate in which transnational security threats are ever-increasing, I hope the SDD becomes a venue for dialogue where senior officials and civilian security experts from numerous countries and international organizations engage in intense discussions to promote substantial defense cooperation and to solve problems.

Wishing you could grace the 2017 Seoul Defense Dialogue with your participation, I will be sincerely grateful if you join us to share your wisdom and farsighted views and thus help bring the conference to its successful fruition.

SUH Choo-suk
Vice Minister of National Defense, Republic of Korea

SDD 2016 Sketch




Seoul Defense Dialogue 2016
2016 서울안보대화
Complex Security Crises: Challenges and Solutions
복합 안보 위기: 도전과 해법
SDD 2016


Seoul Defense Dialogue 2016
2016 서울안보대화

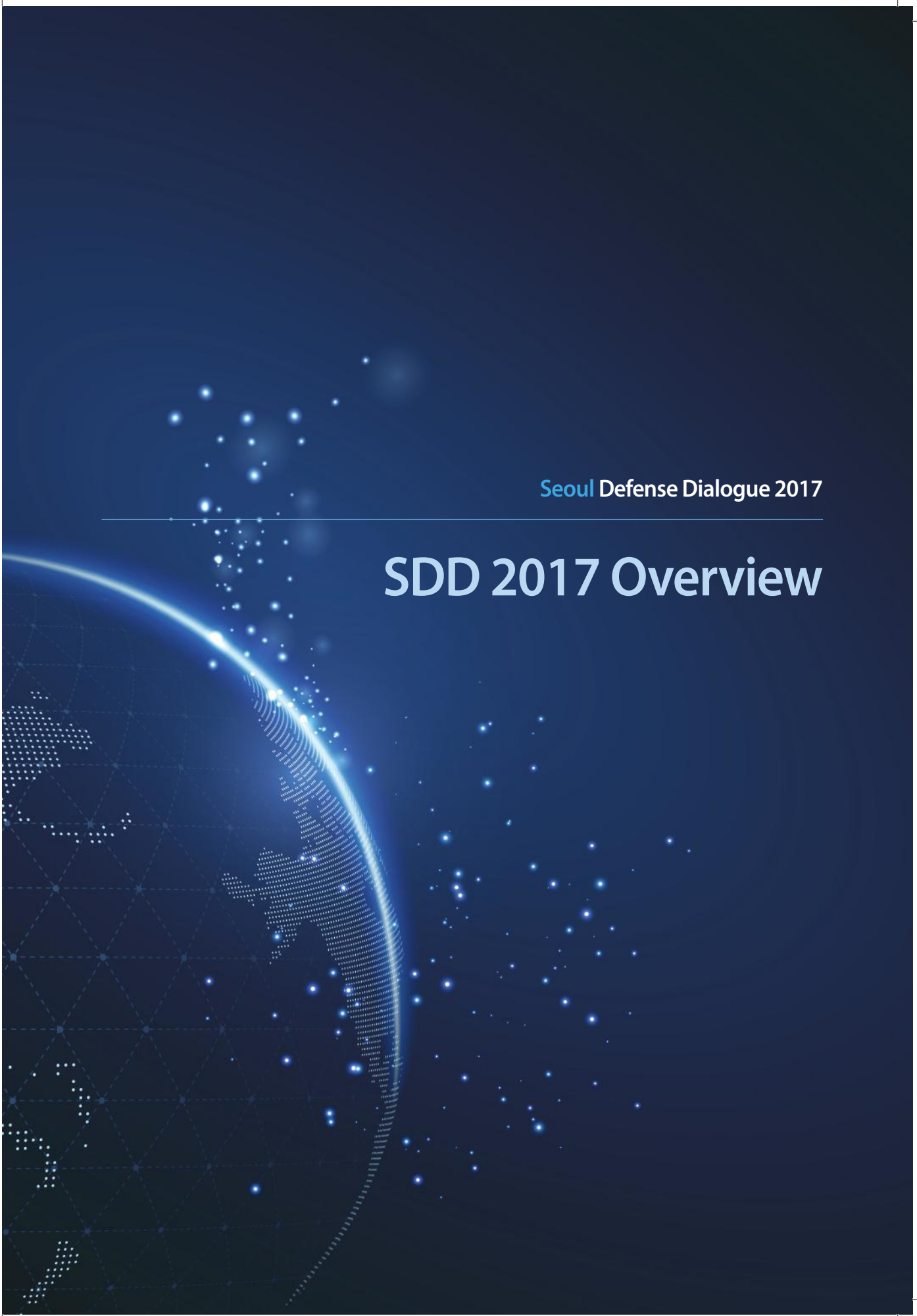

Seoul Defense Dialogue 2016
2016 서울안보대화
September 7-9


Seoul Defense Dialogue 2016
September 7-9


Douglas Paul

SDD 2017 Participants


Cooperation for Security & Peace
2017
SDD
Seoul
Defense
Dialogue



Seoul Defense Dialogue 2017

SDD 2017 Overview

Basic Plan

MAIN THEME

Visions for Security Cooperation in an Age of Uncertainty
불확실성 시대의 안보 협력 비전

DATE

September 6th (Wed)-8th (Fri)
2017년 9월 6일 (수)–8일 (금)

VENUE

The Westin Chosun Hotel Seoul
웨스틴 조선 호텔 서울

OFFICIAL LANGUAGE

English (There will be simultaneous translation into Korean, Chinese, Japanese, Russian, Spanish)
영어 (한국어, 중국어, 일본어, 러시아어, 스페인어 동시통역 제공)

PARTICIPANTS

40 Countries and 3 International organizations, Civilian security experts
40개국 및 3개 국제기구 대표단, 민간안보전문가

Program

DAY 1 September 6th (Wed)

08:00 - 17:00	Cyber Working Group 1	Orchid, 2F
	ISEC Information Security Conference Tour	COEX Exhibition Hall
18:30 - 19:00	Reception	Cosmos + Violet, 2F
	Welcoming Dinner hosted by the Vice Minister	Orchid, 2F

DAY 2 September 7th (Thu)

08:00 - 09:00	**Registration**	Lobby, 1F
09:00 - 09:40	**Opening Ceremony**	GRAND BALLROOM, 1F
	Opening Remarks	**Song Young-moo** Minister of National Defense, Republic of Korea
	Congratulatory Remarks	**Lee Nak-yeon** Prime Minister, Republic of Korea
	Keynote Speech	**Marise Payne** Minister for Defence, Australia
10:00 - 12:00	**[Plenary Session 1]** North Korea's Nuclear and Missile Threats and Security of the Korean Peninsula	GRAND BALLROOM, 1F
	Moderator	**Daniel R. Russel** Diplomat in Residence and Senior Fellow, Asia Society Policy Institute, USA
	Presenter	**Lim Sung-nam** 1st Vice Minister of Foreign Affairs, Republic of Korea
	Discussants	**Thoma W. Bergeson** Deputy Commander, USFK *** Special Briefing** **Markus Garlauskas** National Intelligence Officer for North Korea, DIA, USA **Jia Qingguo** Professor, School of International Studies of Peking University, China **Morimoto Satoshi** Chancellor, Takushoku University, Japan **Alexander I. Nikitin** Director, Center for Euro-Atlantic Security, MGIMO, Russia **SUH Choo-suk** Vice Miniter of National Defense, Republic of Korea
12:00 - 13:30	Luncheon hosted by the Deputy Speaker of the National Assembly	Orchid, 2F
13:40 - 15:40	**[Plenary Session 2]** Maritime Confidence Building Measures	GRAND BALLROOM, 1F
	Moderator	**Tim Huxley** Executive Director, the International Institute for Strategic Studies - Asia, Singapore
	Presenters	**Hong Nong** Executive Director, Institute for China-America Studies, China **Renato Cruz De Castro** Professor, International Studies Department, De La Salle University, Philippines
	Appointed Discussants	**Kaneda Hideaki** Director, Okazaki Institute, Japan **Lee Seo-hang** President, Korea Institute for Maritime Strategy, Republic of Korea
	Special Discussants	**Ralf Brauksiepe** Parliamentary State Secretary, Ministry of National Defence, Germany **Jukka Matti Juusti** Permanent Secretary (Vice Minister), Finland

14:00 - 16:30	Cyber Working Group 2		President Hotel, 31F
16:00 - 18:00	**[Special Session 1]** The Fourth Industrial Revolution and Defense Science and Technology		Cosmos + Violet , 2F
	Moderator	**P. K. Singh** Director, United Service Institution, India	
	Presenters	**John Louth** Director, Defence, Industries and Society, Royal United Services Institute for Defence and Security Studies, UK **Maxim Shepovalenko** Deputy Director, Centre for Analysis of Strategies and Technologies, Russia	
	Appointed Discussants	**Reifqi Muna** Researcher, Center for Political Studies, Indonesian Institute of Sciences, Indonesia **Shim Hyun-chul** Professor, Department of Aerospace Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea	
	Special Discussant	**Suay Alpay** Vice Minister of Nationd Defense, Turkey	
	[Special Session 2] The Nature of Future Warfare and National Defense Policy		Orchid, 2F
	Moderator	**Jean-Pierre Maulny** Deputy Director, French Institute for International and Strategic Affairs, France	
	Presenters	**Margaret E. Kosal** Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, USA **Teng Jianqun** Director, Arms control and disarmament, China Institute of International Studies, China	
	Appointed Discussants	**Tran Viet Thai** Deputy Director-General, Institute for Foreign Strategic Studies, Diplomatic Academy of Vietnam, Vietnam **No Hoon** President, Korea Institute for Defense Analyses, Republic of Korea	
	Special Discussants	**Cardozo Luna** Undersecretary of Nationd Defense, Philippines **Jody Thomas** Senior Associate Deputy Minister, Canada	
18:30 - 19:00	Reception		Cosmos + Violet, 2F
19:00 - 20:40	Dinner hosted by the Minister of National Defense		GRAND BALLROOM, 1F

DAY 3 September 8th (Fri)

08:00 - 09:00	Registration		Lobby, 1F
08:30 - 10:00	**[Plenary Session 3]** Cyber Security Challenges and Defense Solutions		GRAND BALLROOM, 1F
	Moderator	**Lim Jong-in** Professor, Graduate School of Information Security, Korea University, Republic of Korea	
	Presenters	**Dean Cheng** Senior Research Fellow, Chinese Political and Military Affairs, Heritage Foundation, USA **Tsuchiya Motohiro** Professor, Graduate School of Media and Governance, Keio University, Japan	
	Appointed Discussants	**Patryk Pawlak** Brussels Executive Officer, EU Institute for Security Studies, Belgium **Fan Gaoyue** Senior Research Fellow, China Strategic Culture Promotion Association, China	
	Special Discussant	**Paulus Peter Jozef Bekkers** Director, Office of the Secretary General, OSCE	
10:20 - 11:50	**[Plenary Session 4]** New Forms of Terrorism and Global Coordination in Counter-terrorism		GRAND BALLROOM, 1F
	Moderator	**Abdulla Salem Alkaabii** Head, Publications Department, Emirates Center for Strategic Studies and Research, UAE	
	Presenters	**Nicolas Regaud** Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces, France **Mohd Kamarulnizam Abdullah** Professor, Department of International Affairs, School of International Studies-COLGIS, University Utara, Malaysia	
	Appointed Discussants	**Juraev Farrukh** Leading Researcher, Institute of Strategic and Interregional Researches under the President of the Republic of Uzbekistan **Jang Ji-hyang** Senior Research Fellow, ASAN Institute for Policy Studies, Republic of Korea	
	Special Discussants	**Anthony Lynch** Deputy Serretany of Defence, New Zealand **James H. Mackey** Head of Euro-Atlantic and Global Partnership Section - Integration, Partnership and Cooperation Directorate - Political Affairs and Security Policy Division, NATO	
12:00 - 13:00	Closing Ceremony		GRAND BALLROOM, 1F
13:00~14:30	Luncheon hosted by the Vice Minister of National Defense		Cosmos + Violet, 2F
14:30 - 19:00	Security-related on-site Tour		

프로그램

1일차 9월 6일 (수)

08:00 – 17:00	사이버 워킹그룹 1	2층, 오키드
	ISEC 국제안보회의 견학	코엑스 전시장
18:30 – 19:00	리셉션	2층, 코스모스+바이올렛
	차관주재 환영만찬	2층, 오키드

2일차 9월 7일 (목)

08:00 – 09:00	**등 록**	1층, 로비
09:00 – 09:40	**개회식**	1층, 그랜드볼룸
	개회사	**송영무** 국방부 장관
	축사	**이낙연** 국무총리
	기조연설	**마리스 패인** 호주 국방부 장관
10:00 – 12:00	**[본회의 1]** 북한 핵 · 미사일 위협과 한반도 안보	1층, 그랜드볼룸
	사회자	**다니엘 러셀** 미국 아시아사회정책연구소 선임연구원
	발제자	**임성남** 한국 외교부 제1차관
	토론자	**토마스 버거슨** 주한미군 부사령관 * **특별브리핑** **마커스 갈로스카스** 미국 국가정보국장실 북한정보담당관 **자 칭궈** 중국 북경대학교 국제관계학원 교수 **모리모토 사토시** 일본 타쿠쇼쿠대학교 총장 **알렉산더 니키틴** 러시아 국 제관계대학 유럽 – 아틀란틱 안보센터장 **서주석** 한국 국방부 차관
12:00 – 13:30	**국회 부의장 주재 오찬**	2층, 오키드
13:40 – 15:00	**[본회의 2]** 해양신뢰구축 방안 모색	1층, 그랜드볼룸
	사회자	**팀 헉슬리** 영국전략문제연구소 아시아 소장
	발제자	**홍 농** 중국 중미연구소장 **레나토 크루즈 데 카스트로** 필리핀 델 사 살레 대학교 국제학부 교수
	지정 토론자	**카네다 히데아키** 일본 오카자키연구소장 **이서항** 한국 해양전략연구소장
	특별 토론자	**랄프 브라욱지페** 독일 국방부 차관 **유카 매티 유스티** 핀란드 국방부 차관

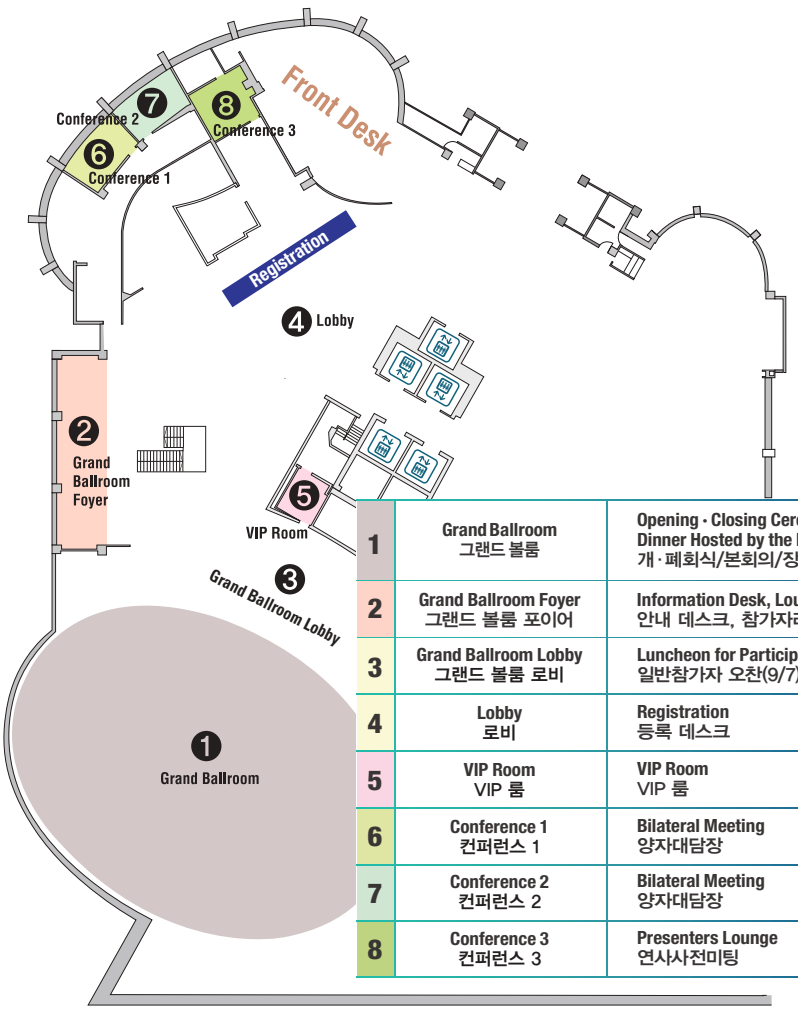
14:00 – 16:30	사이버 워킹그룹 2		31층, 프레지던트 호텔
	[특별세션 1] 4차 산업혁명과 국방과학기술		2층, 코스모스+바이올렛
	사회자	**피케이 싱** 인도 USI 소장	
	발제자	**존 루스** 영국 왕립합동국방안보연구소 국방산업사회연구소장 **막심 셰포바런코** 러시아 전략기술분석센터 부소장	
	지정 토론자	**레이프키 무나** 인도네시아과학원 정치학센터 연구원 **심현철** 한국 과학기술원 항공우주공학과 교수	
	특별 토론자	**수아이 알파이** 터키 국방부 차관	
16:00 – 18:00	**[특별세션 2]** 미래전 양상과 국방정책		2층, 오키드
	사회자	**장 피에르 마울니** 프랑스 국제전략연구소 부소장	
	발제자	**마가레트 코살** 미국 조지아공과대학교 샘 넌 국제대학원 교수 **텅 지옌췬** 중국 국제문제연구원 미국연구소장	
	지정 토론자	**트란 비엣 타이** 베트남 국립외교원 외교전략연구소 부소장 **노 훈** 한국 국방연구원장	
	특별 토론자	**카도조 루나** 필리핀 국방부 차관 **조디 토마스** 캐나다 국방부 차관 수석차관보	
18:30 – 19:00	리셉션		2층, 코스모스+바이올렛
19:00 – 20:40	장관주재 공식만찬		1층, 그랜드볼룸

3일차 9월 8일 (금)

08:00 – 08:30	등 록	1층, 로비
08:30 – 10:00	[본회의 3] 사이버 안보 도전과 해법	1층, 그랜드볼룸
	사회자	**임종인** 한국 고려대학교 정보보호대학원 교수
	발제자	**딘청** 미국 헤리티지재단 중국정치군사문제 선임연구원 **츠치야 모토히로** 일본 게이오대학교 미디어정책대학원 교수
	지정 토론자	**패트릭 퍼락** EU 안보연구소 행정관 **판 가오위에** 중국 전략문화촉진회 선임연구원
	특별 토론자	**폴 베커스** OSCE 사무국장
10:20 – 11:50	[본회의 4] 신종 테러리즘과 대테러 국제공조	1층, 그랜드볼룸
	사회자	**압둘라 살렘 알카비** UAE 전략문제연구소 공보부장
	발제자	**니콜라스 르고** 프랑스 국방부 국제관계전략본부장 인도–태평양 특별대표 **카마룰니잠 압둘라** 말레이시아 우타라 대학교 국제정세학과 교수
	지정 토론자	**주레브 파루크** 우즈베키스탄 대통령직속 지역전략연구소 선임연구원 **장지향** 한국 아산정책연구원 선임연구위원
	특별 토론자	**안토니 린치** 뉴질랜드 정책기획 차관보 **제임스 맥키** 나토 유럽–대서양 국제협력과장
12:00 – 13:00	폐회식	1층, 그랜드볼룸
13:00 – 14:30	차관주재 오찬	2층, 코스모스+바이올렛
14:30 – 19:00	안보현장 견학	

Floor Plan 행사장 안내

The Westin Chosun Seoul (1F)

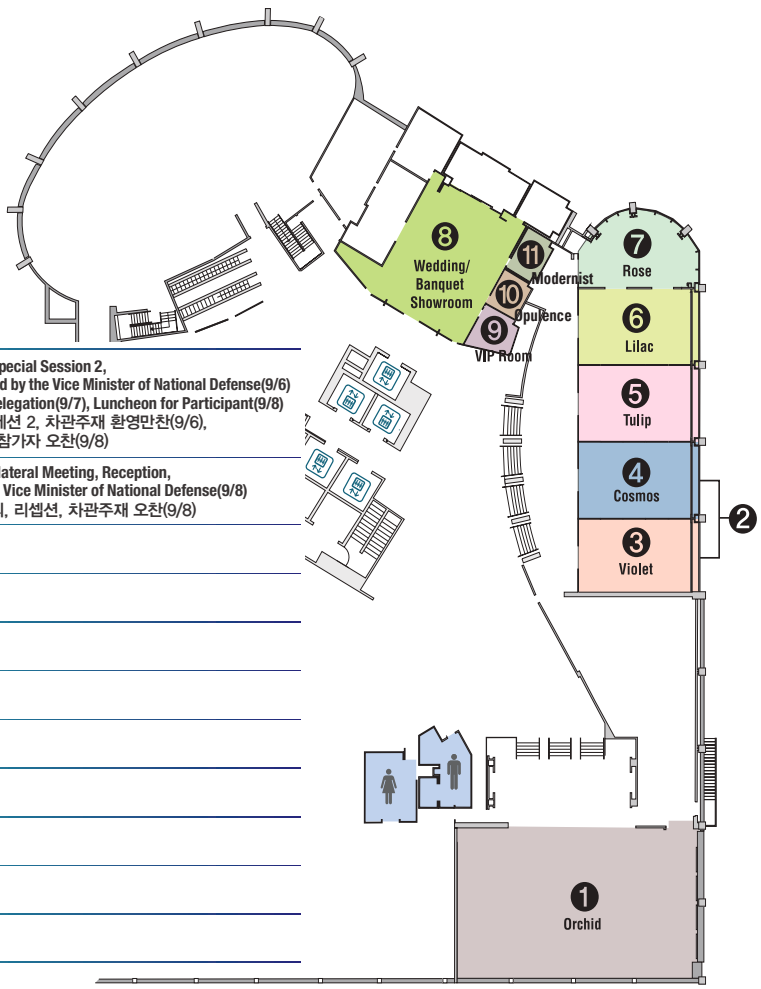


1F

1	Grand Ballroom 그랜드 볼룸	Opening · Closing Ceremony/Plenary Sessions/ Dinner Hosted by the Minister of National Defense(9/7) 개·폐회식/본회의/장관주재 환영만찬(9/7)
2	Grand Ballroom Foyer 그랜드 볼룸 포이어	Information Desk, Lounge 안내 데스크, 참가자라운지
3	Grand Ballroom Lobby 그랜드 볼룸 로비	Luncheon for Participant(9/7) 일반참가자 오찬(9/7)
4	Lobby 로비	Registration 등록 데스크
5	VIP Room VIP 룸	VIP Room VIP 룸
6	Conference 1 컨퍼런스 1	Bilateral Meeting 양자대담장
7	Conference 2 컨퍼런스 2	Bilateral Meeting 양자대담장
8	Conference 3 컨퍼런스 3	Presenters Lounge 연사사전미팅

The Westin Chosun Seoul (2F)

2F



1	Orchid 오키드룸	Cyber Working Group, Special Session 2, Welcoming Dinner Hosted by the Vice Minister of National Defense(9/6) Luncheon for Head of Delegation(9/7), Luncheon for Participant(9/8) 사이버워킹그룹, 특별 세션 2, 차관주재 환영만찬(9/6), 대표자 오찬(9/7), 일반참가자 오찬(9/8)
2	Cosmos+Violet 코스모스+바이올렛	Special Session 1, Multilateral Meeting, Reception, Luncheon Hosted by the Vice Minister of National Defense(9/8) 특별 세션 1, 소다자회의, 리셉션, 차관주재 오찬(9/8)
3	Violet 바이올렛	Bilateral Meeting 양자대담장
4	Cosmos 코스모스	Bilateral Meeting 양자대담장
5	Tulip 튤립	Bilateral Meeting 양자대담장
6	Lilac 라일락	SDD 2017 Secretariat SDD 2017 사무국
7	Rose 로즈	Security Room 경호상황실
8	Wedding/Banquet Showroom 연회예약실	Press Room 프레스 룸
9	VIP Room VIP 룸	Interview Room 인터뷰 룸
10	Opulence 오퓰런스	Medical Office 의무실
11	Modernist 모더니스트	Prayer Room 기도실

General Information 행사 정보

Information Desk

Location Lobby, 1F
Operating Hours September 6~8 08:00-18:00

장소 1층, 로비
운영시간 9월 6일~8일 08:00–18:00

ID Card

Participants are required to wear their ID cards at all time during the SDD 2017. If you lose your badge, you can have it re-issued at the Registration Desk.

행사장에서는 ID카드를 본인이 소지해주십시오. ID카드 분실 시 등록데스크에서 재발급을 요청해주시기 바랍니다.

Seating Arrangement System

If you scan the ID card on the RFID card reader, you can check your designated seat on the front screen.

RFID 카드 리더기에 ID카드를 스캔 하시면 앞쪽 스크린에서 지정 좌석을 확인 하실 수 있습니다.

Dress Code

The dress code is business formal. Active service member of military are kindly requested to wear military dress uniform. (Class-A Uniform)

군 관계자 분들께서는 군복을 착용해주시고, 그 외 참가자는 정장을 착용해주시기 바랍니다.

Bilateral Meetings

The single meeting is limited to 20 minutes. The meeting rooms are available only for bilateral meetings that are pre-approved.

대담별 제한시간은 20분입니다. 양자대담장은 사전 요청 및 승인된 국가만 사용할 수 있습니다.

Prior Meeting for Session Panels

Panels for each session are asked to gather at the Conference 3 (1F) 30 minutes before the session begins. After delivering announcements for the session, all the panels will leave the Conference 3(1F) together.

각 세션 연사 분들께서는 해당 세션 시작 30분 전까지 컨퍼런스 3(1F)으로 모여주십시오..각 세션 운영 및 전달 사항 안내 후 회의장으로 이동해주시기 바랍니다.

Simultaneous interpretation

- Simultaneous Interpretation provided for Korean, Chinese, Japanes, Russian, Spanish.
  - Opeing · Closing Ceremony, Pleanry Sessions
- Simultaneous Interpretation provided for Korean.
  - Special Sessions, Welcoming Dinner
- 한국어, 중국어, 일본어, 러시아어, 스페인어 동시통역 제공
  - 개회식, 폐회식, 본회의
- 한국어 동시통역 제공
  - 특별 세션, 환영만찬

Press Center

SDD 2017 press center provides resources to assist in reporting as well as press releases, Daily Bulletin, photos, LAN cables and etc.
There is the press information desk in the Press Center and the staff will help with any requests or inquire.

Location Wedding/Banquet Showroom, 2F
Operating Hours September 6 (Wed) 09:00-17:00
September 7 (Thu) 08:00-18:00
September 8 (Fri) 08:00-13:00

취재 지원을 위하여 기자실에는 Daily Bulletin, 사진자료, 인터넷 등을 제공합니다. 그 외 필요한 사항에 대하여는 현장 진행요원을 통해 요청해주시기 바랍니다.

장소 2층, 연회예약실
운영시간 9월 6일(수) 09:00–18:00
9월 7일(목) 08:00–18:00
9월 8일(금) 08:00–13:00

Prayer Room

Location Modernist, 2F
Operating Hours September 6(Wed) 08:00-18:00
September 7(Thu) 08:00-18:00
September 8(Fri) 08:00-15:00

There will be sets of compass and mat prepared for the participants who need to use the prayer room.

장소 2층, 모더니스트
운영시간 9월 6일(수) 08:00–18:00
9월 7일(목) 08:00–18:00
9월 8일(금) 08:00–15:00

기도실에는 기도실을 사용하시는 참가자를 위하여 나침반, 매트 세트가 준비되어 있습니다.

F&B

- **Luncheon for Participants**
  September 7(Thu) 12:00-13:30 / Grand Ballroom Foyer
  September 8(Fri) 13:00-14:30 / Orchid
- **Luncheon for Head of Delegation**
  September 7(Thu) 12:00-13:30 / Orchid
  September 8(Fri) 13:00-14:30 / Cosmos+Violet
- **Welcoming Dinner hosted by the Vice Minister of National Defense**
  September 6(Wed) 19:00-20:40 / Orchid
- **Dinner hosted by the Minister of National Defense**
  September 7(Thu) 19:00-20:40 / Grand Ballroom
- **일반참가자 오찬**
  9월 7일(목) 12:00–13:30 / 그랜드 볼룸 로비
  9월 8일(금) 13:00–14:30 / 오키드룸
- **대표자 오찬**
  9월 7일(목) 12:00–13:30 / 오키드룸
  9월 8일(금) 13:00–14:30 / 코스모스+바이올렛
- **차관주재 만찬**
  9월 6일(수) 19:00–20:40 / 오키드룸
- **장관주재 만찬**
  9월 7일(목) 19:00–20:40 / 그랜드 볼룸

Tour Plan 안보견학

Course 01

JSA (Joint Security Area)

September 8 (Fri), 14:30-19:00

The Westin Chosun Seoul

JSA

The Westin Chosun Seoul

- Panmunjom has been installed by the Korean War Armistice Agrement in July 27th, 1953. North of the military demarcation line is managed by the North Korean side, the south side is managed by the UN and this is where military armistice commission meetings are held for the implementation of the armistice agreement.
- May 10, 1953 both of Military Armistice Commission set up a Joint Security Area on the military demarcation line at Panmunjom.

Course 02

The War Memorial of Korea

September 8 (Fri), 14:30-18:00

The Westin Chosun Seoul

The War Memorial of Korea

The Westin Chosun Seoul

The war memorial of Korea was built to commemorate victims in the wars, which led to modern nation state, located in Yongsan-gu, Seoul. It has six indoor exhibition rooms and outdoor exhibition center displaying military equipment.

Moreover, there will be special army performance for SDD 2017; ceremonial guard performance, korean traditional guard performance and military band performance.

코스 01

JSA (공동경비구역)

9월 8일 (금) 14:30–19:00

서울 웨스틴 조선호텔

JSA

서울 웨스틴 조선호텔

- 판문점은 1953년 7월 27일 6·25 전쟁 정전협정 체결 이후 군사분계선의 이북은 북한측이 이남은 UN측이 각각 관할하고 있는 특수지역이다. 또한, 이곳에서는 정전협정 이행을 위한 군사정전위원회 회의가 개최된다.
- 정전협정 조인은 현재의 판문점에서 개성 쪽으로 1km 떨어진 지점에서 이루어졌으나, 1953년 10월 군사정전위원회 쌍방이 군사분계선상에 공동경비구역을 설정하면서 오늘의 판문점이 생겨났다.

코스 02

전쟁기념관

9월 8일 (금) 14:30–18:00

서울 웨스틴 조선호텔

전쟁기념관

서울 웨스틴 조선호텔

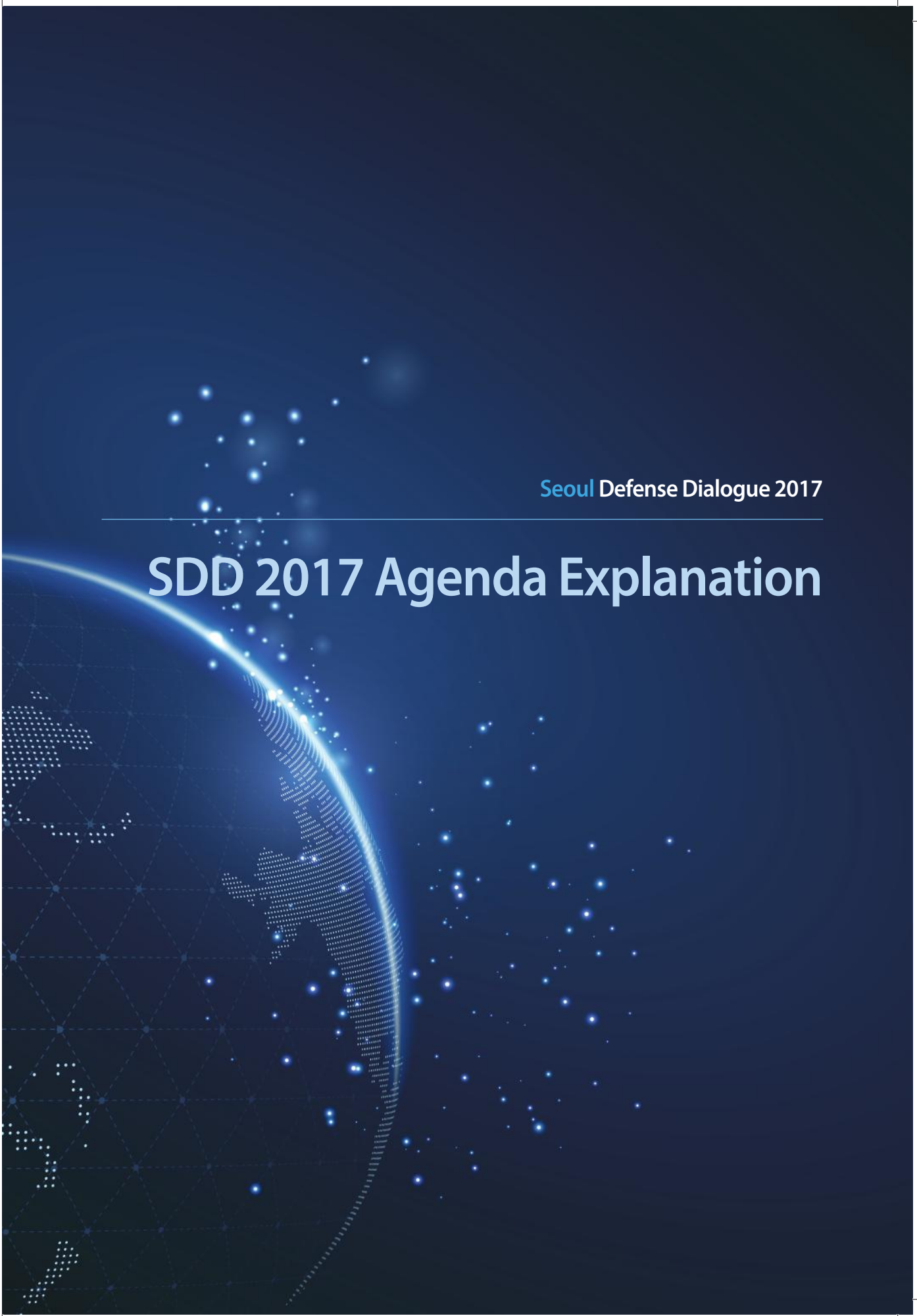
서울 용산구에 위치한 전쟁기념관은 오늘날의 근대 한국을 있게 한 전쟁 희생자들을 기리기 위해 설립되었다. 전시장에는 6개 전시실과 군사 장비를 전시하는 야외 전시실이 갖춰져 있다.

아울러, 2017 SDD를 위한 의식 경호 공연, 한국의 전통 경호 공연, 군악대 공연과 같은 특별 공연이 있을 예정이다.


Cooperation for Security & Peace
2017
SDD
Seoul
Defense
Dialogue

Seoul Defense Dialogue 2017

SDD 2017 Agenda Explanation



Plenary Session 본회의

Plenary Session 01

"North Korea's Nuclear and Missile Threats and Security of the Korean Peninsula"
북한 핵 · 미사일 위협과 한반도 안보

There is a strong need for a more effective and practical cooperation on North Korean denuclearization at both international and regional levels as North Korea continues to develop nuclear and missiles despite international sanctions. However, finding cooperation and solutions for North Korean denuclearization is becoming more difficult as security relations become unstable due to changes in the international environment such as the rise of China and the Trump administration's emphasis on an 'America First' policy. Such changes should to be taken into account in order to create effective and practical international cooperative measures to solve the North Korean problem.

세계적인 제재에도 불구하고 북한의 핵미사일 개발이 지속되고 있는 현실 속에서 북한의 비핵화를 위한 국제사회 및 지역 차원의 보다 효과적이고 실행력 있는 협력 증진이 요구된다. 그러나 미국의 자국 우선주의, 중국의 부상 등 국제환경의 변화로 인해 한반도 안보에 대한 기존의 역학관계가 불안정함에 따라 북한의 핵미사일 문제 해결을 위한 협력과 해법이 더욱 어려워지고 있다. 그러므로 변화된 상황에 맞춰 북한의 핵미사일 문제해결을 위한 효과적이고 실행력 있는 국제공조 방안을 마련할 필요가 있다.

Moderator 사회자

Daniel R. Russel 대니얼 러셀

Diplomat in Residence and Senior Fellow, Asia Society Policy Institute, USA
미국 아시아사회정책연구소 선임연구위원

Presenter 발제자

Lim Sung-nam 임성남

1st Vice Minister of Foreign Affairs, Republic of Korea
한국 외교부 제1차관

Discussant 토론자

Thomas W. Bergeson 토마스 버거슨

Deputy Commander, USFK
주한미군 부사령관

Special Briefer 특별 브리퍼

Markus Garlauskas 마커스 갈로스카스

National Intelligence Officer for North Korea, Office of the Director of National Intelligence, DIA, USA
미국 국가정보국장실 북한정보담당관

Discussant 토론자

Jia Qingguo 자 칭궈

Professor, School of International Studies of Peking University, China
중국 북경대학교 국제관계학원 교수

Discussant 토론자

Morimoto Satoshi 모리모토 사토시

Chancellor, Takushoku University, Japan
일본 타쿠쇼쿠대학교 총장

Discussant 토론자

Alexander I. Nikitin 알렉산더 니키틴

Director, Center for Euro-Atlantic Security, MGIMO, Russia
러시아 국제관계대학 유럽 – 아틀란틱 안보센터장

Discussant 토론자

SHU Choo-suk 서주석

Vice Minister of National Defense, Republic of Korea
한국 국방부 차관

Plenary Session 02

"Maritime Confidence Building Measures"
해양신뢰구축 방안 모색

Activities on the seas are becoming increasingly restricted with the emergence of transnational and unconventional threats as well as coastal states' economic and security matters. Such restrictions on maritime activities greatly impact domestic affairs including areas of national security and the economy which create legal issues and heighten military tensions. Related states are developing and increasing their semi-military naval, marine and coast guard forces in order to protect and promote marine rights and interests. Due to intensified economic interdependence among states and the immense costs of military conflicts, the role of maritime confidence-building measures is being emphasized more than ever.

해양에서의 자유로운 활동이 연안국의 경제 및 안보적 이유와 초국가적 · 비전통적 위협의 등장으로 제한을 받고 있는 실정이다. 이러한 해양활동의 제약은 국내 안보 · 경제 등 전반적인 분야에 커다란 파급효과를 미치기 때문에, 이에 대한 국가 간 법적 및 군사적 갈등이 점점 고조되고 있다. 관련 국가들은 자국의 해양이익과 권리를 보호 · 증진시키기 위해 해군력, 해경, 그리고 해상민병과 같은 준군사력을 발전 및 증강시키고 있는 실정이다.하지만 경제적 측면에서의 국가 간 상호 의존성의 심화와 안보적 측면에서의 상호 충돌로 인한 극심한 피해 등을 고려할 때 국가 간 해양신뢰구축이 절대적으로 필요하다는 인식이 대두되고 있다.

Moderator 사회자

Tim Huxley 팀 헉슬리

Executive Director, the International Institute for Strategic Studies - Asia, Singapore
영국전략문제연구소 아시아 소장

Appointed Discussant 지정 토론자

Lee Seo-hang 이서항

President, Korea Institute for Maritime Strategy, Republic of Korea
한국 해양전략연구소장

Presenter 발제자

Hong Nong 홍 농

Executive Director, Institute for China-America Studies, China
중국 중미연구소장

Special Discussant 특별 토론자

Ralf Brauksiepe 랄프 브라욱지페

Parliamentary State Secretary, Ministry of National Defence, Germany
독일 국방부 차관

Presenter 발제자

Renato Cruz De Castro 레나토 크루즈 데 카스트로

Professor, International Studies Department, De La Salle University, Philippines
필리핀 델 라 살레 대학교 국제학부 교수

Special Discussant 특별 토론자

Jukka Matti Juusti 유카 매티 유스티

Permanent Secretary (Vice Minister), Finland
핀란드 국방부 차관

Appointed Discussant 지정 토론자

Kaneda Hideaki 카네다 히데아키

Director, Okazaki Institute, Japan
일본 오카자키연구소장

Plenary Session 03

"Cyber Security Challenges and Defense Solutions"
사이버 안보 도전과 해법

With the development of information and communications technologies (ICTs), cyber space is a crucial space for prosperity across the world. At the same time, it is a threat factor to national security as cyber attacks on critical national infrastructure and industrial facilities are enabled. Cyber space is mankind's common property without borders. Although they have common understandings of the regulation enactment to prevent the breakdown of order brought about by cyber attacks, states cannot draw conclusions due to hegemonic rivalry. Although states respond to cyber threats by respectively creating their own cyber units, to ensure security and peace in cyber space, it is necessary to create a new cyber security order through international cooperation as well as the endeavors of individual states.

정보통신기술(ICT)의 발전에 따라 사이버 공간은 경제적 번영을 위한 핵심 공간이지만, 주요 국가 기반시설 및 산업시설 등에 대한 사이버공격이 가능하기 때문에 국가 안보의 위협 요인이 되고 있다. 사이버 공간은 국경선이 없는 인류의 공동 재산으로, 각국은 개인이나 국가에 의한 사이버 공격 등 질서 파괴를 방지하기 위한 규정 제정에는 공감하고 있지만, 주도권 경쟁으로 인해 결론이 쉽게 도출되지 않고 있다. 각국은 사이버 부대를 창설하는 등 사이버 위협에 대응하고 있지만, 사이버 공간의 안정과 평화를 위해 개별 국가의 노력뿐만 아니라 전 세계적 협력을 통한 새로운 사이버 안보질서 창출이 필요하다.

Moderator 사회자

Lim Jong-in 임종인

Professor, Graduate School of Information Security, Korea University, Republic of Korea
한국 고려대학교 정보보호대학원 교수

Presenter 발제자

Dean Cheng 딘 청

Senior Research Fellow, Chinese Political and Military Affairs, Heritage Foundation, USA
미국 헤리티지재단 중국정치군사문제 선임연구원

Presenter 발제자

Tsuchiya Motohiro 츠치야 모토히로

Professor, Graduate School of Media and Governance, Keio University, Japan
일본 게이오대학교 미디어정책대학원 교수

Appointed Discussant 지정 토론자

Patryk Pawlak 패트릭 퍼락

Brussels Executive Officer, EU Institute for Security Studies, Belgium
EU 안보연구소 행정관

Appointed Discussant 지정 토론자

Fan Gaoyue 판 가오위에

Senior Research Fellow, China Strategic Culture Promotion Association, China
중국 전략문화촉진회 선임연구원

Special Discussant 특별 토론자

Paulus Bekkers 폴 베커스

Director, Office of the Secretary General, OSCE
OSCE 사무국장

Plenary Session 04

"New Forms of Terrorism and Global Coordination in Counter-terrorism"
신종 테러리즘과 대테러 국제공조

With the constant increase of international terrorist organizations and spontaneous terror threats, the diversification of terror is also posing severe threats to regional and international security. It is necessary to discuss measures to extend the consensus against terrorism and enhance practical defense cooperation with the rise of new forms of terrorism. To ensure the joint response against violent extremism and new forms of terrorism, it is essential to establish a specific action plan.

국제 테러 세력의 증가 및 자생적 테러위협의 지속과 함께 최근에는 테러의 양태가 다양화되어 세계 및 지역 안보의 주요 위협으로 대두되고 있다. 신종 테러리즘 위험의 확산 속에서 각국의 대테러 공감대를 확대하고 실질적인 국방협력 증진을 위한 논의가 필요하다. 폭력적 극단주의와 신종 테러리즘에 대한 국제사회의 공동 대응을 실질화하기 위해 구체적인 행동계획을 마련하는 논의가 필요한 시점이다.

Moderator 사회자

Abdulla Salem Alkaabi 압둘라 살렘 알카비

Head, Publications Department, Emirates Center for Strategic Studies and Research, UAE
UAE 전략문제연구소 공보부장

Presenter 발제자

Nicolas Regaud 니콜라스 르고

Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces, France
프랑스 국방부 국제관계전략본부장 인도-태평양 특별대표

Presenter 발제자

Kamarulnizam Abdullah 카마룰니잠 압둘라

Professor, Department of International Affairs, School of International Studies-COLGIS, University Utara, Malaysia
말레이시아 우타라 대학교 국제정세학과 교수

Appointed Discussant 지정 토론자

Juraev Farrukh 주레브 파루크

Leading Researcher, Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan
우즈베키스탄 대통령직속 지역전략연구소 선임연구원

Appointed Discussant 지정 토론자

Jang Ji-hyang 장지향

Senior Research Fellow, ASAN Institute for Policy Studies, Republic of Korea
한국 아산정책연구원 선임연구원

Special Discussant 특별 토론자

Anthony Lynch 안토니 린치

Deputy Serretany of Defence, New zeal and
뉴질랜드 정책기획 차관보

Special Discussant 특별 토론자

James H. Mackey 제임스 맥키

Head of Euro-Atlantic and Global Partnership Section, NATO
나토 유럽-대서양 및 국제협력과장

Special Session 특별세션

Special Session 01

"The Fourth Industrial Revolution and Defense Science and Technology"
4차 산업혁명과 국방과학기술

Recently the Fourth Industrial Revolution has been actively discussed, including constructs of inter-communication systems between production equipment and products by AI (Artificial Intelligence), IoTs (Internet of things) and robots and seeks the optimization of the whole production process. Efforts for more efficient national defense management and maximized combat power by utilizing new technologies such as AI and robots are being achieved in the national defense area. It is necessary to discuss the effects that the civil technologies developed by the Fourth Industrial Revolution have on defense science and technology and the cooperation between civilians and the military.

오늘날 인공지능, 사물 인터넷, 로봇 등을 통해 생산기기와 생산품 간 상호 소통체계를 구축하고, 전체 생산과정의 최적화를 모색하는 4차 산업혁명에 대한 논의가 활발하다. 국방 분야에서도 인공지능, 로봇 등 새로운 기술을 이용하여 국방경영을 효율화하고 전투력을 극대화하기 위한 노력이 이루어지고 있다. 4차 산업혁명을 통해 발전된 민간기술이 국방과학기술에 미치는 영향과 민군 간 협력에 대한 논의가 필요하다.

Moderator 사회자

P. K. Singh 피케이 싱

Director, United Service Institution, India
인도 USI 소장

Presenter 발제자

John Louth 존 루스

Director, Defence, Industries and Society, Royal United Services Institute for Defence and Security Studies, UK
영국 왕립합동국방안보연구소 국방산업사회연구소장

Presenter 발제자

Maxim Shepovalenko 막심 셰포바런코

Deputy Director, Centre for Analysis of Strategies and Technologies, Russia
러시아 전략기술분석센터 부소장

Appointed Discussant 지정 토론자

Reifqi Muna 레이프키 무나

Researcher, Centre for Political Studies, Indonesian Institute of Sciences, Indonesia
인도네시아 과학원 정치학센터 연구원

Appointed Discussant 지정 토론자

Shim Hyun-chul 심현철

Professor, Department of Aerospace Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea
한국 과학기술원 항공우주공학과 교수

Special Discussant 특별 토론자

Suay Alpay 수아이 알파이

Vice Minister of Nationd Defense, Turkey
터키 국방부 차관

Special Session 02

"The Nature of Future Warfare and National Defense Policy"
미래전 양상과 국방정책

With the development of precision-guided munitions, drones and artificial satellites, wars have changed to a form of destroying specific targets instead of mass destruction. Moreover, it is expected that the appearance of the Fourth Industrial Revolution will accelerate such changes. As the result of the Fourth Industrial Revolution is unpredictable, it is hard to predict forms of future warfare. Thus, it is necessary to predict aspects of future warfare in various angles and to discuss directions of national defense policies.

오늘날 정밀유도무기, 무인기, 인공위성 등의 발달로 전쟁은 과거와 같은 대량 파괴보다는 정해진 목표물만 정밀 파괴하는 방식으로 변화하고 있다. 거기에 더해 4차 산업혁명의 등장은 이러한 변화를 더욱 가속화시킬 것으로 예상된다. 그러나 4차 산업혁명의 결과를 예측하기 힘든 것처럼 새로운 전쟁의 양상이 어떤 식으로 귀결될 것인지 예측하기는 매우 어렵다. 그러므로 미래전의 양상을 다각도로 예측하고, 이에 수반되는 국방정책의 방향을 모색하는 논의가 필요하다.

Moderator 사회자

Jean-Pierre Maulny 장 피에르 마울니

Deputy Director, French Institute for International and Strategic Affairs, France
프랑스 국제전략연구소 부소장

Presenter 발제자

Magaret E. Kosal 마가레트 코살

Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, USA
미국 조지아공과대학 샘 넌 국제대학원 교수

Presenter 발제자

Teng Jianqun 텅 지옌췬

Director, Department for American Studies, China Institute of International Studies, China
중국 국제문제연구원 미국연구소장

Appointed Discussant 지정 토론자

Tran Viet Thai 트란 비엣 타이

Deputy Director-General, Institute for Foreign Strategic Studies, Diplomatic Academy of Vietnam, Vietnam
베트남 국립외교원 외교전략연구소 부소장

Appointed Discussant 지정 토론자

No Hoon 노 훈

President, Korea Institute for Defense Analyses, Republic of Korea
한국 국방연구원장

Special Discussant 특별 토론자

Cardozo Luna 카도조 루나

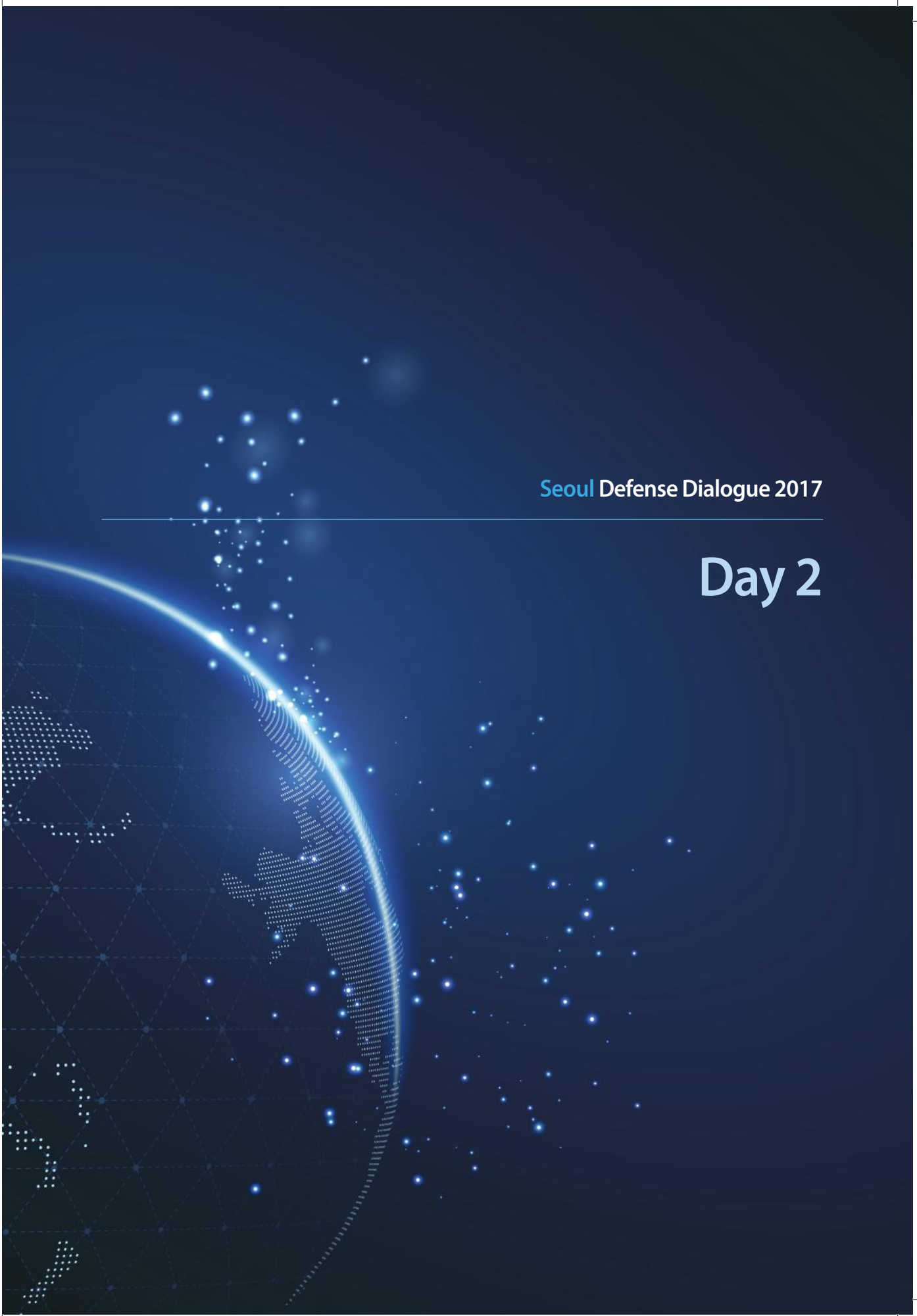
Undersecretary of Nationd Defense, Philippines
필리핀 국방부 차관

Special Discussant 특별 토론자

Jody Thomas 조디 토마스

Senior Associate Deputy Minister, Canada
캐나다 국방차관 수석차관보


Cooperation for Security & Peace
2017
SDD
Seoul
Defense
Dialogue



Seoul Defense Dialogue 2017

Day 2

Opening Ceremony 개회식

09:00-09:40 Grand Ballroom, 1F

Opening Remarks	**Song Young-moo** Minister of National Defense, Republic of Korea
Congratulatory Remarks	**Lee Nak-yeon** Prime Minister, Republic of Korea
Keynote Speech	**Marise Payne** Minister for Defence, Australia

개회사	**송영무** 국방부 장관
축 사	**이낙연** 국무총리
기조연설	**마리스 패인** 호주 국방부 장관

Song Young-moo 송영무

Minister of National Defense, Republic of Korea
대한민국 국방부 장관

Lee Nak-yeon 이낙연

Prime Minister, Republic of Korea
대한민국 국무총리

Marise Payne 마리스 패인

Minister for Defence, Australia
호주 국방부 장관

Plenary Session 1 본회의 1

10:00-12:00 Grand Ballroom, 1F

"North Korea's Nuclear and Missile Threats and Security of the Korean Peninsula"
북한 핵 · 미사일 위협과 한반도 안보

Key Issues

- North Korea's nuclear missile capabilities
- The limits of sanctions against North Korea and effective solutions
- Security dynamics on the Korean peninsula
- International cooperative measures for North Korean denuclearization
- 북한의 핵 및 미사일 능력
- 북한의 핵과 미사일 개발에 대한 제재의 한계와 효과적인 대응 방안
- 한반도를 둘러싼 안보역학 관계
- 북한의 비핵화를 위한 국제적인 안보협력 추진 방안

Moderator	**Daniel R. Russel** Diplomat in Residence and Senior Fellow, Asia Society Policy Institute, USA
Presenter	**Lim Sung-nam** 1st Vice Minister of Foreign Affairs, Republic of Korea
Discussants	**Thomas W. Bergeson** Deputy Commander, USFK * **Special Briefing** **Markus Garlauskas** National Intelligence Officer for North Korea, DIA, USA **Jia Qingguo** Professor, School of International Studies of Peking University, China **Morimoto Satoshi** Chancellor, Takushoku University, Japan **Alexander I. Nikitin** Director, Center for Euro-Atlantic Security, MGIMO, Russia **SUH Choo-suk** Vice Miniter of National Defense, Republic of Korea

사회자	**다니엘 러셀** 미국 아시아사회정책연구소 선임연구원
발제자	**임성남** 한국 외교부 제1차관
토론자	**토마스 버거슨** 주한미군 부사령관 * **특별브리핑** **마커스 갈로스카스** 미국 국가정보국장실 북한정보담당관 **자 칭궈** 중국 북경대학교 국제관계학원 교수 **모리모토 사토시** 일본 타쿠쇼쿠대학교 총장 **알렉산더 니키틴** 러시아 국제관계대학 유럽 – 아틀란틱 안보센터장 **서주석** 한국 국방부 차관

Presentation Summary 발제 요약문

This data will be provided separately.

이 자료는 별도로 제공할 것입니다.

Plenary Session 2 본회의 2

13:40-15:40 Grand Ballroom, 1F

"Maritime Confidence Building Measures"
해양신뢰구축 방안 모색

Key Issues

- Conflicts among states' national interests in the maritime environment
- The current status of each country's maritime military force
- International legal position of coastal states and user states in regards to maritime issues in the region
- Factors that deter and promote confidence building among states in the maritime environment
- 해양에서의 국가 간 국익 갈등 요인
- 각국의 해양 군사력 증강 실태
- 역내 해양이슈에 대한 연안국과 사용국의 국제법적 입장
- 해양에서의 국가 간 신뢰구축의 방해 및 촉진 요인

Moderator	**Tim Huxley** Executive Director, the International Institute for Strategic Studies - Asia, Singapore
Presenters	**Hong Nong** Executive Director, Institute for China-America Studies, China **Renato Cruz De Castro** Professor, International Studies Department, De La Salle University, Philippines
Appointed Discussants	**Kaneda Hideaki** Director, Okazaki Institute, Japan **Lee Seo-hang** President, Korea Institute for Maritime Strategy, Republic of Korea
Special Discussants	**Ralf Brauksiepe** Parliamentary State Secretary, Ministry of National Defence, Germany **Jukka Matti Juusti** Permanent Secretary (Vice Minister), Finland

사회자	**팀 헉슬리** 영국전략문제연구소 아시아 소장
발제자	**홍 농** 중국 중미연구소장 **레나토 크루즈 데 카스트로** 필리핀 델 라 살레 대학 국제학부 교수
지정 토론자	**카네다 히데아키** 일본 오카자키연구소장 **이서항** 한국 해양전략연구소장
특별 토론자	**랄프 브라욱지페** 독일 국방부 차관 **유카 매티 유스티** 핀란드 국방부 차관

Presentation Summary

Nong Hong
Executive Director, Institute for China-America Studies, China

Maritime Confidence Building Measures in the South China Sea

Status Quo in the South China Sea

Four phrases could be used to describe the current situation in the South China Sea, "cooling, mitigation, regression and cooperation". The positive factors of the situation include obtaining a concrete achievement in COC consultation between China and ASEAN countries, the conduct of a relatively successful China-U.S. Diplomatic and Security Dialogue, the reaching of a series of consensuses on conflict prevention and dispute management measures, and the establishment of a bilateral intergovernmental consultation mechanism for settlement of the South China Sea issue between China and the Philippines.

There are also some factors which might lead to uncertainty in the future South China Sea development, e.g., US's FONOP; the scope of activities for the U.S.-Japan military alliance, some country's recent move in oil and gas activities, which will surely have a negative impact on the South China Sea dispute management and the COC consultation process.

Need for MCBM

The hard-earned peace and stability of the South China Sea should not be taken for granted. Regional countries should endeavor to jointly maintain the positive trend in the South China Sea, while extra-regional powers, while pursuing their legitimate interests, should do their share in not disrupting the virtuous dynamism among littoral countries of the South China Sea. To this end, this presentation would propose a mechanism of maritime confidence building measures from four perspectives, political, legal, security, and regional cooperation.

Components of MCBM

Confidence building measures and preventive diplomacy are widely discussed in security discourse. CBMs can be military measures or broader initiatives encompassing almost anything that builds confidence and promotes dialogue between countries.

Political and military

China and the US should establish an effective and integrated mechanism to manage potential crisis in the South China sea. China and ASEAN should work together to speed up the COC consultation, and put into place the China-ASEAN track of the "dual-track approach", that is to properly address the South China Sea disputes through negotiations and consultations among countries directly concerned, and to jointly safeguard peace and stability in the South China Sea. The disputant countries should exercise self-restraint, and avoid unilateral exploration and exploitation of natural resources in disputed areas.

Legal

UNCLOS is a significant MCBM. Effective maritime regimes require adherence to the legal principles of UNCLOS, as well as to other relevant international maritime treaties and customary international law. However, there are still many 'grey areas' with the law of the sea. This is particularly so with provisions relating to the exclusive economic zone (EEZ) regime. The EEZ regime reflects a careful balance between the rights and duties of coastal states and those of user states. Some dialogue towards common understandings of aspects of the law of the sea where uncertainty exists could be a worthwhile MCBM.

UNCLOS is an international regime, but there are other maritime regimes for shipping, fishing, seabed mining, marine environmental protection, search and rescue, and so on. Contemporary users of the seas face a variety of complex rules, norms, principles and decision-making procedures, which when put together in an issue area form an international regime.

This South China Sea Arbitration case is so far the first attempt by a claimant state in the South China Sea to resort the dispute to a third party forum under UNCLOS. However, despite the value ascribed to the compulsory dispute settlement under UNCLOS, this case does not make a desired contribution to resolving the real dispute between the two. This raises a question on the international legal culture. As a legal confidence building measure, all countries' political will on choosing a suitable approach to address maritime issues in political and regional context should be respected.

Navigation

This presentation considers the development and efficacy of maritime confidence-building measures to ensure safe and secure navigation in the region, and to reduce tension and prevent conflict. UNCLOS and the 1972 International Regulations for Preventing Collisions at Sea (COLREG) are multilateral agreements that set forth legally binding obligations of all states. The 2014 Code for Unplanned Encounters at Sea (CUES), non-binding, provides greater fidelity for duties of safe interaction at sea. China and the United States signed in 2014 and 2015 a legally nonbinding Memorandum of Understanding (MOU) on the Rules of Behavior for Safety of Air and Maritime Encounters. Though many problems and unsolved issues exist, the MOU still contributes much to the confidence building between the two navies.

Regional cooperation

With the goal of achieving peace and stability in the region of the South China Sea, this presentation proposes a pragmatic dispute management regime for the SCS dispute from four dimensions, which takes into account the role of environmental security and fishery security, as well as ocean governance: environmental security as a driving force of cooperation in the South China Sea; fisheries cooperation as a start of the south china sea disputes resolution; UNCLOS as a framework for ocean governance in the region; transformation of ways of thinking as a foundation to lead policy and research direction.

발제 요약문

남중국해에서의 해양신뢰구축 방안

홍 농 중국 중미연구소장

남중국해 현황

남중국해의 현황은 네 개의 용어, 즉 "냉각(cooling), 완화(mitigation), 회귀(regression), 협력(cooperation)"으로 설명할 수 있다. 중국과 아세안 국가들 간의 행동강령(COC) 협의에서 나타난 구체적 성취, 성공적이었던 미중 외교안보대화, 일련의 분쟁예방과 분쟁관리방안에 대한 공감대 형성, 그리고 중국과 필리핀 간의 남중국해 문제 해결을 위한 양 정부 간의 협의 메커니즘 구축이 현 상황의 긍정적 요소들이다.

그러나 미래 남중국해 개발의 불확실성을 야기할 수 있는 요소들도 있다. 예를 들어, 미국 항행의 자유(FONOP), 미일 군사동맹 행동의 범위, 석유 및 가스 활동에서 나타난 몇몇 국가들의 최근 움직임은 남중국해 분쟁관리와 행동강령 협의 과정에 부정적 영향을 미칠 것이다.

해양신뢰구축 방안의 필요성

힘들게 얻은 남중국해의 평화와 안정을 당연하게 여겨서는 안 된다. 지역국가들은 남중국해에서의 긍정적 추세를 유지하도록 함께 노력해야 하고, 그들의 합법적 이익을 추구하는 과정에서 남중국해 연안국가들의 긍정적 역동성을 방해하지 않도록 각자의 역할을 감당해야 한다. 이를 위해서 본 발제에서 정치, 법제, 안보 그리고 지역협력이라는 4가지 관점에서 해양신뢰 방안 메커니즘을 제안하고자 한다.

해양신뢰구축 방안의 구성요소

신뢰구축 방안과 예방 외교(preventive diplomacy)는 안보 담론에서 폭넓게 논의되고 있다. 신뢰구축 방안은 국가 사이에서 대화를 촉진하고 신뢰를 구축하는 거의 모든 것을 망라하는 군사 조치 또는 더 넓은 개념의 계획이라고 할 수 있다.

정치/군사

남중국해의 잠재적 위기를 관리하기 위해서 중국과 미국은 효과적이고 통합적인 메커니즘을 구축해야 한다. 중국과 아세안은 행동강령 협의를 빠르게 진행하고, "투 트랙 접근"을 위한 중국과 아세안 트랙을 시행해야 한다. 즉, 당사국 간의 협상과 협의를 통해서 남중국해 분쟁을 적절하게 처리하고, 남중국해의 평화와 안정 보호에 협력해야 한다. 분쟁국들은 또한 분쟁해역에서 일방적인 탐사나 천연자원 채취를 자제해야 한다.

법제

유엔해양법협약(UNCLOS)은 중요한 해양신뢰구축 방안이다. 실질적인 해양국가들은 기타 관련 국제해양협약과 국제관습법 외에도 유엔해양법협약 법규를 지켜야 한다. 그러나 해양법에는 애매한 부분이 다수 존재한다. 특히 배타적경제수역(EEZ) 제도와 관련된 조항에서 그러하다. 배타적경제수역 제도는 연안국들의 권리와 의무, 그리고 사용국들의 권리와 의무 간의 조심스런 균형을 반영하고 있다. 해양법이 불확실성을 가지고 있다는 점을 고려할 때, 공통된 이해를 위한 대화는 아마도 실제적 가치를 지닌 해양신뢰구축 방안일 것이다.

유엔해양법협약은 국제제도이지만, 해상운송, 어업, 해저광물채취, 해양환경보호, 탐색과 구조 등에 관한 다른 해양제도들도 있다. 이에 따라 해양의 현재 사용국들은 어느 문제의 해결을 추진할 때 다양하고 복잡한 규범과 원칙, 정책결정 과정에 직면하고 있다.

남중국해 중재 사건은 남중국해에서의 권리를 주장하는 국가가 유엔해양법협약 하의 제3자에게 분쟁을 맡긴 최초의 시도였다. 그러나 유엔해양법협약 하의 강제적 분쟁 해결 면에서 가진 가치에도 불구하고, 이 사건은 양국의 실제적 분쟁 해결에 만족할 만한 기여를 하지는 못하였다. 이것은 국제 법률문화에 의문을 제기하였다. 법제신뢰구축방안처럼, 정치적이고 지역적 맥락에서 해양 문제를 해결하기 위해서 적절한 접근법을 선택하고자 하는 모든 국가의 정치적 의지가 존중받아야 한다.

항행

발표자는 지역 항행의 안전을 확보할 뿐 아니라 긴장을 줄이고 갈등을 예방하는 해양신뢰구축 방안의 구축에 대해서 생각해 보고자 한다. 유엔해양법협약과 1972년에 채택된 국제해상충돌예방규칙(International Regulations for Preventing Collisions at Sea)은 모든 국가의 의무를 법적으로 구속하는 다자협약이다. 구속력이 없지만, 2014년의 "해상에서의 우발적 충돌방지 기준(Code for Unplanned Encounters at Sea)" 은 해양에서의 안전한 상호작용 의무에 대해서 더 적절한 방안을 제공하였다. 중국과 미국은 2014년과 2015년에 "공중 및 해양 충돌 안전을 위한 행동규칙(Rules of Behavior for Safety of Air and Maritime Encounters)" 에 대해서 법적 구속력이 없는 양해각서를 조인하였다. 비록 많은 문제들이 해결되지 않은 채 존재하지만, 이 양해각서는 양국 해군 간의 신뢰구축에 큰 기여를 할 것이다.

지역협력

남중국해 지역의 평화와 안정을 실현하기 위해서 발표자는 4가지 측면에서 남중국해 분쟁을 위한 실용적 분쟁관리제도를 제안한다. 이것은 환경안보, 어장안전, 그리고 해양 거버넌스의 역할을 설명하는 것인데, 구체적으로 남중국해 협력의 추진력으로서의 환경안보, 남중국해 분쟁 해결의 출발점으로서의 어업 협력, 지역 해양 거버넌스를 위한 틀로서의 유엔해양법협약, 그리고 정책과 연구방향을 결정할 토대로서의 사고방식의 전환이다.

Presentation Summary

Renato Cruz De Castro

Professor, International Studies Department, De La Salle University, Philippines

Confidence-Building Measures and Increasing Great Power Rivalry in the South China Sea: Examining the Ordeal of the ASEAN-China Code of Conduct (COC)

The paper examines the reasons behind the absence of a confidence-building regime in the South China Sea despite the growing tension triggered by the territorial dispute. Since the early 1990s, in the face of China's southward expansion to the South China Sea, the Association of Southeast Asian Nations (ASEAN) sought to establish a conflict management mechanism through the negotiation of a legally binding code of conduct (COC) to lower the risk of conflict among the claimant states. On 2 September 2002, ASEAN and China signed the "Declaration on a Code of Conduct (DOC) for the South China Sea," which was a primarily a political statement of broad principles of behavior aimed to stabilize the situation in the South China Sea and prevent accidental outbreak of conflict in the disputed areas. In addition, the two parties pledged to practice self-restraint in activities that could escalate the disputes, and to deepen their efforts to "build trust and confidence between and among them." When it was signed in 2002, the DOC was considered as an interim accord as well as the first step for further cooperation between China and the ASEAN member states. The two sides therefore were expected to continue working on the eventual adoption of a binding code of conduct in the South China Sea. ASEAN's goal is to transform the DOC to a legally binding Code of Conduct (COC) and not just a broad statement of principles.

As an association of small and medium powers, ASEAN has prioritized the pursuit of a binding conduct because it represents a complex commitment to creating and fostering a rules-based system, as opposed to a power-based, regional order. The COC should serve both as a rules-based framework containing a set of norms, rules, and procedures that guide the conduct of parties in the South China Sea, and a confidence building mechanism in support of "a conducive environment for peaceful settlement of disputes, in accordance with international law." China is an emergent regional power determined to alter the region's geographic status quo. Hence, it has resisted such efforts. In public, China agreed to discuss the South China Sea dispute with ASEAN on a multilateral basis. But in private, however, it sought to discuss the dispute bilaterally with each individual claimant state. Furthermore, China also insists that it can manage the dispute by directly engaging ASEAN without the involvement of external powers.

China's adroit ability to prevent a COC in the South China Sea and its efforts to divide this regional association have diminished ASEAN's role in managing the South China Sea dispute and in effect, have weakened the ASEAN-centric security institutions as part of the security structure in East Asia. This trend continues as the disparity of economic and military power between China and the ASEAN member states become wider and obvious. Consequently, this alarmed the other great powers in the region that warily observed ASAEN's diminishing role in the South China Sea dispute in particular, and in regional security affairs in general.

Currently the United States and Japan are filling this space by strategically balancing China in the South China Sea. Beyond an immediate heighten tension in the disputed waters, increased strategic competition between China on the one hand, and the U.S. and Japan on the other hand, has complicated the peaceful management of the South China Sea dispute and has effectively diminished ASEAN's role on this issue. As the great power rivalry over the South China Sea intensifies, the smaller Southeast Asian states will ultimately make a choice between a superpower determined on maintaining the status quo and an emergent regional power resolute to alter the current territorial arrangements in maritime East Asia. This, in turn, will erode not only ASEAN's clout in East Asian security matters but also threaten its very existence as a regional association of small powers committed to peace and stability in Southeast Asia.

발제 요약문

신뢰구축방안과 남중국해에서 확대되는 강대국 경쟁: 아세안–중국 행동강령(Code of Conduct)의 난관 검토

레나토 크루즈 데 카스트로 필리핀 델 라 살레 대학교 국제학부 교수

본 발제문은 영토 분쟁으로 촉발된 갈등 심화에도 불구하고 남중국해에서 신뢰구축체제가 없는 이유를 검토한다. 1990년대초 이후, 중국의 남중국해로의 팽창에 직면하여, 동남아국가연합(아세안)은 영유권을 주장하는 국가들 간의 갈등 위험을 낮추기 위해서 행동강령(COC)을 합법적으로 구속하는 협상을 진행하며, 갈등관리 메커니즘을 확립하기 위한 노력을 하고 있다. 2002년 9월 2일, 아세안과 중국은 남중국해 행동선언(DOC)에 조인하였다. 남중국해 행동선언은 남중국해의 상황을 안정화하고 분쟁지역에서의 충돌 발생을 방지하기 위한 정치적이고 포괄적인 행동규칙 선언문이다. 게다가 아세안과 중국은 분쟁을 확대할 수 있는 행동을 스스로 규제할 것과 신뢰구축을 위한 노력을 지속할 것을 약속하였다. 2002년 행동선언이 조인되었을 때, 이것은 중국과 아세안 회원국 간의 잠정적 합의이자 차후 협력을 위한 첫걸음으로 고려되었고, 이에 따라 양측은 남중국해에서 행동강령을 구속하는 최종적 채택을 위한 노력을 지속할 것으로 여겨졌다. 아세안의 목표는 행동선언을 포괄적 원칙선언에서 법적 구속력이 있는 행동강령으로 전환하는 것이다.

약소국과 중견국의 연합체인 아세안은 구속력이 있는 행위 추구를 다른 무엇보다 중요시한다. 왜냐하면, 그것은 힘에 기반한 지역 질서에 대항하여 규칙 기반의 체제(rules–based system)를 만들고 발전시키는 복합적 책임을 나타내기 때문이다. 행동강령은 남중국해에서 당사국들의 행동을 설명하는 규범과 규칙, 절차를 포함한 규정 기반의 프레임이면서도 국제법에 따른 분쟁의 평화적 해결에 도움이 되는 환경을 지지하는 신뢰구축 메커니즘으로 사용되어야 한다. 그러나 지역의 지리적 현상유지를 변화시키는 신흥 지역강대국으로서 중국은 이러한 노력에 저항하여 왔다. 공개적으로 중국은 다자적 입장에서 아세안과 남중국해 분쟁을 논의하는 것을 동의했다. 그러나 비밀리에 중국은 각 당사국과 양자적 입장에서 분쟁을 논의하려고 하였다. 게다가 중국은 외부 세력의 개입 없이 중국이 직접적으로 아세안과 접촉함으로써 분쟁을 조정할 수 있다고 주장하고 있다.

중국은 노련하게 남중국해의 행동강령을 막고, 지역연합을 분할하기 위해 노력하고 있다. 이것은 남중국해 분쟁을 처리하는 데에서 아세안의 역할을 축소하였고, 사실상 동아시아안보 구조의 한 부분을 차지하는 아세안 중심의 안보기구를 약화시켰다. 중국과 아세안 회원국 간의 경제력 및 군사력의 차이가 확대됨에 따라 이러한 추세는 지속되고 있다. 결과적으로 지역 내의 기타 강대국은 이런 추세 때문에 남중국해 분쟁에서 아세안의 역할이 약화되는 것을 신중하게 관찰하고 있다.

현재 미국과 일본은 남중국해에서 전략적으로 중국과의 균형을 유지함으로써 이러한 공간을 채우고 있다. 분쟁 해역에서의 즉각적인 긴장 고조 외에도 중국과 미국, 일본 간의 전략적 경쟁의 확대는 남중국해 분쟁의 평화적 해결을 복잡하게 만들었고, 이 문제에 대한 아세안의 역할을 효과적으로 약화시켜왔다. 남중국해에서 강대국 간의 경쟁이 심화됨에 따라, 동남아시아 국가가 현상유지를 바라는 강대국과 동아시아에서 현재 영토를 변화시키려는 신흥 지역강대국 사이에서 선택을 할 수 있는 폭도 좁아지고 있다. 이것은 다시 동아시아 안보 문제에서 아세안의 영향력을 침식시킬 뿐 아니라, 동남아시아의 평화와 안정에 헌신한 약소국들의 지역연합의 존재를 위협할 것이다.

Special Session 1 특별세션 1

16:00-18:00 Cosmos+Violet 2F

"The Fourth Industrial Revolution and Defense Science and Technology"
4차 산업혁명과 국방과학기술

Key Issues

- Applications of new technology in the national defense area
- Development prospects for future weapons
- Each state's defense science policies for new technology
- Technology cooperative policies between civilians and the military
- Integrated cooperative measures covering security and the economy among states
- 국방 분야의 신기술 적용 실태
- 무기 형태의 미래 발전 전망
- 국가별 신기술에 대한 국방과학정책
- 민군 기술협력 정책
- 국가 간 안보와 비즈니스를 포괄하는 통합적 협력 방안

Moderator	**P. K. Singh** Director, United Service Institution, India
Presenters	**John Louth** Director, Defence, Industries and Society, Royal United Services Institute for Defence and Security Studies, UK **Maxim Shepovalenko** Deputy Director, Centre for Analysis of Strategies and Technologies, Russia
Appointed Discussants	**Reifqi Muna** Researcher, Center for Political Studies, Indonesian Institute of Sciences, Indonesia **Shim Hyun-chul** Professor, Department of Aerospace Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea
Special Discussant	**Suay Alpay** Vice Minister of Nationd Defense, Turkey

사회자	**피케이 싱** 인도 USI 소장
발제자	**존 루스** 영국 왕립합동국방안보연구소 국방산업사회연구소장 **막심 셰포바런코** 러시아 전략기술분석센터 부소장
지정 토론자	**레이프키 무나** 인도네시아 과학원 정치학센터 연구원 **심현철** 한국 과학기술원 항공우주공학과 교수
특별 토론자	**수아이 알파이** 터키 국방부 차관

Presentation Summary

John Louth

Director, Defence, Industries and Society, Royal United Services Institute for Defence and Security Studies, UK

Implications of the Fourth Industrial Revolution and Defence Science and Technology Changes from the Perspective of England

The Third Offset Strategy (TOS), announced by the US in November 2014, stressed the need for a step level change in American military capabilities to counter the increasing anti-access/area denial systems being developed by potential adversary states. The TOS emphasis was on the potential for innovation at many levels of defence, but technological change was to have a particularly significant role, given the rate of change in the commercial sector and the availability of disruptive technologies to peer state rivals and non-state groups.

This session will examine the implications of profound technological change from a UK perspective and asks what lessons can be gleaned for other states. The analysis is based on a mixture of desk-based research and three day-long workshops in the UK, from November 2016 to March 2017, which brought together senior stakeholders from the governments and private sectors of the UK, the US and continental Europe. Participants in the workshops were directed and challenged through the chairmanship of Lord Arbuthnot of Edrom, a retired UK defence minister and senior politician.

We will consider the core assertion that potential adversaries have developed or are developing threats to major Western platforms on the sea, in the air and on land that significantly increase the risks of deploying such platforms in strategic areas, including the Baltics and the North Sea, East Asia and the Gulf. Moreover, these potential adversaries continue to develop offensive cyber capabilities and technologies that threaten the Western use of space for surveillance, communication, navigation and other purposes. It would not be accurate to assert that potential adversaries have 'caught up' across the full range of Western defence capabilities, but they have effectively focused their efforts, particularly on sensors and space denial. There is a variety of extended-range precision missiles able to attack targets on land, at sea and in the air. There are thus growing challenges for UK and other NATO forces and their allies, especially for those concerned with force projection. The discussion will recognise that, in any major future conflict, an important part of the battle will be threats to critical national infrastructure from hostile cyber operations.

In response to these threats and uncertainties, the British Ministry of Defence (MoD) launched its own Defence Innovation Initiative in September 2016 and has committed £800 million over a decade for basic research purposes, as well as maintaining the assurance that the MoD's core science and technology budget will

be a minimum of 1.2% of the defence budget. However, these positive steps will need to be supplemented by significant changes to encourage a stronger innovation culture within government defence. The discussion will evolve to suggest that these should include:

- Establishing an appetite for risk in the public and private parts of the UK defence enterprise that recognises the need for experimentation and the inevitability of regular failure. Clearly, work that is not going to succeed needs to be identified quickly, so that failure is early and comparatively inexpensive.
- Managing innovation on a programme-by-programme, case-by-case basis, by being ready to prioritise valued areas, and searching for technology demonstrators and prototypes with potential in a range of capability applications. The potential of a system or piece of equipment to impact positively the UK's exports and prosperity should be taken into account. A range of technologies (including those at low, medium and high technology readiness levels) should be supported, and the balance managed between upgrading existing assets and the development of novel capabilities and systems.
- Reinforcing government readiness to work closely with the private sector, both locally and from around the world, especially given Brexit. If the UK MoD is to incentivise firms – including small and medium-sized enterprises – to bring their best thinking to defence, it may have to put aside an instinctive preference for competitive tendering and the desire to acquire control over the intellectual property it will use.
- Reviewing the Defence Equipment Plan published in January 2017 to ensure that innovation is a guiding principle for capital investment.

The political stances and developing capabilities of potential adversaries require that the UK consider its role in the world, not least its military links with the Middle East and East Asia. The UK must also, in conjunction with its allies, review thinking about how deterrence and conflict avoidance can be strengthened. The readiness of NATO to explicitly consider escalation to the nuclear level in the face of losses at the conventional level seems like a hangover from the Cold War and looks less appropriate and credible in the contemporary world.

As the UK reacts to the changing vulnerability of many of its forces, an overarching claim of the discussant is that, of the seven categories in the UK Defence Capability Framework (prepare, project, inform, command, operate, sustain and protect), most emphasis should be placed on the last of these: protect. This will have significant impact on new and expensive capabilities such as Carrier-Strike.

The work from which this presentation is derived offers a four-category approach to the analysis and treatment of specific capabilities and the hardware on which they are based. Summarised as Tolerate, Treat, Transform or Terminate, it is argued that capabilities that face only acceptable risks can be left in place (Tolerate). Other capabilities can be rendered less vulnerable by modest changes (Treat), which is broadly the agenda of the Strategic Capabilities Office in the US. More drastic additions to capabilities, probably taking longer to introduce, fall into the Transform category. Treat and Transform depend significantly on innovation success. Finally, it is recognised that some areas may have to be abandoned (Terminate) and alternative arrangements made, including possible increased reliance on other allies and partnerships.

The effective management of defence has never been easy and has arguably never been so demanding, given the range of challenges on the agenda, the importance of agility in the use of armed forces, and the prevalence of uncertainty and incidence of surprises. The capacity to innovate is a significant aspect of being able to deal with these issues. To maximise potential in this area, financial and governance changes, as well as a range of behavioural changes, will be needed.

Professor John Louth is Director, Defence, Industries and Society at the Royal United Services Institute for Defence and Security Studies (RUSI), in London, and a specialist adviser to the UK House of Commons Defence Select Committee.

발제 요약문

영국의 관점에서 본 4차 산업혁명과 국방과학기술 변화의 영향

존 루스 영국 왕립합동국방안보연구소 국방산업사회연구소장

2014년 11월 미국이 발표한 제3차 상쇄전략(Third Offset Strategy)은 잠재적 적국의 반접근(anti-access)/지역거부(area denial) 시스템 개발에 대응하기 위해서 미국의 군사력을 한 단계 발전시켜야 할 필요성을 강조하였다. 제3차 상쇄전략의 초점은 국방의 여러 단계의 혁신적인 발전 잠재력에 맞춰져 있다. 특히, 상업 부문의 변화속도와 경쟁국가 및 비국가 단체의 와해성 기술 이용 가능성을 고려할 때, 기술 변화가 가장 중요한 역할을 할 것으로 예상된다.

이 세션에서는 영국의 관점에서 기술 변화의 함의를 연구하고 이를 기초로 어떤 교훈을 배울 수 있는가 물을 것이다. 이 분석은 이차적 연구와 2016년 11월부터 2017년 3월 사이에 진행된 연구의 여러 워크샵에 기초하여 진행된다. 이 워크샵에는 영국, 미국 그리고 유럽 대륙의 정부 및 민간 기관의 고위 관계자들이 참여하였고, 영국 전 국방부 장관이자 고위 정치가인 제임스 아버스넛이 의장을 맡아 워크샵 참가자들을 총괄하였다.

우리는 잠재적 적국이 해양, 공중 그리고 육상에서 서구의 주요 플랫폼에 위협을 가해왔거나 가하고 있다는 핵심 주장을 먼저 살펴볼 것이다. 이와 같은 행위는 발트해 연안과 북해 연안, 동아시아 그리고 걸프지역을 포함하는 전략지역에서 플랫폼 배치의 위험성을 상당히 증가시키고 있다. 뿐만 아니라, 잠재적 적국은 감시, 통신, 항행 및 기타 목적을 위한 서구의 공간 사용을 위협하는 공격적인 사이버 능력과 기술을 지속적으로 개발하고 있다. 이들이 모든 범위에서 서구의 방위력을 '따라잡았다'고 하는 것은 섣부른 주장이겠지만, 그들은 특히 센서 기술과 공간거부(space denial)에 집중하였다. 현재 육지, 해상, 공중에서 표적을 공격할 수 있는 다양한 사거리 연장 정밀 타격 미사일(extended-range precision missiles)이 존재하고 있다. 따라서 영국과 기타 NATO 군, 그리고 그들의 동맹국들, 특히 전투력 투사(force projection)를 걱정을 표하고 있는 국가들에 대한 도전이 증가하고 있다. 이 논의를 통해서 우리는 미래 분쟁에서는 적대적 사이버 작전으로 인한 국가 중요 기반시설에 대한 위협이 전투의 중요 부분을 차지할 것이라는 점을 알게 될 것이다.

이러한 위협과 불확실성에 대응하기 위해 영국 국방부는 2016년 9월 국방혁신 이니셔티브(Defence Innovation Initiative)에 착수하고, 10년에 걸쳐 기본연구에 8억 파운드를 지원하기로 하였다. 이외에도 국방부의 핵심 과학기술 예산이 국방 예산의 최소 1.2%가 될 것을 확약하였다. 그러나 국방의 혁신문화를 장려하기 위해서는 이러한 긍정적인 조치 외에도 상당한 변화가 필요하다. 이와 같은 변화들은 다음과 같은 내용을 포함한다:

- ▣ 영국 국방사업은 실험의 필요성과 필연적인 실패 가능성을 인식하고 있으며, 이에 따라 공공 및 민간 부분에서는 위험 감수의 정도를 설정한다. 성공 가능성이 낮은 사업을 빠르게 식별한다면, 조기에 사업을 중단하거나 비용을 절감할 수 있다.
- ▣ 가치 있는 영역을 우선시하고 다양한 기능의 응용프로그램에서 잠재력을 지닌 기술 모델이나 시제품을 연구하여, 프로그램별로 그리고 사례별로 혁신을 이룬다. 영국의 수출과 번영에 긍정적인 영향을 미칠 수 있는 시스템이나 장비의 잠재성을 고려해야 한다. 로우테크(low technology), 미디엄테크(medium technology), 하이테크(high technology) 단계의 기술들을 포함하여 다양한 기술들을 지원하고, 기존 자산의 개선과 새로운 기능 및 시스템 개발 간의 균형을 유지해야 한다.
- ▣ 민간 부문, 지역 및 세계 각지와의 긴말한 협력을 위해 정부의 준비 태세를 강화시킨다. 특히 브렉시트 이후 이것이 더 필요해졌다. 영국 국방부가 중소기업을 포함한 다양한 기업들이 국방을 최선으로 생각하도록 장려하고자 한다면, 경쟁 입찰에 대한 본능적인 선호와 지적 재산권에 대한 통제권을 얻고자 하는 욕구를 배제해야 한다.

▣ 2017년 1월에 발표된 국방 장비 계획(Defence Equipment Plan)을 검토하여 혁신이 자본 투자의 지침 원리임을 확인해야 한다.

잠재적 적국의 정치적 입장과 역량 증가는 세계 속에서 영국이 가진 역할에 대해 다시 생각하게 한다. 특히, 중동 및 동아시아와의 군사 관계에 있어서 그렇다. 영국은 또한 동맹국과 함께 억제(deterrence) 와 갈등회피(conflict avoidance)를 어떻게 강화할 것인지를 검토해야 한다. NATO가 전통적인 수준에서의 손실에 직면할 때, 그것을 핵 수준으로 확대하려고 하는 것은 냉전의 유물로 보일 뿐이다. 이것은 현 시대에는 적절하지 않아 보인다.

영국이 군대의 취약점 변화에 대응함에 따라, 필자는 영국의 국방력 체제의 7개 분야, 즉 준비, 계획, 정보 제공, 지휘, 운영, 유지 및 보호 중에서 마지막에 있는 '보호'를 가장 강조해야 한다고 생각한다. 이것은 항모공격(Carrier–strike)과 같은 고비용의 새로운 능력에 중요한 영향을 끼칠 것이다.

이 발제문은 그것들의 바탕이 되는 구체적 능력과 하드웨어를 어떻게 분석하고 진단할 것인가에 대한 4가지 분야의 접근법을 제공하고자 한다. 그 접근법은 용인 (Tolerate), 취급 (Treat), 변환 (Transform) 그리고 중단 (Terminate)으로 요약할 수 있다. 수용 가능한 위험에 직면하였을 때, 능력은 유지될 수 있다(용인). 적절한 변화를 통해서 기타 능력이 취약해지지 않도록 할 수 있는데(취급), 이것은 미국 전략능력국(Strategic Capabilities Office)의 전반적인 아젠다이기도 하다. 도입까지 비교적 오래 걸리는 과감한 변화들은 '변환' 범주에 속한다. 취급과 변환은 혁신의 성공에 달려있다. 마지막으로, 일부 지역은 포기해야만 하고(중단), 대안이 만들어져야만 한다는 것을 인정해야 한다. 다른 동맹국 및 협력국에 대한 의존성 증가가 그 대안에 포함될 수 있을 것이다.

국방을 효과적으로 관리하는 일은 결코 쉬운 일이 아니다. 세션 의제가 주는 도전의 범위, 군 부대 활용에 있어서 기민함의 중요성, 불확실성의 증가와 충격적 사건의 발생 등을 고려할 때, 효과적인 국방관리는 더욱 힘든 일이 되었다. 혁신 역량은 이러한 문제를 해결할 수 있는 중요한 측면이다. 이 분야의 잠재력을 극대화하기 위해서는 행동적 변화뿐 아니라 재정적, 행정적 변화가 필요하다.

Presentation Summary

Maxim Shepovalenko

Deputy Director,
Centre for Analysis of Strategies and Technologies (CAST) Moscow, Russia

Fourth Industrial Revolution and Technology Development Prospect

The Fourth Industrial Revolution (4IR) could be best described as the fusion of the physical or real and digital or virtual worlds, generating a cross-disciplinary through-engineering effect across the entire value chain, vertically and horizontally, and across the full life cycle of both products and services.

The transition to the 4IR occurs against the background of the following global trends and challenges:

- Change in the industrial production requirements
- Rise in product sophistication and diversity
- Surge in tempo of manufacture and delivery
- Increase in data volume and timeliness of processing
- Depletion of resources (energy, water, minerals, etc.)
- Pressure onto production as regards price competition

The 4IR is commonly referred to as the Industry 4.0, or Advanced Manufacturing, or whatsoever else, is a networking of hardware, software and human expertise bringing about a threesome change in technology, management and labour.

The evolving technology package is based on full-fledged digitisation throughout the value chain and the product life cycle. This increased digitalisation of the manufacturing process, which rests on the three principal elements, the Internet of Things (IoT), the Big Data and the Cyber-Physical Systems (CPSs), will allow for a decentralised autonomous resource-efficient production, within the physical-to-digital-to-physical cycle, featuring inter alia robotics, additive manufacturing, artificial intelligence and cognitive technologies, advanced materials, augmented reality, etc. This in turn will help attain real-time adaptation to changing customer requirements and profitably whilst producing even the smallest batch product sizes.

Whereas the 4IR represents an integration of the information technologies (ITs), related to business process and office automation, and operations technologies (OTs), related to industrial process and factory automation, only few of them could be attributed to as the revolutionary ones. In fact, these are the CPSs, artificial intelligence and cognitive technologies, and, perhaps prescriptive analytics. The rest are of reformist (IoT, virtual and augmented reality, swarm intelligence, big data, cloud computing, robotics, machine learning, additive manufacturing, etc.) or even evolutionary (wearables, C-RAM, mobile computing, sensor miniaturisation, wireless broadband, AIDC, microchip implants, etc.) nature. A revolution in any system leads to all-out qualitative changes mandating the abandoning of status quo. A reform

implies much of the same, yet relative only to a certain part of the system, leaving the main body untouched. Evolution transforms the whole system in an unhasty and pitch-free manner.

With due regard to the above, the 4IR-related technologies abound, but so far they hardly bring about truly fundamental changes as regards the entirety of the system, just enable doing the mixture as before slightly faster, slightly better, slightly leaner. Simply put, this technology package is not the 4IR proper; rather a precursor or a runup thereto. The problem lies with basic research discoveries which are running behind the schedule in quantum technologies, photonic technologies, membrane technologies, micromechanics, fusion nuclear energy, gene engineering, and others; in the absence of fundamental breakthroughs, all that is left to do is to 'polish up' the existing technologies, cutting the costs associated therewith.

Nevertheless, digital technologies are ultimately of disrupting nature as regards the existing manufacturing value chain, calling for the new patterns in the business management process. This implies redesigned interaction between system (subsystem) integrators, typically large, multinational corporations, and component/material providers, typically small- and medium-sized businesses (SMEs), at national or regional levels. The latter are facing challenges in sustaining the Industry 4.0 supply chains (costs and risks related to information security, reduced flexibility and strategic independence), the former are taking risks associated with integrity of supply chains and those of eventual oligopoly of key component/material providers.

The labour roles will change in terms of content, work processes and work environment. These will require greater freedom in decision-making, increased personal responsibility, decentralised management, more holistic and socio-technical methods of work organization as compared to the previous division of labour concept. The typical Industry 4.0 worker is currently seen as a STEM degree graduate, also enjoying sufficient managerial and communication skills. Essentially, the 4IR-related neo-industrialisation is the issue of a mass-scale skilled labourer jobs.

As regards the industry New Look, the 4IR effect will be coming into its own on the three interconnected levels:

- on macroeconomics level – regionalization and localization of added value chains (business clusters)
- on microeconomics level – focus onto economy of scale, lean manufacturing, product life cycle management (PLM), product customization, etc.
- on technology level – production automation and robotisation, use of advanced materials, etc.

The emerging post-industrial economy in the developed nations is often called the innovation one. In reality, the once industrial capitalism has evolved into the finance capitalism, and the end product of today's finance capitalism is a neo-rentier economy. The prime factor standing behind the GDP growth in such an economy is not the sustainable development and effective use of productive forces within the knowledge economy, but rent-seeking behavior aimed at creating added value associated with monopoly over material resources, intellectual wealth and organizational health, mostly in the soft, and primarily finance, services sector. This transformation of the industrial capitalism into the financial one, in some cases, was accompanied by de-industrialisation and transfer of production capacity to low-wage countries.

Currently, the global economy is layered in three tiers: four Tier 1 economic powerhouses (the United States, the European Union, China and Japan), thirteen Tier 2 economic powerhouses (Brazil, Russia, India, Australia, Mexico, Republic of Korea, Saudi Arabia, Turkey, Indonesia, Argentina, Nigeria, South African Republic and Egypt), and the rest of the world's Tier 3 developing economies.

Tier 1 economic powerhouses make their living by obtaining four kinds of rent, i.e. leadership rent (size of the economies), finance rent (issue of reserve currencies and marketable securities), technology rent (patent monopoly), and migration

rent (brain drain). Tier 2 economic powerhouses and Tier 3 developing economies are surviving at the cost of resource rent (oil and gas, other mineral resources), or social and ecological rent (low-wage pollution-intensive production), or geostrategic rent (foreign military infrastructure), or combination thereof.

The ongoing, or rather upcoming, 4IR will see the increased competition for innovation rent, with attempts by most of contenders, especially those of the Tier 2 economic powerhouses, to create new global value chains at most or significantly modify the existing ones at least. This will occur against the background of reshoring efforts by Tier 1 economic powerhouses. It might well be that we see quite a few novel alliances appear, on both global and regional scale, based on shared access to innovative technology and qualified labour.

In the context of defence science and technology, the 4IR and technology package associated therewith would have the following implications:

- Skilled and qualified labour, and not machinery, however precise it might be, is the most valuable asset. High-wage economy prevails not the low-wage one, which calls for revisiting the notion of competitiveness. A consistent lifelong STEM education is the key to success.
- Increased affordability of programmes regardless of production rates, with the acquisition cost not being dependent on the acquisition quantity and with the prime costs being those of the R&D (in the U.S. DOD parlance, Technology Maturation and Risk Reduction (TMRR) + Engineering and Manufacturing Development (EMD) phases, i.e. between MS A and MS C).
- Usage data collected online facilitates the workup of the user requirements paper for upgrading the system and developing the follow-up capability.
- Improved data reliability for the system Life Cycle Sustainment planning; Performance-Based Logistics (PBL) becomes not the preferred, but the only viable modus operandi in the Operations and Support (O&S) phase, minimising both system down time and logistics enterprise footprint.
- Customisation throughout the system lifecycle promotes opportunities for Configuration Management (CM) multinational collaboration programmes and cross-border sales, as well as the ease of block-to-block transfer for the home user.
- Ease of prototyping significantly shortens the system development time (time to market).
- Blurred distinction between the 'low-end' military and the 'high-end' civilian technologies; predominant double-use open-architecture orientation on the equipment/subsystem level, yet specialised design on the platform/system level.
- In the long run, agility and flexibility permitting to switch production from one class of systems to another.
- Improved business efficiency: production costs down by 10 to 50 percent, production time down by 20 to 70 percent, earnings growth by 10 to 50 percent, slump in manufacturing defects, innovative SME clustering.

Provided the rates of economic growth and technology progress keep up the current pace, one might expect the above Industry 4.0/Advanced Manufacturing mode of operations for the defence science and technology come into being in the 2020s and move further into maturity phase in the 2040s. Furthermore, in 2020-25, or perhaps shortly thereafter, the true 4IR, encompassing all much held off breakthroughs in basic research and the relevant applied technologies, might occur, in which case the minimum needed industrial infrastructure, i.e. (i) end-to-end digitalization, including 3D digital design; (ii) advanced materials, including smart ones, and (iii) smart control systems, smart grids, reconfigurable and flexible collaborative self-learning industrial robot systems, would hopefully be already in place.

End-user-wise, artificial intelligence (AI) and military robots, or autonomous weapon systems, are the mainstream. Yet it will take decades before AI will be able to get around to human intelligence in situations that require judgment and knowledge against the background of high uncertainty. Currently, the military have a range of Gen 1 robots fielded which are mostly meant for accomplishing combat support and combat service support missions. These are remotely operated (human-in-the-loop) systems performing skill- and rule-based tasks. Tested and evaluated are Gen 2 robots which are essentially quasi-autonomous (human-on-the-loop) systems with synthetic sensorium and artificial neural networks which can operate in a-priory unknown environment and adapt themselves to the situation changes. These are capable of detecting, identifying, prioritising and destroying targets, yet provisions are made for human override. The advent of Gen 3 robots, or truly autonomous (human-out-of-the-loop) systems, depends on development of self-starting AI techniques combined with the state-of-the-art technologies in navigation, identification friend or foe (IFF), safe and controllable use of weapons, independent power source, camouflage and signature reduction, etc. So far, prototypes of these systems exist only on the laboratory model level. The two major stumbling blocks are efficient problem-setting/problem-solving algorithms and solving tasks and foolproof IFF. In the average-case scenario, fully autonomous systems will be fielded in the 20 to 30 years from now, or, in the best-case scenario, even earlier.

발제 요약문

4차 산업혁명과 기술 발전 전망

막심 셰포바런코 러시아 전략기술분석센터 부소장

4차 산업혁명은 물질/실제 세계와 디지털/가상 세계와의 융합으로 묘사할 수 있다. 이것은 모든 가치사슬(value chain)과 상품 및 서비스의 전체 수명주기를 공학 효과를 통하여 다양한 분야로 수직적이면서도 수평적으로 창출한다.

4차 산업혁명으로의 이행은 다음과 같은 세계적 추세와 도전 배경에 대응하여 일어난다.

- ▣ 산업생산 요건의 변화
- ▣ 상품의 고급화와 다양성 상승
- ▣ 제조 및 배달의 급격한 속도
- ▣ 데이터의 규모와 처리의 적시성 증가
- ▣ 에너지, 수자원, 미네랄 등 자원의 고갈
- ▣ 가격경쟁에 따른 생산 압박

4차 산업혁명은 흔히 인더스트리 4.0(Industry 4.0) 혹은 차세대 제조기술(Advanced Manufacturing) 등으로 언급되는데, 기술, 관리 및 노동에서 변화를 가져오는 하드웨어, 소프트웨어 그리고 전문가의 네트워킹이라고 할 수 있다.

발전하는 기술패키지는 가치사슬과 상품 수명주기의 완전한 디지털화에 기반을 두고 있다. 사물 인터넷(Internet of Things), 빅 데이터(Big Data), 가상물질 체계(Cyber–Physical System)라는 3개의 중요요소에 기반을 두고, 증가한 제조과정의 디지털화는 물질–디지털–물질로 순환하는 사이클 안에서 분산화되고 자율적인 고효율 생산을 가능하게 할 것이다. 특히, 이것은 로봇공학, 첨삭 가공, 인공지능, 인지기술, 신소재, 증강현실 등을 포함한다. 이것은 변화하는 고객 요구에 대한 실시간 대응을 가능하게 하고, 가장 작은 크기의 제품을 생산하더라도 이익을 창출하게 할 것이다.

4차 산업혁명은 비즈니스 프로세스 및 사무자동화와 관련된 정보기술(information technology)과 산업공정 및 공장자동화와 관련된 운영기술(operations technology)의 통합으로 나타낸다. 그러나 실질적으로 혁명적이라고 부를 수 있는 것은 거의 없다. 사실 혁명적이라 부를 수 있는 것들은 가상물리시스템과 인공지능, 인지기술, 그리고 어쩌면 처방분석(prescriptive analytics) 정도이다. 이외의 것들은 개혁적(사물인터넷, 가상현실, 집단지성, 빅 데이터, 클라우드 컴퓨팅, 로봇공학, 기계 학습, 첨삭 가공 등)이거나, 진화적(착용장치, C–RAM, 모바일 컴퓨팅, 센서 소형화, 와이브로, AIDC, 마이크로칩 이식 등)이다. 어떤 시스템에서의 혁명은 현상유지를 포기하게 하는 전면적 질적 변화를 야기한다. 반면에 개혁은 혁명과 동일한 특징을 암시하지만, 오직 시스템의 어느 부분과 관련되어 있고, 시스템 전체에는 영향을 끼치지 않는다. 그리고 진화는 시스템 전부를 점진적으로 변화시킨다.

위에서 언급한 것과 같이, 4차 산업혁명과 관련된 기술이 많음에도 불구하고, 지금까지 이 기술들은 시스템 전체에 대한 근본적인 변화를 일으키지는 못하고 있다. 다만 조금 더 빠르고 날렵한 기술의 융합을 가능케 하였을 뿐이다. 간단하게 말하면, 이 기술패키지는 4차 산업혁명이라기보다는 4차 산업혁명의 선도자 또는 4차 산업혁명으로의 준비라고 할 수 있겠다. 문제는 양자 기술(quantum technology), 광자 기술(photonic technology), 막이용 기술(membrane technology), 마이크로공학(micromechanics), 핵융합에너지(fusion nuclear energy), 유전자공학(gene engineering) 등에서 행해지는 기본연구가 점점 늦춰지고 있다는 것이다. 확실한 돌파구가 없는 현재 상황에서, 할 수 있는 것은 존재하는 기술을 숙달하고 관련비용을 최소화하는 것이다.

그럼에도 불구하고, 디지털 기술은 사업 경영 프로세스에서 새로운 패턴을 요구하기 때문에 기존의 제조 가치사슬에 대한 파괴의 속성을 지니고 있다. 이것은 시스템 통합자(보통 대기업 또는 다국적기업)와 부품/원재료 공급자(보통 국가 및 지역

차원의 중소기업) 간 상호작용의 재설정을 암시한다. 후자는 인더스트리 4.0 공급망 유지(정보 보안에 관련된 비용과 위험, 유연성과 전략적 독립성의 감소)에 어려움을 겪고 있으며, 전자는 주요 부품/원재료 공급자의 소수 독점과 공급망 보존과 관련하여 위험을 감수하고 있다.

콘텐츠와 작업 프로세스, 그리고 작업 환경 면에서 노동의 역할은 변화할 것이다. 이 변화는 기존의 노동 개념과 비교할 때, 의사 결정의 자유, 개인의 책임 확대, 분권화된 경영, 업무 조직의 사회기술적 방식을 요구할 것이다. 전형적인 인더스트리 4.0 노동자는 STEM 학위 수여자이면서 충분한 경영능력과 의사소통 능력을 갖추고 있는 사람이다. 본질적으로, 4차 산업혁명과 관련된 신산업화는 대규모의 숙련노동 직업에 관한 문제가 될 것이다.

산업의 새로운 유행이라는 측면에서, 4차 산업혁명의 효과는 다음과 같이 상호 연결된 3가지 차원으로 나타날 것이다:

- ▣ 거시경제적 차원 · 부가가치사슬(비즈니스 클러스터)의 지역화와 현지화
- ▣ 미시경제적 차원 · 규모의 경제, 린 제조(lean manufacturing), 제품수명주기관리(PLM), 제품 특화 등에 집중
- ▣ 기술적 차원 · 생산의 자동화와 로봇화, 신소재 사용 등

선진국에서 나타나고 있는 산업화 이후 경제(post-industrial economy)는 자주 이노베이션 원(Innovation One)이라고 언급된다. 현실에서 산업자본주의는 금융자본주의로 진화했으며, 오늘날 금융자본주의의 최종 산출물은 신임대 경제(neo-rentier economy)이다. 이와 같은 경제에서 GDP성장을 지원하는 중요요소는 지속 가능한 발전이나 지식경제 안에서 생산력의 효과적 사용이 아니다. 오히려 주로 금융 및 서비스 부분에서 원재료 독점, 지적 재산(intellectual wealth), 조직건강과 관련하여 부가가치 창출을 목적으로 하는 금리추구 행위이다. 산업자본주의에서 금융자본주의로의 전환은 어떤 경우 탈산업화와 저임금 국가로의 생산능력 이동을 수반한다.

현재 글로벌 경제는 3개의 층으로 나누어져 있다: 제1층에 있는 4개의 경제강국(미국, EU, 중국, 일본), 제2층에 있는 13개의 경제강국(브라질, 러시아, 인도, 호주, 멕시코, 대한민국, 사우디아라비아, 터키, 인도네시아, 아르헨티나, 나이지리아, 남아프리카 공화국, 이집트), 그리고 제3층에 있는 나머지 개발도상국들이 그것이다.

제1층에 있는 경제강국은 4종류의 임대료(rent)를 획득함으로써 국가를 운영한다. 예를 들어, 리더십 임대료(경제의 규모), 금융 임대료(준비 통화 및 시장성 유가증권 발행), 기술 임대료(특허 독점), 이주 임대료(두뇌 유출)가 그것이다. 제2층의 경제강국과 제3층의 개발도상국은 자원 임대료(석유, 가스, 천연자원 등), 사회생태학적 임대료(저임금이면서도 환경오염을 야기하는 생산), 전략 지정학적 임대료(해외 군사 기반시설) 등과 그것들의 조합으로 연명한다.

현재 진행 중인, 또는 앞으로 다가올 4차 산업혁명으로 인해서 혁신 임대(innovation rent)에서의 경쟁이 증가할 것이다. 이것은 제2층의 경제강국들이 새로운 글로벌 가치사슬을 창출하거나, 최소한 기존의 가치사슬들을 상당부분 수정하고자 시도할 것이기 때문이다. 이것은 제1층 경제강국들의 리쇼어링(reshoring) 노력에 대응하여 일어날 것이다. 그리고 아마도 혁신 기술과 숙련 노동에 대한 접근이 공유되면서, 글로벌과 지역적 규모에서 새로운 동맹들이 등장하는 것을 보게 될 것이다.

국방과학기술의 관점에서 4차 산업혁명과 기술 패키지는 다음과 같은 함의를 내포할 것이다.

- ▣ 기계가 얼마나 정교하든지 간에, 기계가 아닌 숙련노동이 가장 중요한 자산이다. 고임금 경제가 저임금 경제를 이기는 것이 아니다. 이것은 경쟁으로의 귀환을 요구할 뿐이다. 꾸준한 STEM 교육이야말로 성공의 열쇠다.
- ▣ 취득원가가 취득량에 의존하지 않고 원가가 R&D의 가격이 되면서, 생산율과 상관없이 프로그램 비용이 증가한다. (미국 국방부의 표현에 따르면, 이것은 기술 성숙화와 위험 감소(Technology Maturation and Risk Reduction) + 엔지니어링 및 제작 개발(Engineering and Manufacturing Development)이다.)
- ▣ 온라인에서 수집된 활용 데이터는 시스템 업데이트와 후속조치 능력 개발을 위한 사용자 요구자료 구축을 가능하게 한다.

- ▣ 시스템 수명주기 유지 계획에 대한 데이터의 의존성이 개선된다; 성과기반군수(PBL)가 하나의 선택지가 아니라 운영 및 지원(Operations and Support) 단계에서 유일하게 실행 가능한 방식이 될 것이다.
- ▣ 시스템 수명주기를 통한 맞춤화(customisation)는 형상관리(configuration management) 다국적 공동 프로그램과 범국가 판매 및 일반가정 사용자에게 용이한 블록 투 블록 전송(block to block transfer)의 기회를 촉진한다.
- ▣ 용이한 시제품 생산은 시스템 개발 시간과 제품 출시 시기를 단축한다.
- ▣ 저가(low-end) 군사기술과 고가(high-end) 민간기술의 구분이 모호해진다. 뚜렷한 이중사용 개방형 구조(double-use open-architecture) 성향이 장비/하부시스템 단계에서 나타나고, 플랫폼/시스템 차원에서 전문화된다.
- ▣ 장기적으로 볼 때, 민첩성과 유연성 때문에 생산이 어느 한 시스템에서 다른 시스템으로 전환되는 것이 허용된다.
- ▣ 비즈니스의 효율성이 개선된다: 생산비용은 10~50%, 생산시간은 20~70% 하락할 것이다. 그리고 수익성장률은 10~50% 증가할 것이다. 제조상의 결함은 낮아지고, 혁신적 SME는 집단으로 모일 것이다.

경제성장률과 기술진보가 현재 속도를 유지한다고 가정할 때, 혹자는 국방과학기술을 위한 인더스트리 4.0/차세대 제조기술 운영방식이 2020년대에 나타날 것이며, 2040년대에는 성숙단계에 들어설 것이라고 예상한다. 게다가 2020-2025년, 또는 그로부터 얼마 지나지 않아 기본연구와 관련 응용기술에서 수많은 혁신적 발전을 이루는 진정한 4차 산업혁명이 등장할 수도 있다. 그러면 (i) 3D 디지털 디자인을 포함하는 엔드투엔드(end-to-end) 디지털화, (ii) 스마트 소재들을 포함하는 첨단 소재, (iii) 스마트 제어 시스템, 스마트 그리드(smart grid), 그리고 유연하고 협력적인 가변 구조형의 자기 학습 산업로봇 시스템이 존재할 수도 있을 것이다.

엔드유저와이즈(end-user-wise), 인공지능(AI)과 군사 로봇 혹은 자율무기시스템이 대세가 될 것이다. 그럼에도 불구하고, 불확실성에 대한 판단과 지식이 요구되는 상황에서 인공지능이 인간지능을 대체하기까지는 수십 년이 걸릴 것이다. 현재 군대에서는 전투지원과 전투근무지원을 수행하는 Gen 1 로봇이 현장에서 활용되고 있다. 이 로봇은 기술과 규범에 기초한 임무를 실행하는 원격 조정형(인간 참여형) 시스템이다. Gen 2 로봇에 대한 실험과 평가가 진행되었는데, 이 로봇은 준자율형(인간 개입형) 시스템으로, 합성 감각과 인조 신경망을 장착해 미지의 환경에 스스로 적응하여 작동된다. 이 로봇은 목표물을 감지 및 식별하고 우선순위를 부여하여 파괴할 수 있지만, 인간이 이 기능을 무효화할 수 있다. Gen 3 로봇, 혹은 자율형(인간 배제형) 시스템은 자기 시동 AI 기술과 기타 최첨단 기술(예를 들어, 최첨단 항행기술, 피아식별(Identification Friend of Foe), 안전하고 제어 가능한 무기 사용, 독립적인 전력원, 위장 기술 등)의 융합 개발에 의존한다. 아직까지 이러한 시스템의 원형은 실험실 모델로만 존재한다. 두 개의 가장 큰 걸림돌은 효율적 문제 인식 및 해결 알고리즘과 너무 단순한 IFF기술이다. 현재 상황으로는 완전 자율 시스템이 현장에 투입되기까지는 20-30년 정도가 걸릴 것으로 예측된다. 물론 경우에 따라 이 시기가 앞당겨질 수도 있을 것이다.

Special Session 2 특별세션 2

16:00-18:00 Orchid 2F

"The Nature of Future Warfare and National Defense Policy"
미래전 양상과 국방정책

Key Issues

- Changes and future direction of warfare accompanied by the development of new weapons
- Acquisition, integration and analysis of combat intelligence
- Changes of ways to strike targets
- Development direction of strategies and tactics
- States' defense policies regarding future warfare
- 현재 신무기 개발이 미치는 전쟁 방식의 변화 및 미래 발전 방향
- 전투정보의 획득과 통합 및 분석
- 목표물에 대한 타격 방식의 변화
- 전략 전술의 변화 방향
- 미래전에 대비하는 각국의 국방정책

Moderator	**Jean-Pierre Maulny** Deputy Director, French Institute for International and Strategic Affairs, France
Presenters	**Margaret E. Kosal** Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, USA **Teng Jianqun** Director, Department for American Studies, China Institute of International Studies, China
Appointed Discussants	**Tran Viet Thai** Deputy Director-General, Institute for Foreign Strategic Studies, Diplomatic Academy of Vietnam, Vietnam **No Hoon** President, Korea Institute for Defense Analyses, Republic of Korea
Special Discussants	**Cardozo Luna** Undersecretary of Nationd Defense, Philippines **Jody Thomas** Senior Associate Deputy Minister, Canada

사회자	**장 피에르 마울니** 프랑스 국제전략연구소 부소장
발제자	**마가레트 코살** 미국 조지아공대학 샘 넌 국제대학원 교수 **텅 지옌췬** 중국 국제문제연구원 미국연구소장
지정 토론자	**트란 비엣 타이** 베트남 국립외교원 외교전략연구소 부소장 **노 훈** 한국 국방연구원장
특별 토론자	**카도조 루나** 필리핀 국방부 차관 **조디 토마스** 캐나다 국방부 차관 수석차관보

Presentation Summary

Margaret E. Kosal
Associate Professor,
Sam Nunn School of
International Affairs
Georgia Institute of Technology,
USA

The Future of Warfare – It Won't Be the One We Expect

Emerging innovations within cutting-edge science and technology (S&T) areas are cited as carrying the potential to revolutionize governmental structures, economies, and military capabilities; others have argued that such technologies will yield doomsday scenarios and that applications of such technologies have even greater potential than nuclear weapons to radically change the balance of power.[1] These S&T areas include robotics and autonomous unmanned system; artificial intelligence; biotechnology, including synthetic and systems biology; the cognitive neurosciences; nanotechnology, including stealth meta-materials; additive manufacturing (aka 3D printing); and the intersection of all with information and computing technologies, i.e., cyber-everything and the internet of things.

As new and unpredicted technologies are emerging at a seemingly unprecedented pace globally, communication of those new discoveries is occurring faster than ever, meaning that the unique ownership of a new technology is no longer a sufficient position, if not impossible. They're becoming less expensive and more readily available. In today's world, recognition of the potential applications of a technology and a sense of purpose in exploiting it may be far more important than simply having access to it. While the suggestions that a new class of weapons that will alter the geopolitical landscape remain unrealized, a number of unresolved security puzzles underlying emerging technologies have implications for international security, defense policy, deterrence, governance, and diplomacy.

Conceptually, technologies can be seen as evolutionarily advancing current capabilities or those pressing to the 'bleeding edge' that enable disruptive, revolutionary capabilities developments. The ability to differentiate or gain insight into such has thus far not been explored or analyzed robustly with respect to strategic implications beyond a technologically-deterministic lens. The novel scientific principles that underlie the character of these uncertain technologies and their convergence with political and social institutions reveal conceptual and empirical confusion associated with assessing the security implications. There also is palpable confusion over the technical and strategic distinguishability and dominance of prospective offensive and defensive systems.

Contemporary analyses of these emerging technologies often expose the tenuous links or disconnections among mainstream scholarship on international security, understanding of the military technological innovation and acquisition processes, and fundamental understanding of the underlying science. Future trend analysis is a tricky task. Colin Gray has written, "Trend spotting is easy. It is the guessing as to the probable meaning and especially the consequences of trends that is the

real challenge."[2] The extent to which these emerging technologies may exacerbate or mitigate the defense challenges that states will pose in the future needs to be examined. How, when, where, and in what form the shifting nature of technological progress may bring enhanced or entirely new capabilities, many of which are no longer the exclusive domain of any single state, is contested and requires better understanding.

Claims for the potential impacts of technology can seem fantastic; at times, differentiating rhetoric from reality can be difficult. Of critical importance in considering the national and international security implications of technology is that anticipated scenarios should be plausible within constraints of physical viability as well as likely within institutional capacities and tacit capabilities.

The penultimate goal should not be to predict specific new technologies, which is rarely a high-fidelity pursuit except in retrospective, and one should be skeptical of any one or group that claims thy can do such. The aim should be to develop implementable and executable analytical frameworks to explain variable approaches to the development of strategically significant emerging S&T programs, to understand the impact of emerging technology on security in the 21st Century, to enable mechanisms for the world to govern the implications of its own ingenuity, and to inform defense and foreign policies.

There is a need to think strategically beyond current challenges. In the late twentieth and early twenty-first century, the world has struggled – and continues to do so – to deal with the proliferation challenges of new technologically-enabled weapons. Anticipating the types of threats that may emerge as science and technology advance, the potential consequences of those threats, and the probability that new and more disperse types of enemies will obtain or pursue them is necessary. The potential synergies between biotechnology and other emerging technologies, like additive manufacturing and the cognitive neurosciences, not only suggest tremendous potential for advancement in technology for commercial and beneficial applications but also raise new concerns. When asked what are the current approaches and thinking on means for deterring emerging technologies of concern, then-USSTRATCOM Commander General Robert Kehler (USAF) responded that "surprise is what keeps me up at night" and cited current uncertainty in how to assess and address emerging and disruptive technologies.[3]

Understanding these changing paradigms and the implications for modern warfare starts with an awareness of the factors driving the capabilities, understanding the underlying science and the challenges of foreign policy, considering the changing nature of technological progress and the changing nature of conflict, and the relationship between science and security domestically and internationally. The importance of bridging the technical and the human domain is increasing; the challenges are organizational, strategic, and enabling the right people to implement and execute it.

---

1 ADM David E Jeremiah (USN, ret), "Nanotechnology and Global Security," Palo Alto, CA; Fourth Foresight Conference on Molecular Nanotechnology, 9 November 1995.

2 Colin Gray, Another Bloody Century: Future Warfare, London, UK: Phoenix, 2007, p 38.

3 Comments at the "Sustaining the Triad: the Enduring Requirements of Deterrence" Conference, 8 November 2013, Naval Submarine Base Kings Bay, Georgia.

발제 요약문

미래전 – 우리의 예상과는 다를 것이다

마가레트 코살 미국 조지아공대학 샘 넌 국제대학원 교수

최첨단 과학기술 영역에서의 혁신은 정부 구조, 경제, 군사능력에서 대변혁을 일으킬 가능성을 수반하고 있다. 또한 어떤 이들은 그러한 기술들이 인류종말을 야기할 것이고, 그러한 기술들의 적용은 세력균형의 급격한 변화 측면에서 핵무기보다 더 큰 잠재력을 가지고 있다고 주장한다. 이러한 과학기술 영역은 로봇공학과 무인자동시스템, 인공지능, 합성생물학과 체계생물학을 포함하는 생명공학기술, 인지신경과학, 스텔스 메타물질을 포함하는 나노기술, 3D 프린팅으로 알려진 적층 가공, 그리고 사물인터넷과 같은 교집합적 특징을 지닌 모든 정보컴퓨터 기술을 포함한다.

예측 불가능한 신기술들이 전례 없는 속도로 전 세계에서 출현함에 따라, 새로운 발견들에 대한 의사소통도 더 빠르게 일어나고 있다. 이것은 가능하기만 하면 신기술의 특정 소유권이 더 이상 충분한 입장이 아니라는 것을 의미한다. 기술들은 더 싸지고 더 빠르게 사용 가능하게 되고 있다. 현시대에는 명확한 목적의식을 가지고 기술의 적용가능성을 인식하는 것이 단순히 그 기술에 접근하는 것보다 더욱 중요할 것이다. 지정학적 지형을 변화시킬 새로운 무기가 실현되지 않았음에도 불구하고, 새로 개발되는 기술의 기저에 깔린 수많은 미해결의 안보퍼즐은 국제안보, 국방정책, 전쟁억제, 거버넌스와 외교에 중요한 함의를 가지고 있다.

개념적으로, 기술은 점진적으로 발전하는 현재의 능력 또는 파괴적이고 혁명적인 능력개발을 가능케 하도록 '최첨단'을 촉구하는 능력으로 볼 수 있다. 그래서 기술상의 결정론적 시야에서 이것을 구분하거나 통찰하는 능력을 연구하여 왔고, 전략적 함의에 따라서 연구되거나 분석되지는 않았다. 이러한 불확실한 기술의 특징과 정치사회기구와의 결합의 기저를 이루고 있는 새로운 과학원리들은 안보적 의미 평가와 관련하여 개념적이고 실증적인 혼란을 드러내고 있다. 또한 기술적/전략적 분별능력과 장래의 공격/방어시스템의 우세에 있어서도 분명한 혼란이 존재한다.

최근 개발된 기술들에 대한 현재의 분석들은 국제안보, 군사기술 혁신과 그 취득과정 이해, 그리고 기본과학 이해 측면에서 주류학자와 미약하게 연결되었거나 단절되어 있다. 미래 동향분석은 까다로운 임무이다. 콜린 그레이(Colin Gray)는 "동향인식은 쉽다. 그러나 그것의 개연적 의미와 동향의 결과를 예측하는 것이 진정한 과제이다." 라고 하였다. 최근 발생하는 기술들이 미래에서 국가들이 제기할 국방과제를 가속화할 것인지 아니면 약화시킬 것인지에 대한 연구가 필요하다. 변화중인 기술발전이 어떻게, 언제, 어디에서 그리고 어떤 형태로 개선된 능력 혹은 완전히 새로운 능력을 가져올 것인가 하는 문제는 치열한 경쟁을 일으킬 것이고, 더 깊은 이해를 요구한다. 그러나 여기에 대한 해답은 더 이상 어느 한 국가만의 배타적 영역이 아니다.

기술의 잠재적 영향에 대한 요구는 공상처럼 보인다. 가끔 수사적 표현을 현실과 구분하는 것이 어려울 수 있다. 기술이 가진 국가적/국제적 안보 함의를 고려할 때, 예상시나리오는 물리적 실현가능성의 한계, 기관의 능력과 암묵적 능력(tacit capability)을 고려하여 타당하게 만들어져야 한다.

구체적 신기술을 예측하는 것이 목표가 되어서는 안 된다. 회고록을 제외하면 이런 방식은 충실한 결과를 얻기 어렵다. 그래서 어느 개인이나 단체가 그렇게 할 수 있다고 주장한다면 그들을 의심해야 한다. 목표는 실행 가능한 분석틀을 개발하는 것이다. 이 분석틀은 전략적으로 중요하게 개발되는 과학기술 프로그램의 발전에 대한 다양한 접근법을 설명하고, 21세기 안보에 있어서 신기술들의 영향을 이해할 뿐 아니라, 세계가 자신만의 창의성을 관리하는 메커니즘을 개발하고, 국방외교정책을 알리는 데 유익할 것이다.

현재의 도전과제를 초월하여 전략적으로 사고해야 할 필요가 있다. 20세기말과 21세기초에, 세계는 기술적으로 가능한 신무기의 확산문제를 다루기 위해서 노력하였고, 지금도 그렇게 하고 있다. 과학기술의 발전에 따라 새로 발생하는 위협 형태, 그 위협들의 잠재적 결과, 각처로 흩어지는 적들이 얻을 개연성을 예측하는 것이 필요하다. 생명공학과 적층 공학, 혹은 인지신경과학과 같은 신기술 간의 시너지 가능성은 상업적 또는 이윤 창출을 위한 기술의 거대한 발전 가능성을 제기할 뿐 아니라, 새로운 우려도 일으키고 있다. 우려스러운 신기술을 탐지하는 수단에 대한 현재 접근법이나 생각이 무엇이냐는 질문을 받았을 때, 미국 전략사령관 로버트 켈러(Robert Kehler)는 "놀라운 소식 때문에 나는 잠자리에 들지 못한다"고 대답하면서 새로 개발되는 파괴적 기술을 평가하고 다루는 방법에 있어서의 불확실성을 언급하였다.

변화하는 패러다임과 현대전쟁의 의미를 이해하는 것은, 기본과학과 외교정책의 과제를 이해하고 기술발전과 충돌의 변화하는 속성을 고려하여, 능력을 추진하는 요소들과 과학과 안보 간의 국내/국제적 관계를 인식하는 것에서 시작된다. 과학영역과 인간영역을 연결하는 것이 더욱 중요해지고 있다. 이런 시점에서 과제는 적합한 사람들이 그것을 실행하게 하는 것이다.

Presentation Summary

Teng Jianqun
Director, Department for American Studies, CIIS, China

China's Military Reform and its New Posture

There have been at least ten rounds of military reform in PRC since its founding in 1949. For most of these rounds of reform, the reduction of troops and weapon has been the core part of it. The new round of military reform, which was initiated from September 2015 during the parade in commemorating the 70th anniversary of anti-Japanese war victory, is not only the reduction of troops but also a quality streamline of the PLA.

I. The new changes of the PLA

As Chairman of CMC Xi jiping addressed that this round of military reform is targeted as the streamline of the PLA and re-establishment of new military doctrine for the country. After more than two years restructuring of the PLA, we have witnessed the following changes of China's Armed Forces.

1. Commanding Chain

A. The new Centralized Central Military Committee.
B. The new 5 Commands.

2. The 4 services of the PLA: Army, Navy, Air Force, and Rocket Force.

In line with the strategic requirement of offshore waters defense and open seas protection, the PLA Navy (PLAN) will gradually shift its focus from "offshore waters defense" to the combination of "offshore waters defense" with "open seas protection," and build a combined, multi-functional and efficient marine combat force structure. The PLAN will enhance its capabilities for strategic deterrence and counterattack, maritime maneuvers, joint operations at sea, comprehensive defense and comprehensive support.

In line with the strategic requirement of building air-space capabilities and conducting offensive and defensive operations, the PLA Air Force (PLAAF) will endeavor to shift its focus from territorial air defense to both defense and offense, and build an air-space defense force structure that can meet the requirements of informationized operations. The PLAAF will boost its capabilities for strategic early warning, air strike, air and missile defense, information countermeasures, airborne operations, strategic projection and comprehensive support.

In line with the strategic requirement of being lean and effective and possessing both nuclear and conventional missiles, the PLA Second Artillery Force (PLASAF) will strive to transform itself in the direction of informationization, press forward with independent innovations in weaponry and equipment by reliance on science and technology, enhance the safety, reliability and effectiveness

of missile systems, and improve the force structure featuring a combination of both nuclear and conventional capabilities. The PLASAF will strengthen its capabilities for strategic deterrence and nuclear counterattack, and medium- and long-range precision strikes.

In line with the strategic requirement of performing multiple functions and effectively maintaining social stability, the PAPF will continue to develop its forces for guard and security, contingency response, stability maintenance, counter-terrorism operations, emergency rescue and disaster relief, emergency support and air support, and work to improve a force structure which highlights guard duty, contingency response, counter-terrorism and stability maintenance. The PAPF will enhance its capabilities for performing diversified tasks centering on guard duty and contingency response in informationized conditions.

3. The establishment of the strategic support troops

II. The new tasks of PLA

Building a strong national defense and powerful armed forces is a strategic task of China's modernization drive and a security guarantee for China's peaceful development. Subordinate to and serving the national strategic goal, China's military strategy is an overarching guidance for blueprinting and directing the building and employment of the country's armed forces. At this new historical starting point, China's armed forces will adapt themselves to new changes in the national security environment, firmly follow the goal of the Communist Party of China (CPC) to build a strong military for the new situation, implement the military strategic guideline of active defense in the new situation, accelerate the modernization of national defense and armed forces, resolutely safeguard China's sovereignty, security and development interests, and provide a strong guarantee for achieving the national strategic goal of the "two centenaries" and for realizing the Chinese Dream of achieving the great rejuvenation of the Chinese nation.

China's national strategic goal is to complete the building of a moderately prosperous society in all respects by 2021 when the CPC celebrates its centenary; and the building of a modern socialist country that is prosperous, strong, democratic, culturally advanced and harmonious by 2049 when the People's Republic of China (PRC) marks its centenary. It is a Chinese Dream of achieving the great rejuvenation of the Chinese nation. The Chinese Dream is to make the country strong. China's armed forces take their dream of making the military strong as part of the Chinese Dream. Without a strong military, a country can be neither safe nor strong. In the new historical period, aiming at the CPC's goal of building a strong military in the new situation, China's armed forces will unswervingly adhere to the principle of the CPC's absolute leadership, uphold combat effectiveness as the sole and fundamental standard, carry on their glorious traditions, and work to build themselves into a people's military that follows the CPC's commands, can fight and win, and boasts a fine style of work.

China's armed forces mainly shoulder the following strategic tasks:

- To deal with a wide range of emergencies and military threats, and effectively safeguard the sovereignty and security of China's territorial land, air and sea;
- To resolutely safeguard the unification of the motherland;
- To safeguard China's security and interests in new domains;
- To safeguard the security of China's overseas interests;
- To maintain strategic deterrence and carry out nuclear counterattack;
- To participate in regional and international security cooperation and maintain regional and world peace;

- To strengthen efforts in operations against infiltration, separatism and terrorism so as to maintain China's political security and social stability; and
- To perform such tasks as emergency rescue and disaster relief, rights and interests protection, guard duties, and support for national economic and social development.

On July 30th, 2017 during the most recent parade in commemorating the 90th anniversary of PLA founding, Chairman of CMC Xi Jiping also addressed that the PLA is not only to defend the sovereignty and integrity of the country but also to safeguard the development interests. Xi said the PLA has been undertaking a great cause and has arduous tasks, with a bright prospect of development. He called on the Party, the army and the people to unite and move forward, making new contribution to building a strong nation and strong military.

III. The implication of China's military reform

Under the leadership of Chairman Xi Jinping since 2012, China actually has undertaken its in-depth reform in every aspect of the country. However, the military should be playing a leading role in the future open-up and reform.

China started its open-up and reform in late 1978. The starting point was from the countryside. Mr. Deng Xiaoping redistributed the land property from public share to private share in the countryside, which greatly liberated the productivity of the farmers. Later the freedom of many revolutionary veterans including Chairman Xi's father, gave great political support for Deng's reform of the country. Mr. Deng succeeded in his reform.

When President Xi Jinping took the office as the leader of China, he faced a very different country: political transition under its way; economic slowdown; anti-corruption in-depth. In my opinion, military reform will open a new door to President Xi and the country.

1. The military reform will play a leading role in the comprehensive reform of China.
2. The military reform will consolidate the leadership of CPC.
3. The country will have a strong armed force just following the suite of world RMA (revolution in military affairs).
4. The security cooperation with its neighboring countries will be increased
5. China will contribute much more in the framework of UN, including world peacekeeping.

발제 요약문

중국의 군사개혁과 새로운 태세

텅 지옌친 중국 국제문제연구원 미국연구소장

1949년 건국 이래로 중국에서는 적어도 10회의 군사개혁이 있었다. 대부분의 개혁에서 병력과 무기의 감축이 핵심을 차지하였다. 2015년 9월 항일승전 70주년을 기념하는 열병식 기간에 제기된 새로운 군사개혁은 병력 감축뿐만 아니라 인민해방군의 질적 간소화를 표방하고 있다.

Ⅰ. 인민해방군의 새로운 변화

중앙군사위원회 주석으로서 시진핑은 이번 군사개혁은 인민해방군의 간소화와 중국을 위한 새로운 군사정책의 재설립을 목표로 한다고 말하였다. 2년 이상 진행된 인민해방군의 재조정의 결과로 우리는 중국 군대의 다음과 같은 변화를 목격하였다.

1. 지휘 계통

A. 새롭게 중앙집권화된 중앙군사위원회
B. 새로운 5개의 사령부

2. 인민해방군의 4개 군: 육군, 해군, 공군 그리고 로켓 부대

연안 방어와 공해 보호에 대한 전략적 요구에 따라, 인민해방군 해군은 점진적으로 "연안 방어"에 대한 초점을 "연안 방어"와 "공해 보호"의 결합으로 옮기고, 다기능적이고 효율적인 합동 해양전투부대 구조를 설립하였다. 인민해방군 해군은 전략적 억제, 반격, 해양 기동, 연합 해상작전, 포괄적 방어와 지원을 위한 능력을 강화할 것이다.

영공 능력 개발과 공격 및 방어 작전 시행에 대한 전략적 요구에 따라 인민해방군 공군은 영공 방어에서 영공 방어 및 공격으로 초점을 맞출 것이고, 정보화 작전의 요구를 충족시키는 영공 방어 부대를 설립할 것이다. 인민해방군 공군은 전략적 조기경보, 공중 요격, 방공, 미사일 방어, 정보 보호조치, 공군 작전, 전략적 투사와 포괄적 지원을 위한 능력을 향상시킬 것이다.

비용을 절감하면서도 효과적인 핵미사일과 재래식 미사일을 보유한다는 전략적 요구에 따라, 인민해방군 제2포병부대는 정보화의 방향으로 전환할 것이고, 과학기술을 바탕으로 무기와 장비에서 독립적 혁신의 길을 재촉할 것이다. 또한 미사일 시스템의 안전, 신뢰, 효율성을 강화하고, 핵 능력과 재래식 능력이 결합하는 부대구조로 개선할 것이다. 인민해방군 제2포병부대는 전략적 억제와 핵 반격, 그리고 중장거리의 정밀요격 능력을 강화할 것이다.

다양한 기능을 수행하고 사회 안정을 효율적으로 유지한다는 전략적 요구에 따라 중국 인민무장경찰은 경비와 보안, 우발사태 대응, 안정 유지, 대테러 작전, 응급구조, 재난구조, 응급지원, 공중지원을 위한 부대를 지속적으로 발전시킬 것이다. 그리고 경비 업무, 우발사태 대응, 대테러, 안정 유지를 초점을 맞추는 부대구조로 개선할 것이다. 인민무장경찰은 정보화 시대 경비 업무와 우발사태 대응을 중점으로 하는 다양한 임무 수행을 위한 능력을 강화할 것이다.

3. 전략적 지원부대 설립

Ⅱ. 인민해방군의 새로운 임무

강력한 국방능력과 군부대를 개발하는 것은 중국 현대화의 전략적 임무이며, 중국의 평화발전을 위한 안보보장이다. 국가전략 목표의 하위목표인 동시에 국가전략 목표를 뒷받침하는 중국의 군사전략은 군부대의 개발과 사용을 관리하는 매우 중요한 청사진이다. 이 역사적인 출발점에서 중국의 군부대는 국가안보환경에의 새로운 변화에 적응하며, 중국공산당의

목표를 확고하게 따를 것이다. 즉, 새로운 시대에 강한 군사력을 갖추고, 새로운 시대에 적극적 방어에 대한 군사전략적 지침을 시행하며, 국방과 군부대의 현대화를 가속화하여 단호하게 중국의 주권, 안보, 발전 이익을 지킬 것이다. 또한, "두 개의 백 년" 이라는 국가전력적 목표와 중화민족의 재부흥이라는 중국의 꿈(中國夢)을 실현하기 위해 노력할 것이다.

중국의 국가전략 목표는 중국공산당이 창당 100주년을 기념하는 2021년까지 전면적 샤오캉 사회(小康社會, 모든 국민이 물질적으로 풍족한 생활을 누리는 사회)를 건설하고, 중국이 건국 100주년이 되는 2049년까지 부강 · 민주 · 문명 · 조화의 사회주의 현대국가를 건설하는 것이다. 이것은 중화민족의 재부흥을 이루는 중국의 꿈이다. 중국의 꿈은 국가를 부강하게 만드는 것이다. 중국의 군사력은 중국의 꿈의 일부분으로 군대를 강하게 만드는 꿈을 꾸고 있다. 강한 군대 없이는 국가는 안전할 수도 부강할 수도 없다. 새 시대에 강한 군대를 갖추겠다는 중국공산당의 목표를 지향하면서, 중국의 군사력은 중국공산당의 절대적 리더십의 원칙을 확고하게 따르고 전투효율을 확고한 핵심기준으로 확정하며, 영광스런 전통을 이어갈 것이다. 중국공산당의 명령에 따라 싸우고 승리하는 인민의 군대를 세우는 데 노력할 것이다.

중국의 군사력은 주로 다음과 같은 전략적 임무를 담당한다.

- 폭넓은 긴급상황과 군사위협에 대응하고, 중국의 영토, 영공, 영해의 주권과 안보를 보호한다.
- 조국의 통일을 확고하게 보호한다.
- 새로운 영역에서 중국의 안보와 이익을 보호한다.
- 중국의 해외 이익 안보를 보호한다.
- 전략적 억제를 유지하고 핵 반격을 완수한다.
- 지역적, 국제적 안보협력에 참여하고 지역평화와 세계평화를 유지한다.
- 중국의 정치적 안보와 사회 안정을 유지하기 위해서 침투, 분리주의, 테러리즘에 대한 작전을 강화한다.
- 응급구조, 재난구조, 권리와 이익 보호, 경비 임무와 같은 임무를 수행하고, 국가의 경제발전과 사회발전을 지원한다.

2017년 7월 30일 인민해방군 설립 90주년 기념 열병식에서 중앙군사위원회 주석 시진핑은 인민해방군은 국가의 주권과 영토 보존을 방어할 뿐 아니라 개발 이익을 보호한다고 언급하였다. 시진핑은 인민해방군은 대의를 맡아왔고 고된 임무를 수행해왔으며, 밝은 발전 전망을 가지고 있다고 말했다. 그는 강한 국가, 강한 군대를 세우는 데 새로운 기여를 하기 위하여 당, 군대, 그리고 국민이 단결하여 앞으로 나아가자고 요청하였다.

Ⅲ. 중국 군사개혁의 함의

2012년 이래 중국은 시진핑 주석의 지도 하에 국가의 모든 분야에서 심도 있는 개혁을 수행하였다. 그러나 군대는 미래의 개혁개방에서 지도적 역할을 담당해야만 한다.

중국은 1978년에 개혁개방을 실시하였다. 그 출발은 농촌에서 시작되었다. 덩샤오핑은 농촌의 토지재산을 사유재산으로 재분배했고, 이것은 농부들의 생산성을 급격하게 발전시켰다. 이후 시 주석의 부친을 포함하는 많은 혁명원로들이 덩샤오핑의 국가 개혁을 정치적으로 지지하였고, 덩샤오핑은 개혁을 성공할 수 있었다.

시진핑 주석이 중국 지도자로 취임하였을 때, 그는 정치변화, 경기후퇴, 반부패 등 매우 다른 국가 상황에 직면하였다. 개인적 의견으로는 군사개혁은 시 주석과 중국에 새로운 문을 열 것이다.

1. 군사개혁은 중국의 포괄적 개혁에서 지도적 역할을 할 것이다.
2. 군사개혁은 중국공산당의 리더십을 공고히 할 것이다.
3. 중국은 세계 군사업무의 혁명(Revolution in Military Affairs)에 따라 강한 군부대를 보유할 것이다.
4. 주변국가와의 안보협력을 확대할 것이다.
5. 중국은 세계 평화유지를 포함하여 UN 체제에 더 많은 기여를 할 것이다.

Seoul Defense Dialogue 2017

Day 3

Plenary Session 3 본회의 3

08:30-10:00 Grand Ballroom, 1F

"Cyber Security Challenges and Defense Solutions"
사이버 안보 도전과 해법

Key Issues

- Cyber security challenges which each state is facing
- Cyber security posture of each state
- Confidence Building Measures(CBMs) for cyber security based on the characteristics of the region
- Exploration of a model for cyber security cooperation and its application
- Possibility and limit of military measures for cyber security

- 각국이 직면한 사이버 안보 도전
- 국가별 사이버 안보태세
- 지역 특성을 고려한 사이버안보 신뢰구축조치(CBMs)
- 사이버 안보 협력 모델에 대한 탐색과 적용 방안
- 사이버 안보를 위한 군사적 조치 가능성과 한계

Moderator	**Lim Jong-in** Professor, Graduate School of Information Security, Korea University, Republic of Korea
Presenters	**Dean Cheng** Senior Research Fellow, Chinese Political and Military Affairs, Heritage Foundation, USA **Tsuchiya Motohiro** Professor, Graduate School of Media and Governance, Keio University, Japan
Appointed Discussants	**Patryk Pawlak** Brussels Executive Officer, EU Institute for Security Studies, Belgium **Fan Gaoyue** Senior Research Fellow, China Strategic Culture Promotion Association, China
Special Discussant	**Paulus Bekkers** Director, Office of the Secretary General, OSCE

사회자	**임종인** 한국 고려대학교 정보보호대학원 교수
발제자	**딘 청** 미국 헤리티지재단 중국정치군사문제 선임연구원 **츠치야 모토히로** 일본 게이오대 미디어정책대학원 교수
지정 토론자	**패트릭 퍼락** EU 안보연구소 행정관 **판 가오위에** 중국 전략문화촉진회 선임연구원
특별 토론자	**폴 베커스** OSCE 사무국장

Presentation Summary

Dean Cheng
Senior Research Fellow,
Chinese Political and Military Affairs, Heritage Foundation, USA

Diverging American and Chinese Concepts of Deterrence: Implications for Cyber Stability

- The United States and the People's Republic of China (PRC) hold very divergent views of deterrence. The United States and the West tend to view deterrence as primarily focusing on dissuasion. The PRC tends to view deterrence as incorporating both dissuasion and coercion.
- The PRC has also demonstrated a different perspective on crisis stability, as it has exhibited a willingness to engage in direct confrontations with nuclear armed powers. The United States and the Soviet Union tended to avoid such confrontations, for fear that these could lead to escalation.
- During the Cold War, both the United States and the Soviet Union tended to avoid each other's nuclear command, control, and communications (NC3) systems, for fear of raising doubts about its ability to function, and thereby and lowering the nuclear threshold. This included general avoidance of interference with each other's space-based missile early warning systems, which play a central role in crisis stability by providing reliable warning time. This paradigm continues to dominate American thinking.
- China's focus on establishing "information dominance" as a central part of fighting and winning future "informationized wars" places a premium on understanding an adversary's information networks and systems. This includes extensive peacetime reconnoitering of those networks and systems.
- In the Chinese view, such actions may serve to dissuade and coerce an adversary, making them more likely to concede to Chinese political demands. In event of conflict, Chinese military writings suggest that these systems are likely to be among the highest priority targets for the Chinese military, employing electronic warfare, network warfare, and firepower strike methods.
- In addition, given the Chinese investment in short-range, medium-range, as well as intercontinental ballistic missiles, neutralizing adversary development of ballistic missile defenses (BMD) is important. A successful BMD system would jeopardize Chinese tactical and operational as well as strategic capabilities.
- This Chinese approach raises the potential for destabilizing behavior with regards to the United States. Reconnaissance of NC3 networks is liable to be seen as an attempt to interfere with a vital part of strategic operations. Attacks against NC3 networks are similarly likely to reduce the nuclear threshold, especially in wartime, but also in peacetime. This would include cyber intrusions into NC3 networks.
- The PRC and the United States are applying very divergent lessons from their respective nuclear and general histories in pursuit of deterring each other. This is

further exacerbated by the limited experience all nations have in terms of space and cyber deterrence.

- It is in the interests of the United States and the PRC (and other nuclear powers) that trust and confidence-building measures be undertaken in the network warfare/cyber-warfare realm. However, such measures would be very hard to enforce, given difficulties in attribution, detection, and enforcement.
- It may be possible, however, to persuade various states to agree not to engage in actions or reconnaissance of each other's NC3 networks. This would entail, however, a disaggregation of tactical and strategic missile early warning; otherwise, the result would be asymmetrically tilted against Chinese interests.

발제 요약문

미국과 중국의 억제 개념 차이:사이버 안정화에 대한 함의

딘 청 미국 헤리티지재단 중국정치군사문제 선임연구원

- 미국과 중국은 억제에 대한 매우 다른 시각을 가지고 있다. 미국과 서구는 만류(dissuasion)에 초점을 맞추어 억제를 바라보지만, 중국은 억제를 만류와 강제(coercion)의 결합으로 보는 경향이 있다.
- 또한 중국은 핵무장 국가들과 직접적인 대립도 불사할 것이라는 의지를 드러냄으로써 위기 안정에 대해서도 다른 관점을 보이고 있다. 미국과 소련은 그러한 대립이 사태의 악화로 끝날 것이라는 공포 때문에 대립을 피하려는 경향을 보였다.
- 냉전 시기, 미국과 소련은 상대방의 핵 지휘, 통제, 통신 (NC3) 체계를 회피하려고 하였다. 그것의 작동능력에 대한 의구심을 불러일으킬 것이라는 공포가 있었기 때문이다. 그렇게 함으로써 미국과 소련은 핵무기 사용단계를 낮출 수 있었다. 또한, 신뢰할 수 있는 경고시간을 제공함으로써 위기 안정에서 핵심 역할을 하는 상대방의 우주 미사일조기경보 시스템에 대한 간섭도 회피하였다. 이런 패러다임이 미국의 사고를 계속 지배하였다.
- 중국은 "정보우위"를 미래 "정보전쟁"에서의 전투와 승리를 위한 핵심부분으로 설정하였고 이에 따라 경쟁국의 정보 네트워크와 시스템에 대한 이해를 매우 중요하게 여기고 있다. 이것은 정보 네트워크와 시스템에 대한 폭넓은 평시 정찰을 포함하고 있다.
- 중국의 관점에서 보면, 이런 행위는 경쟁국을 만류하고 강제하여, 경쟁국이 중국의 정치적 요구를 허용하도록 하는 것이다. 중국의 군사관련 서적들은 충돌 발생 시 이 시스템들이 중국군의 최우선 목표물이 될 것이며, 전자 전쟁, 네트워크 전쟁, 그리고 화력타격방식을 사용할 것이라고 암시하고 있다.
- 게다가 대륙간탄도미사일과 중국의 중장기 투자를 고려할 때, 경쟁국의 탄도미사일방어(BMD) 개발을 무효화하는 것이 중요하다. 성공적인 BMD 시스템은 중국의 전략적 능력뿐만 아니라 전술과 작전 능력을 위태롭게 할 것이기 때문이다.
- 이런 중국의 접근법은 미국에 대해 불안정을 야기하는 행동을 할 수 있다는 가능성을 제고한다. NC3 네트워크의 정찰은 전략적 작전의 핵심 부분을 간섭하는 시도로 보이기 쉽다. NC3 네트워크에 대한 공격은 전시뿐 아니라 평시에도 핵무기 사용단계를 낮출 것이다. NC3 네트워크로의 사이버 침입이 여기에 포함된다.
- 중국과 미국은 상대방을 억제한다는 목표를 추구함에 있어서 각각의 핵 및 일반 역사로부터 매우 다른 교훈을 배우고 적용하고 있다. 이것은 우주와 사이버 억제 측면에서 모든 국가가 제한된 경험을 가지고 있기 때문에 더욱 악화될 것이다.
- 네트워크 전쟁/사이버전쟁 영역에서 신뢰구축방안에 착수하는 것은 미국과 중국, 그리고 다른 핵무기 보유국가들의 이해관계에 달려 있다. 그러나 권한(attribution), 탐지(detection), 그리고 집행(enforcement)에서의 어려움을 고려할 때, 그러한 방안은 실시되기가 매우 어려울 것이다.
- 그러나 다양한 국가들이 상대방의 NC3 네트워크에 대한 정찰이나 간섭 행위를 하지 않는 것에 동의하도록 설득하는 것은 가능할 것이다. 하지만, 이것은 전술적 미사일 조기경보와 전략적 미사일 조기경보의 분리를 수반할 것이다. 그렇지 않으면 그 결과는 중국의 이익에 반하는 방향으로 불균형하게 나타날 것이다.

Presentation Summary

Tsuchiya Motohiro
Professor, Graduate School of Media and Governance, Keio University, Japan

Japan's Response to Cyber Threats

Most of the "cyber attacks" reported in the mass media are actually better characterized as "cyber crimes," "cyber espionage" or "cyber sabotage." These so-called "cyber attacks" employ what I will refer to as "weapons of mass disturbance" (WMD) rather than real weapons, which cause physical damage. However, we cannot deny the possibility of a real cyber attack in the future, that is, a "cyber operation… [that causes] injury or death to persons or damage or destruction to objects.[1]" In the seven years that have passed since the revelation of the STUXNET attack on Iran's nuclear facility in 2010, it is possible that state and non-state actors may have developed the ability to employ such destructive cyber weapons.

The first shocking cyber operation against the Japanese government occurred in 2000. Some government web sites were taken over and their contents were falsified. This incident occurred right after the government published a policy against cyber terrorism. However, it was regarded as a technical problem, not as a national security one that would directly affect Japanese society and the Japanese economy.

Nowadays, broadly defined cyber attacks (including cyber crimes and cyber espionage) are everyday things in Japan and the world. Not only web falsifications but also the deliberate sabotaging of critical infrastructure, the causing of disorder in financial markets, and the penetration of defense systems constitute possible risks.

The three most serious cyber incidents for Japan in the past several years were Mitsubishi Heavy Industries (MHI) in 2011, Sony Pictures Entertainment (SPE) in 2014 and Japan Pension Service in 2015.

Mitsubishi Heavy Industries (MHI) is the 36th largest defense contractor in the world and its size is around one-fifteenth of Lockheed Martin (the world's largest defense industrial firm). However, MHI is the largest defense firm in Japan.[2] In September 2011, it was reported that eighty-six personal computers and servers at MHI had been compromised. However, MHI was not the first target. Attackers had previously compromised the Society of Japan Aerospace Companies (SJAC), an industry association related to others. This incident impressed upon the Japanese nation that Japan itself was a target of hostile cyber operations; it also strengthened the tendency of private sector companies to hide evidence of having been hacked for fear of damaging their reputations with capital markets.

1 Michael N. Schmitt, ed., The Tallinn Manual on the International Law Applicable to Cyber Warfare, New York: Cambridge University Press, 2013, Rule 30.

2 Defense News, " Top 100 for 2015," Defense News <http://people.defensenews.com/top-100/>, publish date unknown.

In November 2014, Japan watched the developing story of the cyber attacks against Sony Pictures Entertainment (SPE) with great interest and a high degree of shock. While the company is an American firm, the Sony brand has Japanese origins and many Japanese citizens view the hack as if it happened to a Japanese company. The U.S. government pointed the finger at the Democratic People's Republic of Korea (DPRK; North Korea). Since the MHI case, many Japanese companies became sensitized to the possible fallout of cyber attacks, particularly as nation states have begun to target private companies. This rarely happened in the Cold War era, but now seems a defining characteristic of cyber conflict.

In May 2015, the servers of the Japan Pension Service (JPS) were compromised by four different computer viruses and the personal pension information of up to 1.25 million enrollees was leaked. This attack became a major political issue. Media attention has focused largely on the theft of pension records, but this breach may represent only the tip of a more extensive operation. Later investigations by NHK (Nippon Hoso Kyokai), Japan's public broadcasting service, revealed that more than 1,000 organizations were under cyber-attacks at the same time with the JPS. It was a huge operation, much larger than previously thought. At least 20,000 documents and files may have been stolen from the affected government and private organizations.[3]

Even before the SPE incident became public, the Japanese Diet was taking steps to reinforce cyber security. In November 2014 the Diet passed the "Cybersecurity Basic Law[4]" and it became effective in January 2015; in the Japanese system, a basic law sets the country's long-term strategic goals in a certain policy area.

There is an international component of the Cybersecurity Basic Law. Article 23 requires Japan to contribute to international arrangements that improve its cyber security. The SPE incident came at a timely moment to test Japan's new responsibilities.

Based on the Cybersecurity Basic Law, a new Cybersecurity Strategy was finalized on August 20, 2015. The strategy demonstrated Japan's high-level commitment to cyber security and formed the basis of measures to be implemented henceforth at ministries, agencies, and other government organizations.

There is more to cyber security than building sturdy walls and hiding behind them. The value of an interconnected society comes from the free flow of information. There is no such thing as a perfect defense, since black hat hackers will exploit the tiniest holes and cracks in any system of fortifications to infiltrate, steal information, or even carry out attacks.

The first step, as called for in the 2015 cyber security strategy, in guarding against cyber attacks is to develop highly capable human resources to work both in government and the private sector, overcoming sectionalism to share information and promote cooperation both at the individual and organizational levels. Going forward, this will form the core of Japan's approach to cyber security.

3 "NHK Special: CYBER SHOCK" was on air on February 7, 2016.

4 The text in Japanese is available at House of Representatives' web site <http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm>.

발제 요약문

사이버 위협에 대한 일본의 대응

츠치야 모토히로 일본 게이오대학교 미디어정책대학원 교수

언론에서 보도되는 대부분의 "사이버공격"은 실제로 "사이버범죄", "사이버간첩", 또는 "사이버사보타주"의 특징을 가지고 있다. 소위 "사이버공격"은 물리적 피해를 야기하는 실제 무기가 아닌 "대량방해무기(WMD, Weapons of Mass Disturbance)라고 필자는 사용하고 있다. 그러나 미래에 실제 사이버공격의 가능성을 부인할 수 없다. 즉, 실제 사이버공격은 "인체의 상해나 사망, 또는 물건의 손상이나 파괴를 야기하는 사이버작전"이라고 할 수 있다. 2010년 이란 핵시설에 대한 스턱스넷(STUXNET) 공격이 폭로된 이후, 지난 7년 동안 국가나 비국가 행위자는 아마도 이러한 파괴적 사이버무기를 이용할 능력을 발전시켰을 것이다.

일본 정부에 대한 최초의 충격적인 사이버작전은 2000년에 일어났다. 몇몇 정부 웹사이트가 공격을 받고 내용이 조작되었다. 이 사건은 정부가 사이버테러에 대한 정책을 공표한 후 일어난 것이었지만, 일본은 이것을 기술적 문제로 여겼을 뿐 일본 사회나 경제에 직접적으로 영향을 주는 국가안보 문제로 여기지 않았다.

요즘 폭넓게 규정되는 사이버공격은 사이버범죄와 사이버간첩을 포함하며, 일본과 세계에서는 일상적인 것이다. 웹사이트 조작 외에도 중요시설에 대한 의도적 사보타주, 금융시장의 무질서 야기, 국방시스템 침투는 가능성 있는 위험요소가 되고 있다.

과거 몇 년간 일본에 대한 가장 심각한 3개의 사이버사건은 2011년 미츠비시 중공업(NHI) 사건, 2014년 소니 영화사(SPE) 사건, 그리고 2015년 일본연금기구(JPS) 사건이다.

미츠비시 중공업은 세계에서 36번째로 큰 방위산업 도급업체로, 규모가 세계 최대 방위산업회사인 록히드마틴사의 약 1/15에 이른다. 그러나 미츠비시 중공업은 일본 최대의 방위산업 회사이다. 2011년 9월 미츠비시社는 86개의 퍼스널 컴퓨터와 서버의 정보가 유출되었다고 보고하였다. 하지만, 미츠비시社가 최초의 표적은 아니었다. 공격자들은 그전에 일본 항공우주공업회사(SJAC)의 정보를 유출하였다. 이 사건으로 일본은 일본 자신이 적대적 사이버작전의 표적이라는 것을 알게 되었다. 동시에 이 사건은 민간부분 회사가 자본시장의 명성에 해가 될 것을 염려하여 해킹 당한 것을 숨기는 추세를 강화하기도 하였다.

2014년 11월, 일본은 소니 영화사에 대한 사이버공격을 큰 관심 가운데 지켜보았다. 소니 영화사는 미국 회사임에도 불구하고, 소니 브랜드가 일본에서 만들어진 것이었기 때문에, 많은 일본인들이 일본회사가 해킹을 당한 것으로 생각한다. 미국 정부는 배후로 북한을 지목하였다. 미츠비시 중공업 사건 이래로, 일본 현들이 민간회사들을 주목하기 시작하면서, 많은 일본회사들은 사이버공격으로 야기되는 부정적 결과에 민감해졌다. 이것은 냉전시기에는 거의 일어나지 않았지만, 현재는 사이버 충돌의 결정적 특징으로 보인다.

2015년 5월 일본연금기구의 서버가 4개의 다른 컴퓨터 바이러스에 노출되었고, 125만 가입자들의 개인연금정보가 누출되었다. 이 공격은 주요 정치 이슈가 되었다. 언론의 관심은 연금기록 절도에 집중되었지만, 이 사건은 보다 더 대규모 작전에 대한 정보를 나타내는 것이었다. NHK의 조사결과 일본연금기구 사건과 같은 시기에 1,000개 이상의 조직이 사이버공격을 받았다. 이것은 생각보다 거대한 작전이었고, 최소한 2만개의 문건과 파일이 정부 및 민간 조직에서 도난 당했다.

소니 영화사 사건이 알려지기 전, 일본의회는 사이버안보를 강화하는 단계를 진행하였다. 2014년 11월 의회는 "사이버안보 기본법(Cybersecurity Basic Law)"을 통과하였고, 이 법은 2015년 1월에 시행되었다. 일본시스템에서 볼 때, 이 기본법은

국가의 장기적 전략목표이다.

사이버안보 기본법에는 국제적 요소가 있는데, 23조는 일본이 사이버안보를 개선하기 위해서 국제적 협의에 기여하는 것을 요구한다. 소니 영화사 사건은 일본의 새로운 책임을 시험하는 시기 적절한 순간이 되었다.

사이버안보 기본법에 기초하여, 새로운 사이버안보 전략이 2015년 8월 20일에 세워졌다. 이 전략은 사이버안보에 대해서 일본이 가진 높은 수준의 책임을 설명하고, 각 정부조직에서 실행될 기본방식들을 구성하였다.

사이버안보에서는 견고한 벽을 세우고 그 뒤에 숨는 것보다 더 중요한 것이 있다. 상호 연결된 사회의 가치는 정보의 자유로운 흐름에서 나온다. 악질적 해커들이 방어시설의 아주 작은 구멍과 틈을 악용하여 침투하고 정보를 훔치거나 공격을 하기 때문에 완벽한 방어라는 것은 없다.

2015 사이버안보 전략에서 필요로 하는, 사이버공격에 대한 보호의 첫째 단계는 정부와 민간에서 높은 수준의 인력을 양성하고, 개인 및 조직 차원에서 정보를 공유하고 협력을 촉진하기 위해서 파벌주의를 극복하는 것이다. 앞으로 이것이 사이버안보에 대한 일본 대응의 핵심을 형성할 것이다.

Plenary Session 4 본회의 4

10:20-11:50 Grand Ballroom, 1F

"New Forms of Terrorism and Global Coordination in Counter-terrorism"
신종 테러리즘과 대테러 국제공조

Key Issues

- Recent activity trend and influence of violent extremism
- Possible patterns of terrorism in East Asia
- Information sharing measures for the suppression of terrorist activities
- Measures to establish a response system to prevent the proliferation of violent extremism and terrorism
- Ranges of self defense for the prevention of terrorist activities
- 폭력적 극단주의 세력의 최근 활동 추세 및 영향력
- 동아시아에서 발생 가능한 테러 유형
- 테러활동 저지를 위한 정보 공유방안
- 폭력적 극단주의와 테러리즘 확산 방지를 위한 대응체제 구축 방안
- 테러활동 방지를 위한 자위권 행사의 범위

Moderator	**Abdulla Salem Alkaabi** Head, Publications Department, Emirates Center for Strategic Studies and Research, UAE
Presenters	**Nicolas Regaud** Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces, France **Mohd Kamarulnizam Abdullah** Professor, Department of International Affairs, School of International Studies-COLGIS, University Utara, Malaysia
Appointed Discussants	**Juraev Farrukh** Leading Researcher, Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan **Jang Ji-hyang** Senior Research Fellow, ASAN Institute for Policy Studies, Republic of Korea
Special Discussants	**Anthony Lynch** Deputy Secretary of Defence, New Zealand **James H. Mackey** Head of Euro-Atlantic and Global Partnership Section, Political Affairs and Security Policy Division, NATO

사회자	**압둘라 살렘 알카비** UAE 전략문제연구소 공보부장
발제자	**니콜라스 르고** 프랑스 국방부 국제관계전략본부장 인도–태평양 특별대표 **카마룰니잠 압둘라** 말레이시아 우타라 대학교 국제정세학과 교수
지정 토론자	**주레브 파루크** 우즈베키스탄 대통령직속 지역전략연구소 선임연구원 **장지향** 한국 아산정책연구원 선임연구원
특별 토론자	**안토니 린치** 뉴질랜드 정책기획차관보 **제임스 맥키** 나토 유럽–대서양 국제협력과장

Presentation Summary

Nicolas Regaud
Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces, France

Trend Analysis and Prospects of New Forms of Terrorism and International Cooperation in Counter-terrorism

1. Analysis of recent trends

Among the recent trends, it can be noted that apart from the major centres of confrontation with terrorist armed groups, countries victims of terrorism in surrounding countries are facing three forms of terrorist actions which cannot be anticipated or fought in the same way: 1) Terrorist actions organised and directly led by terrorist groups (for example, 13 November 2015 in Paris), generally sophisticated. 2) Terrorist independent actions, in conjunction, sometimes tenuous, with terrorist armed groups abroad (66% of identified attacks). 3) Individual terrorist actions, in particular those inspired by jihadist propaganda online, but unrelated to the terrorist armed groups (26%).

Therefore, in European and North American countries, the threat is widely coming from terrorists acting in their own country and against their compatriots: in the last few years, we have noted that three-quarters of the perpetrators of terrorist attacks have the nationality of the country assaulted.

There is also a growing hybridisation of criminal activities (kidnapping, smuggling) and terrorist activities in many theatres (Sahel, AfPak, Philippines…), which provide funding for terrorist networks. In many cases, terrorist groups take advantage of political, social and economic frustrations at a local level, and inability of the states to resolve it. Terrorists benefit from the support of the local populations, reinforced by the creation of matrimonial and patrimonial links and de facto from a territorial base.

2. Perspectives / future threats

The ineluctable destruction of the proto-state established by IS/Daesh in 2014 will not stop the terrorist threat it embodies. Daesh will go underground, using the Sunni solidarities to blend in with the population of the Levant, and adapt its modes of action, in particular by developing its operations in other theatres.

In Asia, there is concern that many foreign fighters could flee the Iraqi-Syrian theatre or renounce going there in order to join regions that seem to offer them prospects of intensification of fights, particularly in the Philippines. Recent fighting in Mindanao illustrates the internationalisation of this terrorist activism, as numerous fighters from other countries in South-East Asia, South Asia and the Middle-East countries have been identified. The regional impact of this conflict is likely to be substantial and it is very concerning.

Thus, we are witnessing a phenomenum of dissemination of combatant cells where, as Daesh is losing control of its proto-state in the Levant, other action centres are gaining prominence or are likely to change: in East Asia, we can therefore be concerned about upcoming establishment of operational links between terrorist groups acting from Bangladesh to the Philippines, through Thailand, Malaysia, and Indonesia. It is this possible territorial and logistical continuity that needs to be prevented, the same way France and its partners are preventing and combatting links between terrorist cells from Sahel, Libya, and the Levant. To do this, we must have appropriate means to control human and material flows, and naturally, act in a coordinated manner at a regional level.

3. International and regional cooperation

There is no unique or easy solution to combat terrorism that demonstrated its plasticity and its constant adaptation to very different socio-political contexts. We have to be patient and build, at a national, regional and international level, general approaches combining civilian and military responses, as well as political and in terms of development.

It is the approach defended by Europe and France in particular, in supporting the G5 Sahel initiative, a security and development organisation focusing its efforts on borders, connectivity and ungoverned areas, to create a task force of 5 000 soldiers, policemen and civilian able to lead joint and transnational operations to combat terrorism and organised crime. This initiative demonstrates the willingness of concerned countries to respond collectively to common challenges.

In Sahel as in Southeast Asia, the response to the terrorist threat should not be only considered from a security perspective. It should be political, part of a comprehensive response gathering economic development, education and connectivity. The military response to the terrorist threat is crucial but, to have lasting results, it must be accompanied by an action aimed at starving terrorist groups of their sources of funding and to decouple them from civilian populations who indirectly benefit from trafficking in offering them alternatives in terms of development.

Each region has its own characteristics and some recipes which are good in certain circumstances and cases cannot be replicated elsewhere. Nevertheless, we should consider the lessons to be drawn from the Sahelian experience to meet the growing threats in South-East Asia. The Philippines, Indonesia and Malaysia are engaged in strengthening their cooperation, particularly in the Sulu Sea in order to better fight trafficking and criminal activities of groups such as Abu Sayyaf. However, the tragic events of Marawi / Mindanao and the consequences of Daesh's setbacks in the Levant could encourage our friends and partners from East Asia to extend and intensify their cooperation in this field, in a comprehensive way, which is what the G5 Sahel members are doing in Sahelian Africa today.

발제 요약문

신종 테러리즘의 동향분석과 전망, 국제적 대테러 공조

니콜라스 르고 프랑스 국방부 국제관계전략본부장 인도 – 태평양 특별대표

1. 최근 동향 분석

최근 동향을 살펴보면, 테러 무장단체와의 대립이라는 중심점 외에도 테러 피해국가들은 동일한 방식으로는 예측하거나 대응할 수 없는 세 가지 형태의 테러 행위를 직면하고 있다. 1) 테러단체가 직접적으로 조직하거나 주도하는 테러행위(예를 들어, 2015년 11월 13일 파리 테러), 이러한 테러는 대개 복잡하다. 2) 테러리스트의 독립적 행위, 미약하지만 해외 테러 무장단체와 공조한다. 확인된 공격의 66%가 그렇다. 3) 개인의 테러 행위, 특히 온라인 자하디스트 선전에 영감을 얻은 사람들이다. 하지만 이들의 행위는 테러 무장단체와 관계가 없다. 26%가 여기에 해당한다.

그러므로 유럽과 북미 국가에서는 해당 국가에서 활동하거나 자국민들에게 대항하는 테러리스트로부터 폭넓은 위협이 나오고 있다: 우리는 최근 몇 년 간 테러행위 가해자들의 3/4이 공격받은 국가의 국적을 가지고 있다는 점을 주목한다.

또한 사헬, 아프카니스탄–파키스탄, 필리핀 등과 같은 곳에서 납치, 밀수와 같은 범죄행위와 테러행위의 연합이 증가하고 있다. 이것은 테러리스트 네트워크에 자금을 제공한다. 많은 사례에서 볼 수 있듯이, 테러단체는 지역 수준에서 정치적, 사회적, 경제적 좌절과 그러한 문제를 해결하지 못하는 국가의 무능력을 이용하고 있다. 테러리스트들은 지역주민들로부터 지지를 얻고 있으며, 부부 간의 유대와 세습적 유대의 창출로 강화되고 있다.

2. 전망과 미래 위협

2014년 이슬람국가/다에시에 의해서 설립된 원시국가가 파괴되더라도 그것이 상징하는 테러 위협을 멈출 수는 없다. 다에시는 레반트 주민들에 동화되기 위해서 수니파 결속을 이용하여 지하로 숨어들 것이고, 이후 다른 지역으로까지 그들의 작전들을 발전시키면서 행동방식을 조정할 것이다.

아시아에서는 많은 외국 군인들이 이라크–시리아 지역으로의 투입을 포기하고 극화된 전투 가능성이 있는 지역으로 오는 것을 염려한다. 특히 필리핀이 그렇다. 최근 민다나오 전투는 이런 테러행위가 국제화되고 있음을 설명하고 있다, 동남아시아, 남아시아 그리고 중동의 여러 국가에서 온 수많은 군인들이 확인되었으며, 이러한 충돌이 지역에 주는 영향은 상당하다.

그러므로 우리는 다에시가 레반트의 원시국가에서 그들의 통제력을 잃어감에 따라 전투 조직이 확대되고, 다른 행위중심이 우세해지거나 변화되는 것을 보고 있다. 그러므로 우리는 동아시아에서, 즉 방글라데시에서 태국, 말레이시아, 인도네시아를 거쳐 필리핀에 이르기까지 테러단체 사이의 작전이 곧 연계될 것을 걱정하고 있다. 우리는 이것을 방지해야만 한다. 프랑스와 협력국들은 사헬, 리비아 그리고 레반트의 테러단테 간의 연계를 방지하고 싸우고 있다. 이것을 위해서 우리는 반드시 인적, 물적 이동을 통제할 적절한 방법을 가지고 있어야 하며, 또한 지역 차원에서 협력하여 행동해야 한다.

3. 국제적/지역적 공조

테러리즘은 매우 다른 사회정치적 맥락에 대해서 지속적인 적응성과 가소성을 입증하였다. 그래서 이런 테러리즘과 싸우는 특별하거나 쉬운 해결책은 없다. 우리는 정치적 접근법뿐 아니라 국가적, 지역적, 국제적 차원에서 민군이 결합하는 전반적 접근법을 확립해야 한다.

이것은 유럽과 프랑스가 G5 사헬 이니셔티브를 지원하는 데에서 특히 선호하는 접근법이다. 이것은5,000명의 군사, 경찰, 그리고 민간인으로 이루어진 기동부대(Task Force)로서, 국경선과 미 통치지역에 집중하는 안보조직이자 개발조직이다. 이 조직은 테러리즘 및 조직범죄와 싸우는 연합작전이나 초국가적 작전을 주도할 수 있다. 이 이니셔티브는 공동의 도전에 대하여 총괄적으로 대응하는 관심국가의 의지를 보여줄 수 있다.

동남아시아와 같이, 사헬은 테러 위협에 대한 대응법을 안보 관점에서만 고려해서는 안 된다. 대응법은 정치적이면서도 경제발전과 교육, 연계성을 포함하는 종합적인 방식이어야 한다. 테러 위협에 대한 군사 대응은 중요하지만, 지속적인 결과를 위해서는 테러 단체의 자금원을 끊고, 그들을 밀매로부터 간접적인 이익을 얻는 민간인들과 분리시키는 행위가 수반되어야 한다.

각 지역은 각각의 환경에 유리한 그 지역만의 특징과 해결책을 가지고 있으며, 각각의 사건들은 다른 곳에서 동일하게 나타나지 않는다. 그럼에도 불구하고 우리는 동남아시아에서 증가하는 위협에 직면하기 위해서 사헬에서 얻은 교훈을 고려해야 한다. 필리핀, 인도네시아 그리고 말레이시아는 협력 강화에 힘쓰고 있는데, 특히, 아부 사야프(Abu Sayyaf)와 같은 조직의 밀매 및 범죄 행위와 싸우기 위해서 술루해(Sulu Sea)에서의 협력을 강화하고 있다. 그러나 마라위/민다나오의 비극적 사건들이나 레반트 지역에서 다에시의 퇴각이 지연된 결과는 오히려 동아시아의 우리 친구들과 협력국들이 G5 사헬 회원국들이 사헬 아프리카에서 오늘날 하고 있는 종합적 방식으로 이 지역에서의 협력을 확대 및 강화하도록 장려하고 있다.

Presentation Summary

Mohd Kamarulnizam Abdullah

Professor, Department of International Affairs, School of International Studies-COLGIS, University Utara, Malaysia

Managing the Threats of Religious Terrorism: Malaysia's Experiences and Approaches

Threats from religious motivated terror groups create another new challenges to counterterrorism strategies. Despite continuous government's efforts and media exposure to the threats, religious motivated terror groups, such as Daesh or also known as the Islamic State of Iraq and the Levant (ISIL), have been able to successfully attract sympathy and support. Daesh's selection and exclusion of religious texts to justify its jihadi struggle, furthermore have undermined Muslim countries' effort to improve the moderate image of Islam since the September 11 incidents. Terror acts or unlawful uses of force in the name of religion are in fact a worrying development. The phenomenon raises a question of why violent religious extremism has become a norm rather than an exception nowadays. Why these groups resort to terror and violence attacks? There have been myriad arguments explaining the phenomenon. Some experts highlight the global and regional context of the issue yet, some appear to blame it on the international political conspiracy and the new economic order imposed by major powers that pitted against Islam. The major argument of this paper is that the so-called jihadi acts totally deviate from Islam, as a religion of peace.

The paper highlights four inter-related factors that could explain the phenomenal rise of religious terror groups. Those factors include the globalization of information technology and communication especially the rapid expansion of popular social networks; the role of the make-believed sole Muslim leader, the lack of knowledge on Islamic teaching especially on the concept of jihad, and the involvement of young generation. The rapid use of information technology as a vehicle of jihadi propaganda is nothing new. It was used by the al-Qaeda to propagate its ideology in various websites. Yet its successor, Daesh is more innovative in its war strategy and terror methods by taking advantageous of new technology. Its Messianic discourse and marketing strategy reach the masses through various platforms of social media. Aided by an increased use of encryption software developed by internet service providers, Daesh simply modifies all available security programs and applications to their devices in order to conceal their activities from authorities' detection. Another contributing factor in explaining the rising attractiveness of religious terror groups is leadership. Leadership plays an important role spreading the influence of Muslim terror group like Daesh and al-Qaeada. Leaders in these groups have portrayed themselves closed to their followers, polite, knowledgeable, and compassionate. Both leaders possess charisma and charm that could attract ordinary people to join the group. Another factor is the lack of understanding of Islam among the so-called jihadists. The problem lies on the simplistic way of seeking religious answer to the problem. They were rather googling answers from unauthoritative sources

especially in social media such as Facebook, and other applications. This has led to oversimplification of ideas on religious teaching where terror Muslim groups like Daesh has capitalized. Furthermore, religious motivated terror groups tend to glorify their success in the battlefields. The victory and success were then shared to social media application thus attracted admiration among the masses especially the innocent younger generation who are searching for the divine answer for their life.

How to deal with this kind of growing threats of religious motivated terror? Some countries like Malaysia and Singapore, use various preventive measures. Malaysia used to have the Internal Security Act (ISA) as a preventive mechanism in order to suppress organized violence and terror acts but subsequently it has been replaced by the Security Offences (Special Measures) Act or SOSMA 2012. The Malaysian government also introduces the 2015 Preventions for Terror Attacks Act (POTA) to handle the growing terror threats. Another approach is to beef up the intelligent capability. To have an effective counterterrorism, intelligent gathering and sharing are the utmost important. It needs concerted domestic and cross-border cooperation. This has been proved during the Malaysia's counter terrorism campaign against communist threats. The current ability to deter possible religious motivated terror strikes, furthermore, is also credited to the role played by the intelligent community of the security forces. Finally, although laws and enforcement as well as cross-border intelligent gathering may prove to be an effective weapon to counter terror threats, it would not be able to wipe out completely the growing expansion of radical ideas in years to come if the radical ideologies are not neutralized. This is because the current counterterrorism challenge is also dealing with sophisticated ideological debates. Malaysia has offered various de-radicalization program for the detainees. Various counter-narrative and de-radicalization programs have been put in place to debunk those theological arguments put forward by the Muslim-terror groups. The counter-narrative programs are not only meant for the detainees but also targeted for the would-be extremists. The counter-narrative approaches have been channeled not only through traditional medium of information such radio and television, but also through various alternative media platforms, such as twitter, YouTube, Facebook, and WhatsApp. The main targeted group is the youth. Based on the Malaysia's Royal Police data, the youth especially without sound foundation of Islamic understanding has been the easy prey for Daesh recruitment. But critics argue that counter narrative approach would lose its steam if its contents emphasize more on dos and don'ts in Islam. It needs to be attractive in contents and appearance. Therefore, it is suggested that rehabilitation for the so-called jihadist need to be reviewed, adjusted and consolidated. Firstly, having psychological "heart and mind" approaches as being adopted now should continue. Although the syllabus has been heavily emphasis on Islamic jurisprudence and Koranic interpretation and evaluation, the authorities have to ensure that those involve in bringing back ex-jihadi in its correct path are experienced and well respected scholars. In addition, rehabilitation process also needs to go beyond religious dialogues. What if the future terror threats emanate beyond Islamic based groups? Therefore, the rehabilitation process needs to integrate religious and non-religious discourse with the ex-jihadists> the discourse should cover some interesting subjects of international issues, political justice and societal developments. Secondly, in lights with strong democratization process that has swept across the society, government needs to be seen as more caring, transparent and accountable. Public needs to be informed about the detention of members of the terror groups so that it would not be capitalized or manipulated for political mileages by certain individuals or political groups. Furthermore, the post detention program is also important. The government needs to design a concrete post-detention program for former detainees so that they would not fall back to terror activities. Ex-detainees and their family members need financial support in terms of employments and health needs after the release. At the same time, family members and the society need to get involved in the post-detention programs by giving spiritual and moral support for ex-detainees to reintegrate into society.

발제 요약문

종교적 테러리즘에 대한 위협 관리: 말레이시아의 경험과 접근법

카마룰니잠 압둘라 말레이시아 우타라 대학교 국제정세학과 교수

종교적 동기를 가진 테러단체의 위협은 대테러 전략에 새로운 도전을 창출한다. 위협에 대한 지속적인 정부와 언론의 노력에도 불구하고, 다에시(Daesh) 혹은 이라크-레반트 이슬람국가(ISIL)로 알려진 종교적 동기를 가진 테러단체들은 동정과 지원을 성공적으로 끌어들였다. 자하디 투쟁을 정당화하기 위해서 다에시는 경전을 선택하거나 배제하여 9.11 사건 이후 약화된 무슬림 국가들이 이슬람의 중도적 이미지를 개선하는 노력을 하게 하였다. 종교라는 이름 하에 행해지는 테러행위 또는 불법적 폭력 사용은 사실상 걱정스러운 상황이다. 이러한 현상은 현재 왜 폭력적이고 종교적인 극단주의가 예외가 아니라 일상이 되었는가 하는 의문을 낳는다. 어떤 전문가들은 이 문제가 가진 세계적 맥락이나 지역적 맥락을 강조하고, 어떤 전문가들은 이슬람에 대응하는 강대국들에 의한 새로운 경제질서나 국제정치적 음모론의 관점에서 그것을 비난한다. 이 발제문의 주요 논거는 소위 자하디 행위가 평화의 종교라는 이슬람에서 완전히 벗어났다는 것이다.

이 발제문은 종교적 테러단체의 놀라운 발전을 설명할 수 있는 4개의 상호 관련된 요인을 강조한다. 이 요인들은 1) 정보기술과 의사소통의 세계화, 특히 소셜 네트워크의 급속한 확장, 2) 신앙을 위해서 만들어진 무슬림 리더의 역할, 3) 이슬람 교육, 특히 자하디 개념에 대한 지식의 부재, 4) 청년들의 개입이다. 자하디의 선전수단으로서 정보기술의 급속한 사용은 새로운 것이 아니다. 그것은 알 카에다가 여러 웹사이트에 자신의 이데올로기를 선전하는 데에도 사용되었다. 그럼에도 그 계승자인 다에시는 새로운 기술을 이용함으로써 전쟁 전략과 테러 수단에서 더욱 창의적인 모습을 보인다. 그 메시아적 담론과 마케팅 전략은 소셜미디어의 다양한 플랫폼을 통해서 대중들에게 도달한다. 인터넷서비스 제공자들에 의해서 개발된 암호화 소프트웨어의 사용 증가에 힘입어, 다에시는 정부당국이 그들의 행위를 감지하지 못하도록 사용 가능한 모든 보안프로그램과 앱을 활용한다. 종교적 테러단체가 대중을 끌어들이는 다른 요인은 리더십이다. 리더십은 다에시나 알 카에다와 같은 무슬림 테러단체의 영향력을 확대하는 데 매우 중요한 역할을 한다. 이 세력들의 리더들은 추종자들에게 자신이 공손하고 배려심이 많으며 지식적으로 보이도록 하지 않는다. 오히려 리더들은 일반사람들이 세력에 참여하도록 이끄는 카리스마와 매력을 가지고 있다. 다른 요인은 소위 자하디스트 사이에서 이슬람에 대한 이해가 부재하다는 것이다. 이 문제는 어떤 문제에 대한 종교적 해답을 찾는 단순화된 방법에 기인한다. 그들은 오히려 페이스북이나 다른 소셜미디어에서 검증되지 않는 출처로부터 답을 찾는다. 이것은 다에시와 같은 무슬림 테러단체들이 활용하는 종교 교육에서 지나치게 단순화된 생각으로 만들어진다. 게다가 종교적 동기를 가진 테러단체들은 전투에서 그들의 성공을 미화하는 경향이 있다. 승리와 성공은 소셜미디어 앱을 통해서 공유되고, 대중으로부터, 특히 그들의 인생을 위해 신성한 해답을 찾고 있는 순수한 청년들에게 존경을 받는다.

어떻게 종교적 동기를 가진 테러의 위협을 처리할 수 있는가? 말레이시아와 싱가포르 같은 국가들은 다양한 예방책을 사용한다. 말레이시아는 조직폭력과 테러행위를 억제하기 위해서 국내보안법(Internal Security Act)을 예방 메커니즘으로 사용했다. 그러나 결국 그것은 안보범죄 특별조치법(Security Offences Special Measures Act)로 대체되었다. 또한 말레이시아 정부는 증가하는 테러 위협을 다루기 위해서 2015 테러공격 예방법(2015 Preventions for Terror Attacks Act)을 도입하였다. 다른 접근법은 정보역량을 보강하는 것이다. 효과적인 대테러 역량을 보유하기 위해서 정보 수집과 공유는 매우 중요하며, 이것은 국내외 협력이 필요하다. 이것은 공산주의 위협에 대한 말레이시아의 대테러 캠페인 기간에 증명이 되었다. 이외에도 종교적 동기를 가진 테러 공격의 가능성을 감지하는 능력은 보안부대의 정보 커뮤니티의 역할 덕분이다. 결론적으로 국경을 초월한 정보수집, 관련법, 그리고 집행기관이 테러 위협에 대응하는 효과적인 무기이지만, 급진적 이데올로기가 중화되지 않으면 최근 수년 동안 급격하게 확대된 급진적 사상을 완전히 말살시킬 수는 없을 것이다. 이것은 현재 대테러 문제가 복잡한 이데올로기적 논쟁을 처리해야 하기 때문이다. 말레이시아는 억류자들에게 다양한 온건화 프로그램을

제공해 왔다. 다양한 대응논리와 온건화 프로그램은 무슬림 테러단체로부터 받은 신학적 주장들이 허구임을 밝히도록 시행되었다. 이 대응논리 프로그램은 억류자만을 위한 것은 아니라, 잠재적 극단주의자들을 대상으로 하고 있다. 대응논리 접근법은 라디오나 텔레비전 같은 전통적 정보매체를 통해서 송출될 뿐 아니라, 트위터, 유튜브, 페이스북, 왓츠앱 등과 같은 다양한 대안 미디어 플랫폼을 통해서도 송출되고 있다. 주요 대상은 청년들이다. 말레이시아 왕립 경찰 자료에 의하면, 이슬람 이해에 대한 올바른 기초가 없는 청년들이 다에시 신병 모집에 쉽게 속고 있다. 그러나 비평가들은 대응논리 접근법이 이슬람의 행동수칙에 집중된다면, 그 열기가 식을 것이라고 주장한다. 그것은 내용과 외관에서 매력적이어야 한다. 그러므로 소위 자하디스트에 대한 갱생은 검토되고 조정되고 강화될 필요가 있다. 첫째, 현재 채택된 심리적인 "마음과 정신(heart and mind)" 접근법이 지속되어야 한다. 강의 요강이 과도하게 이슬람 법학과 코란 해석과 평가에 집중되어 있음에도 불구하고, 정부당국은 이것이 이전의 자하디를 올바른 길로 회복시키는 것으로 확신해야 한다. 이외에도 갱생과정이 종교적 담화를 넘어설 필요가 있다. 만약에 미래 테러 위협이 이슬람 기반의 단체 외에서 나온다면 어떻게 할 것인가? 그러므로 갱생과정은 종교적이고 비종교적 과정을 통합해야 할 필요가 있다. 그 과정은 국제적 이슈, 정치적 공정성과 사회발전과 같은 흥미로운 주제를 포함해야 한다. 둘째, 사회 전반을 휩쓰는 강력한 민주화와 함께, 정부는 더욱 투명하고 책임 있게 국민을 보살피는 모습을 보일 필요가 있다. 대중들은 테러단체 회원들의 구류에 대해서 알 필요가 있다. 이렇게 되면 어떤 개인이나 단체가 정치적 이득을 위해 관련 사건을 조작하지 못할 것이다. 게다가, 구류 이후의 프로그램도 중요하다. 정부가 출소자를 위해서 구류 이후의 프로그램을 설정한다면, 그들은 테러 행위로 다시 빠지지 않을 것이다. 또한 출소자들과 가족들은 취업과 의료 면에서 재정적 지원이 필요하다. 동시에 가족 구성원들과 사회는 프로그램에서 정신적, 도덕적 지원을 제공하여 그들이 사회로 복귀하도록 도울 수 있을 것이다.

Closing Ceremony 폐회식

12:00-13:00 Grand Ballroom, 1F

Sequence of proceedings 진행 순서

• **Summary Session** 요약 세션

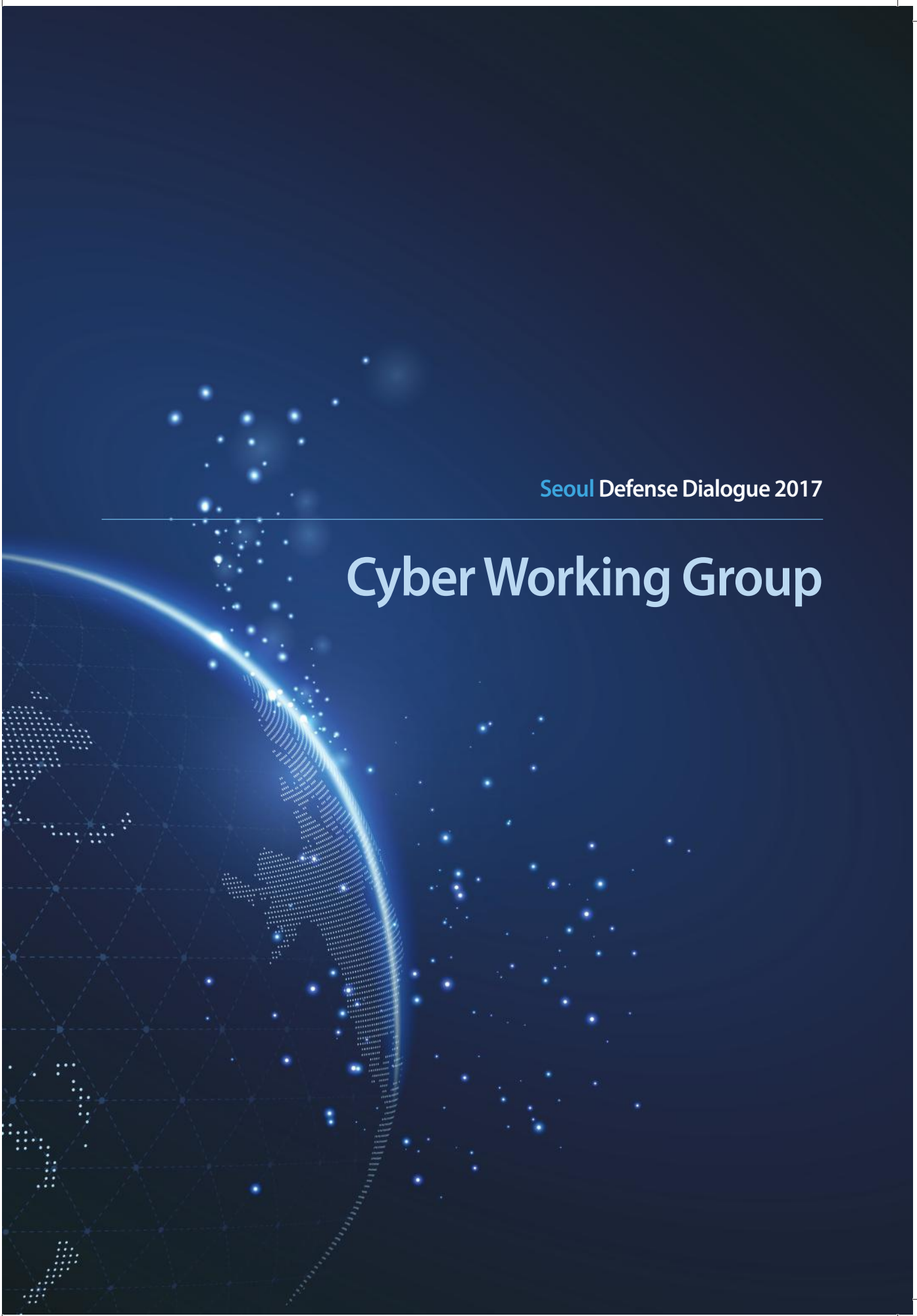
Moderator	**Kim Changsu** Research Fellow Emeritus, Korea Institute for Defense Analyses, Republic of Korea
Session Moderators	Plenary Session 1 **Daniel R. Russel** Diplomat in Residence and Senior Fellow, Asia Society Policy Institute, USA
	Plenary Session 2 **Tim Huxley** Executive Director, the International Institute for Strategic Studies - Asia, Singapore
	Special Session 1 **P. K. Singh** Director, United Service Institution, India
	Special Session 2 **Jean-Pierre Maulny** Deputy Director, French Institute for International and Strategic Affairs, France
	Plenary Session 3 **Lim Jong-in** Professor, Graduate School of Information Security, Korea University, Republic of Korea
	Plenary Session 4 **Abdulla Sallem Alkaabi** Head, Publications Department, Emirates Center for Strategic Studies and Research, UAE

사회자	**김창수** 한국 국방연구원 명예연구위원
세션 사회자	**본회의 1 다니엘 러셀** 미국 아시아사회정책연구소 선임연구원
	본회의 2 팀 헉슬리 영국전략문제연구소 아시아 소장
	특별세션 1 피케이 싱 인도 USI 소장
	특별세션 2 장 피에르 마울니 프랑스 국제전략연구소 부소장
	본회의 3 임종인 한국 고려대학교 정보보호대학원 교수
	본회의 4 압둘라 살렘 알카비 UAE 전략문제연구소 공보부장

• **Closing Remarks** 폐회사

SUH Choo-suk, Vice Minister of National Defense, Republic of Korea
서주석, 대한민국 국방부 차관


Cooperation for Security & Peace
2017
SDD
Seoul
Defense
Dialogue



Seoul Defense Dialogue 2017

Cyber Working Group

Cyber Working Group 사이버워킹그룹

About Cyber Working Group

SDD Cyber Working Group is a multilateral dialogue for director-level defense officials on cyber security. It allows officials to share their opinions and experiences in dealing with cyber security issues, and thus provides an opportunity to build confidence in the process. Since its inception in 2014, with a common recognition on the need for international cooperation in the cyber domain, participating countries shared their respective cyber defense policy, reviewed international law issues pertaining to the cyber domain, and discussed cyberspace workforce management policy.

서울안보대화 사이버워킹그룹은 사이버 분야에 특화된 과장급 실무대화체로서, 사이버 현안에 대한 의견과 경험을 공유하며 신뢰를 구축하는 다자 대화의 장이다. 2014 서울안보대화에서 처음 시작된 이래, 사이버워킹그룹은 사이버 국제협력의 필요성에 대한 공감을 바탕으로 국방 사이버 정책 공유, 사이버 관련 국제법적 이슈 검토, 사이버 인력양성정책 논의 등의 성과를 거두었다.

Overview

DATE September 6.(Wed)-7.(Thu), 2017
2017년 9월 6일(수)–7일(목)

PURPOSE Enhance Cyber Security Capacity and Promote Confidence Building
각국 사이버안보 역량 증대 및 국가간 신뢰관계 증진

PROGRAM

	September 6th (Wed)	September 7th (Thu)
Morning	• Opening • Working Session 1 • Cyber Working Group Luncheon	-
Afternoon	• Attend International Cyber Conference * 2017 ISEC (Seoul COEX)	• Working Session 2 * President Hotel

CyberWG_Working Session 1

9.6.(Wed) 10:20-12:00 / Orchid, 2F

During Working Session 1 on the topic of Civil-Military cooperation based Cybersecurity technology, participants will hear from a discussion panel composed of experts from academia/industry and will be given the opportunity to share their thoughts. Session 1 is composed of three subtopics. First is on the spin-on/off of civil-military Cybersecurity technology; Second is Cybersecurity Challenge and game-like training system; Third is Cybersecurity in the Fourth industrial revolution era. The objective of the session is to have the participants discuss freely with experts from academia/industry and to identify avenues where defense Cybersecurity could be enhanced.

워킹세션 1에서는 '민–군 협력기반 사이버보안기술'에 대한 산 · 학계 전문가 패널의 의견을 듣고, 참석자들의 의견을 공유하는 시간을 마련한다. 주제는 크게 3가지 방향으로 이루어진다. 첫째는 '민–군 사이버보안기술의 'Spin–On/Off', 둘째는 '사이버보안 챌린지 & 게임형 훈련체계', 셋째는 '4차 산업혁명 시대의 Cybersecurity'이다. 산 · 학계 전문가들과 참석자들의 자유로운 논의를 통해 국방영역 사이버안보의 역량을 강화할 수 있는 방안을 모색한다.

Moderator	**Park Hyun Gyu** Professor, Myongji University
Panel	**Lee Won Jong** Professor, Seoul University Graduate School of convergence Science & Technology **Noh Jong Hyuk** Managing Director, LSA, Microsoft **Stephen Dane** General Director, Cybersecurity, Cisco Asia Pacific

진 행	**박현규** 명지대학교 보안경영공학과 교수
패 널	**이원종** 서울대학교 융합과학기술대학원 교수 **노종혁** Microsoft 이사 (법무정책기획 총괄본부) **Stephen Dane** Cisco Asia Pacific 보안분야 총괄

CyberWG_Working Session 2

9.7.(Thu) 14:00-17:00 / Mozart (President Hotel), 31F

During working sesseion 2 on the topic of 'Confidence-Building for transnational Cybersecurity', participants will be put into groups for a discusstion. As cyber threats are uncertain and ambiguous by nature, Confidence-building measures(CBMs) are essential in the effort to minimize state conflict in Cyberspace. Through the group discussions, participants representing 20 or so countries will share their confidence-building policies, exchange vies, and explore ways in which an international system for cooperation could be developed.

워킹세션 2는 '초국가적 사이버안보 신뢰구축' 을 주제로, 참가자들의 그룹토의를 진행한다. 사이버위협은 그 특성상 주체가 모호하고 불확실하여, 사이버공간에서의 신뢰구축조치(CBM)는 국가간 충돌 가능성을 최소화하기 위한 필수적인 요소이다. 20여개국 참석자들의 그룹토의를 통해 신뢰구축을 위한 각국의 정책을 공유하고, 상호 의견을 교환하며 국제협력체계를 발전시킬 수 있는 방안을 모색한다.

Attend International Cyber Conference (2017 ISEC)

9.6.(Wed) 14:00-17:00 / Seoul Coex

Participants will also attend the 2017 ISEC (Information Security Conference) hosted and funded by both the Ministry of Interior(MOI) and the Ministry of Science and ICT(MSIT), being fully mindful of the discussions they had during session 1. The ISEC is the Largest of its kind in Asia, and it provides the participants with an opportunity to get a bird's-eye view of the latest trends in Cybersecurity technology and to witness firsthand the state of private sector cyber technology.

워킹세션1과 연계성을 고려하여, 참석자들은 행정안전부 · 과학기술정보통신부가 주최 · 후원하는 아시아 최대 규모의 국제 사이버시큐리티 컨퍼런스인 2017 ISEC(Information Security Conference)에 참가한다. 사이버시큐리티 분야의 신기술트렌드를 조망할 수 있는 2017 ISEC에 참가하여, 참가자들이 민간의 최신 사이버기술을 직접 확인할 수 있는 기회를 마련한다.

Seoul Defense Dialogue 2017

Participants

Head of Delegate 수석대표

REPUBLIC OF KOREA

SUH Choo-suk

Vice Minister of National Defense, Republic of Korea
대한민국 국방부 차관

AUSTRALIA

Marise Payne

Minister for Defence, Australia
호주 국방부 장관

AZERBAIJAN

Karim Valiyev

Lieutenant General, Deputy Minister of Defense for Personnel-Chief of Main Department for Personnel, Azerbaijan
아제르바이잔 국방 인력차관

CAMBODIA

Vuth Khun

Under-Secretary of State, Cambodia
캄보디아 국방부 차관

CANADA

Jody Thomas

Senior Associate Deputy Minister, Canada
캐나다 국방차관 수석차관보

CHILE

Fernando Danus

Ambassador, Embassy of the Republic of Chile in Korea, Chile
칠레 주한 대사

CZECH REPUBLIC

Tomáš Husák

Ambassador, Embassy of the Czech Republic in Korea, Czech Republic
체코 주한 대사

DENMARK

Carsten Rasmussen

Danish Defense Attaché to China, Denmark
덴마크 주중국방무관

ETHIOPIA

Yohannes Dinkayehu Eba

State Minister for The Financial Management Section, Ministry of National Defense, Ethiopia
에티오피아 국방부 차관

FINLAND

Jukka Matti Juusti

Permanent Secretary (Vice Minister), Finland
핀란드 국방부 차관

FRANCE

Nicolas Regaud

Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, France
프랑스 국방부 국제관계전략본부장 인도–태평양 특별대표

GERMANY

Ralf Brauksiepe

Parliamentary State Secretary, Ministry of National Defence, Germany
독일 국방부 차관

GREECE

Stavroula Pentarvani

Deputy Head of Mission, Embassy of the Greece in Korea, Greece
그리스 주한 공관차석

HUNGARY

Roland Kerekgyarto

Defence Attaché to China, Hungary
헝가리 주중국방무관

INDIA

Jiwesh Nandan

Add'l Secretary, Ministry of Defence, India
인도 국방차관보

INDONESIA

Hadiyan Sumintaatmadja

Secretary General, Ministry of National Defense, Indonesia
인도네시아 국방사무차관

ITALY

Domenico Rossi

Under Secretary of State for Defence, Italy
이탈리아 국방부 차관

JAPAN

Masami Oka

Deputy Director General for the Bureau of Defense Policy, Japan
일본 방위정책차장

LAO PEOPLE'S DEMOCRATIC REPUBLIC

Phayvanh Chanthaphomma

Deputy Director General, Foreign Relation Department, Lao People's Democratic Republic
라오스 대외관계 차장

MALAYSIA

Mohd Sobirin Mohd Yusof

Defense Attache, Embassy of the Malaysia in Korea, Malaysia
말레이시아 주한 국방무관

MEXICO

Alejandro Saavedra Hernandes

Comptroller and General Inspector of the Mexican Army and Air Force. (Inspectory Contralor General del Ejército y Fuerza Aérea), Mexico
멕시코 국방감찰감

MONGOLIA

Dulamdorj Togooch

Vice Minister, Ministry of Defense, Mongolia
몽골 국방부 차관

MYANMAR

Myint Nwe

Deputy Minister, Ministry of Defence, Myanmar
미얀마 국방부 차관

NETHERLANDS

Kim Johanna Christina Cornelia De Jong

First Secretary, Embassy of the Netherlands in Korea, Netherlands
네덜란드 주한대사관 1등 서기관

NEW ZEALAND

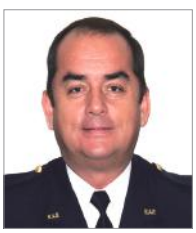
Anthony Lynch

Deputy Secretary of Defence, New Zealand
뉴질랜드 정책기획차관보

NORWAY

Veslemøy Lothe Salvesen

Chargé d'affaires, Embassy of Norway in Korea, Norway
노르웨이 주한 대리대사



PERU

David Martin Gonzalez Leon

Defense & Air Attaché, Embassy of the Republic of Peru in Korea, Peru
페루 주한 국방무관

PHILIPPINES

Cardozo Luna

Undersecretary of National Defense, Philippines
필리핀 국방차관

POLAND

Bartłomiej Grabski

Undersecretary of State, Poland
폴란드 국방차관

RUSSIAN FEDERATION

Iurii Tuchkov

Director, Institute for National Defense Management, and Vice-President, Academy, Russian Federation
러시아 총참모대 부총장

SAUDI ARABIA

Mohammed A. A. Almazid

Assistant Defense Minister, Saudi Arabia
사우디 국방장관 보좌관

SINGAPORE

Aaron Yao Cheng Beng

Director (Policy), Defence Policy Office, Singapore
싱가포르 국방정책과장

THAILAND

Udomdej Sitabutr

Deputy Minister of Defence, Thailand
태국 국방 부장관

TURKEY

Şuay Alpay

Vice Minister of National Defense, Turkey
터키 국방부 차관

UGANDA

Charles Macodwogo Okello Engola

Minister of State for Defence - General Duties, Uganda
우간다 국방국무장관

UNITED ARAB EMIRATES

Mohamed Rashid Bu Afra Al Ali

Assistant Undersecretary for Policy and Strategic Affairs, United Arab Emirates

국방정책전략실장

UNITED KINGDOM

Charles John Hay

Ambassador, British Embassy in Korea, United Kingdom

영국 주한 대사

UNITED STATES OF AMERICA

Thomas W. Bergeson

Deputy Commander, USFK

주한미군 부사령관

UZBEKISTAN

Rustam Khalilov

Commander of Eastern Military District, Uzbekistan

우즈베키스탄 군관구 사령관

VIET NAM

Nguyen Chi Vinh

Deputy Minister of Defense, Viet Nam

베트남 국방차관

EU/EEAS

Clara Ganslandt

Head of Division - Common Security and Defense Policy, EU
대외관계청 공동안보 및 국방정책과장

NATO

James H. Mackey

Head of Euro-Atlantic and Global Partnership Section - Integration, Partnership and Cooperation Directorate - Political Affairs and Security Policy Division, NATO
나토 유럽–대서양 및 국제협력과장

OSCE

Paulus Peter Jozef Bekkers

Director, Office of the Secretary General, OSCE
OSCE 사무국장

Official Experts 정부 전문가

Presenter, Plenary Session 1 | 발제자

Lim Sung-nam 임성남

1st Vice Minister of Foreign Affairs, Republic of Korea
한국 외교부 제1차관

Discussant, Plenary Session 1 | 토론자

SHU Choo-suk 서주석

Vice Minister of National Defense, Republic of Korea
한국 국방부 차관

Discussant, Plenary Session1 | 토론자

Thomas W. Bergeson 토마스 버거슨

Deputy Commander, USFK
주한미군 부사령관

Lieutenant General Thomas W. Bergeson is the Deputy Commander, United Nations Command Korea; Deputy Commander, U.S. Forces Korea; Commander, Air Component Command, South Korea/U.S. Combined Forces Command; and Commander, 7th Air Force, Pacific Air Forces, Osan Air Base, South Korea. He is also the U.S. representative to the joint committee for the Status of Forces agreement between the two countries. General Bergeson was commissioned in 1985 as a graduate of the U.S. Air Force Academy. The general has commanded a fighter squadron, operations group, fighter wing and has held various staff assignments, including positions as Executive Officer to the Commander, Air Combat Command; Chief of Aviation, Strategic Operations, Multi-National Forces Iraq; and Senior Defense Official and Defense Attaché in the United Kingdom. Prior to his current assignment, the general was Director, Legislative Liaison, Office of the Secretary of the Air Force, the Pentagon, Washington, D.C. General Bergeson is a command pilot with more than 3,100 hours in fighter aircraft, including the A-10C, F-15 and F-22.

Civilian Security Experts 민간안보전문가

Plenary Session 1

Moderator | 사회자

Daniel R. Russel 다니엘 러셀

Diplomat in Residence and Senior Fellow, Asia Society Policy Institute, USA
미국 아시아사회정책연구소 선임연구원

Mr. Daniel Russel has served at the Asia Society Policy Institute as Diplomat in Residence and Senior Fellow since April 2017. A career member of the Senior Foreign Service at the U.S. Department of State, he most recently served as the Assistant Secretary of State for East Asian and Pacific Affairs. Prior to his appointment as Assistant Secretary on July 12, 2013, Mr. Russel served at the White House as Special Assistant to the President and National Security Council (NSC) Senior Director for Asian Affairs. During his tenure there, he helped formulate President Obama's strategic rebalance to the Asia Pacific region, including efforts to strengthen alliances, deepen U.S. engagement with multilateral organizations, and expand cooperation with emerging powers in the region.

Special Briefer | 특별 브리퍼

Markus Garlauskas 마커스 갈로스카스

National Intelligence Officer for North Korea, Office of the Director of National Intelligence, Defense Intelligence Agency, USA
미국 국가정보국장실 북한정보담당관

Markus Garlauskas has been the National Intelligence Officer for North Korea on the National Intelligence Council at the Office of the Director of National Intelligence (DNI) of the United States since July 2014. He oversees the production of coordinated US intelligence community strategic analysis on North Korea, while serving as the DNI's senior subject matter expert and analytic advisor on North Korea issues in support of his role as the principal intelligence adviser to the US President. Garlauskas also leads analytic outreach to experts outside the US intelligence community to enhance intelligence analysis on North Korea issues. From 2002 to 2014, Garlauskas served on the staff of United Nations Command, Combined Forces Command and U.S. Forces Korea in Seoul, including as Chief of Intelligence Estimates and Chief of the Strategy Division. In the latter capacity, he served as the principal civilian advisor to three successive commanders on strategic political-military issues, and worked closely with ROK counterparts on strategies for countering North Korean missiles and WMD. For his work in Korea, he received a commendation from the ROK Minister of National Defense and the highest award for a civilian from the US Chairman of the Joint Chiefs of Staff, the Joint Civilian Distinguished Service Award. He holds a Master of Arts in National Security Studies from Georgetown University.

Discussant | 토론자

Jia Qingguo 자 칭궈

Professor, School of International Studies of Peking University, China
중국 북경대학교 국제관계학원 교수

Jia Qingguo is Professor and Associate Dean of the School of International Studies of Peking University. He has taught in University of Vermont, Cornell University, University of California at San Diego, University of Sydney in Australia as well as Peking University. He has published extensively on U.S.-China relations, relations between the Chinese mainland and Taiwan, Chinese foreign policy as well as Chinese politics. He is a member of the editorial board of Journal of Contemporary China (USA), Political Science (New Zealand), International Relations of the Asia-Pacific(Japan) and China Review (Hong Kong). He is also Vice President of the China Association for Asia-Pacific Studies, board member of the China Association of American Studies, and board member of the National Taiwan Studies Association.

Discussant | 토론자

Morimoto Satoshi 모리모토 사토시

Chancellor, Takushoku University, Japan
일본 타쿠쇼쿠대학교 총장

Mr. Satoshi Morimoto currently acts as a Chancellor of Takushoku University. After graduating the National Defense Academy, he joined JSDAF (Japan Self Defense Air Forces), the Japan Defense Agency. In 1977, he was assigned to the National Security Division of the American Bureau at the Ministry of Foreign Affairs (MOFA). After officially joined the MOFA in 1979, he was consistently put in charge of national security practices including the posts of the First Secretary of the Japanese Embassy in the United States and the head of the National Security Policy Division of the MOFA Information Research Bureau. He was assigned to the Minister of Defense under DPJ (Democratic Party Japan) administration in 2012. He also served Special Adviser to the Minister of Defense (2015-2016). He specialized in national security arms control, national defense and international politics.

Discussant | 토론자

Alexander I. Nikitin 알렉산더 니키틴

Director, Center for Euro-Atlantic Security, MGIMO, Russia
러시아 국제관계대학 유럽 – 아틀란틱 안보센터장

Prof. Alexander I. Nikitin is a professor in the Moscow State Institute of International Relations and a Director of the Center for Euro-Atlantic Security at MGIMO. He is also an Elected member of the Russian Academy of Military Sciences. From 2004 to 2008, he served a President of the Russian Political Science Association. Since 2008, he has been an elected President Emeritus of the Association and Chair of the RPSA International Cooperation Council. From 2005 to 2012, Prof. Nikitin served an official external expert of the United Nations, nominated by the UN High Commissioner on Human Rights and a Member of Scientific Council of the Security Council of Russia. He organized more than 50 international scientific and academic conferences and workshops in Russia and abroad.

Plenary Session 2

Moderator | 사회자

Tim Huxley 팀 헉슬리

Executive Director, the International Institute for Strategic Studies - Asia, Singapore
영국전략문제연구소 아시아 소장

Dr. Tim Huxley is the Executive Director of the International Institute for Strategic Studies (IISS)-Asia. He has worked for many years in the overlap between strategic studies and Asian area studies, his research focusing particularly on Southeast Asian states' security and defence policies. He has also followed domestic political developments throughout Southeast Asia closely since the 1980s. His PhD is from the Australian National University, he has held research and teaching positions in British and Australian universities, and he was a resident Fellow at the Institute of Southeast Asian Studies in Singapore from 1985-7. Before joining the senior staff of the IISS in 2003, he was Reader in South-East Asian Politics and Director of the Centre for South-East Asian Studies at the University of Hull. As an Executive Director of IISS-Asia, Dr. Huxley has subsequently taken a leading role in organising the annual IISS Shangri-La Dialogue defence ministers' meeting and, since 2012, the IISS Fullerton Lecture series.

Presenter | 발제자

Hong Nong 홍 농

Executive Director, Institute for China-America Studies, China
중국 중미연구소장

Dr. Nong Hong is the Executive Director and Senior Fellow of Institute for China– America Studies. She holds a PhD of interdisciplinary study of international law and international relations from the University of Alberta, Canada and held a Postdoctoral Fellowship in the University's China Institute. She was ITLOS-Nippon Fellow for International Dispute Settlement (2008-2009), and Visiting Fellow at the Center of Oceans Law and Policy, University of Virginia (2009) and at the Max Planck Institute for Comparative Public Law and International Law (2007). She is concurrently a research fellow with the National Institute for South China Sea Studies, China, and China Institute, University of Alberta, Canada. Her research takes an interdisciplinary approach to examining international relations and international law, with focus on International Relations and Comparative Politics in general; ocean governance in East Asia; law of the sea; international security, particularly non-traditional security; and international dispute settlement and conflict resolution.

Presenter | 발제자

Renato Cruz De Castro 레나토 크루즈 데 카스트로

Professor, International Studies Department, De La Salle University, Philippines
필리핀 델 라 살레 대학 국제학부 교수

Prof. Renato Cruz De Castro is a full professor in the International Studies Department, De La Salle University, Manila, and holds the Charles Lui Chi Keung Professorial Chair in China Studies. He was a visiting research fellow in the Japan Institute of International Affairs (JIIA) from June to August 2017. From September to December 2016, he was based in East-West Center in Washington D.C. as the U.S.-ASEAN Fulbright Initiative Researcher from the Philippines. He is an alumnus of the Daniel Inouye Asia-Pacific Center for Security Studies in Hawaii, U.S.A. In 2009, Dr. De Castro became the U.S. State Department ASEAN Research Fellow from the Philippines and was based in the Political Science Department of Arizona State University. Prof. He is also a member of the Board of Trustees of the Albert Del Rosario Institute for Strategic and International Studies (ADR Institute), and was a consultant in the National Security Council of the Philippines during the Aquino Administration. Prof. De Castro's research interests include Philippine-U.S. security relations, Philippine defense and foreign policies, U.S. defense and foreign policies in East Asia, and the international politics of East Asia.

Appointed Discussant | 지정토론자

Kaneda Hideaki 카네다 히데아키

Director, Okazaki Institute, Japan
일본 오카자키연구소장

Vice Admiral Hideaki Kaneda, JMSDF (Japan Maritime Self Defense Force) (ret.) is the Director and Special Research Advisor of The Okazaki Institute, an Adjunct Fellow of the Japan Institute of International Affairs. He was a Senior Fellow of Asia Center and J. F. Kennedy School of Government of the Harvard for last two years. He became a Guest Professor of Faculty of Policy Management of Keio University for last two and a half years. Admiral Kaneda is a graduate of the National Defense Academy in 1968, the Maritime Staff College in 1983, and the U.S. Naval War College in 1988. He served in the JMSDF from 1968 to 1999, primarily in Naval Surface Warfare at sea, while in Naval & Joint Plans and Policy Making on shore.

Appointed Discussant | 지정토론자

Lee Seo-hang 이서항

President, Korea Institute for Maritime Strategy, Republic of Korea
한국 해양전략연구소장

Dr. Seo-Hang Lee is President of the Korea Institute for Maritime Strategy and Professor Emeritus at Korea National Diplomatic Academy. He is also Vice President of UNA-ROK. Before he was appointed to the current position, Dr. Lee was Consul-General to Mumbai, India. He was also a professor at the Institute of Foreign Affairs and National Security (IFANS), the policy research arm of the Ministry of Foreign Affairs and Trade. He joined IFANS in 1989 and served as Dean of Research from 2004 to 2008. Dr. Lee was also Co-Chairman of the Korean Committee of the Council for Security Cooperation in the Asia Pacific (CSCAP). He also served as Chairman of the SLOC Study Group-Korea, a scholarly organization composed of professors, government and naval officers, and other experts on maritime affairs. Dr. Lee received a Ph.D. from Kent State University and a B.A. and M.A. from Seoul National University. He is the recipient of the Killam Post-Doctoral Fellowship, Dalhousie Law School, Canada. Dr. Lee has published or edited more than 80 monographs and books on international security issues and maritime affairs.

Plenary Session 3

Moderator | 사회자

Lim Jong-in 임종인

Professor, Graduate School of Information Security, Korea University, Republic of Korea
한국 고려대학교 정보보호대학원 교수

Prof. Jong-in Lim is the representative expert in Cyber Security in Korea. He served as a special advisor to the president for national security in 2015. As the pioneer of information security in Korea, he started the field as a Cryptography expert, and now he is working as a cyber security policy expert. Currently he is a professor of the Graduate School of Information Security at Korea University, and participating many advisory works for the Korean government. He is working as a chairman of the Digital Forensic Advisory Committee under Supreme Prosecutor's Office, and a chairman of the Expert Group in Financial Security Agency. Also, he was a former President of the Korea Institute of Information Security and Cryptography, and a member of the Personal Information Protection Commission under direct jurisdiction of the President. On the first 'Day of Information Security' in 2012, Korea government awarded him the Order of Merit by the President, for his contribution to the Information Security Field in Korea.

Presenter | 발제자

Dean Cheng 딘 청

Senior Research Fellow, Chinese Political and Military Affairs, Heritage Foundation, USA
미국 헤리티지재단 중국정치군사문제 선임연구원

Dr. Dean Cheng is the Senior Research Fellow for Chinese Political and Military Affairs at the Heritage Foundation, after working at the Center for Naval Analysis, SAIC, and the US Congress Office of Technology Assessment. He is a long-time observer of China's military, with a particular interest in China's space program and Chinese military doctrine. He has testified before Congress, and spoken at various institutions, including MIT and the US National Defense University. He is the author of Cyber Dragon: Inside China's Information Warfare and Cyber Operations from Praeger Publishing (2016).

Presenter | 발제자

Tsuchiya Motohiro 츠치야 모토히로

Professor, Graduate School of Media and Governance, Keio University, Japan
일본 게이오대학교 미디어정책대학원 교수

Prof. Motohiro Tsuchiya is a professor of Graduate School of Media and Governance at Keio University in Japan and Deputy Director at Keio Global Research Institute (KGRI). Prior to joining the Keio faculty, he was associate professor at Center for Global Communications (GLOCOM), International University of Japan. He is a visiting scholar at the Institute for International Socio-Economic Studies (IISE) and was a visiting scholar at University of Maryland, George Washington University, Massachusetts Institute of Technology and East-West Center. He is interested in the impact of the information revolution on international relations; regulations regarding telecommunications and the Internet; global governance and information technologies; and cyber security. He earned his BA in political science, MA in international relations, and Ph.D. in media and governance from Keio University.

Appointed Discussant | 지정토론자

Patryk Pawlak 패트릭 퍼락

Brussels Executive Officer, EU Institute for Security Studies, Belgium
EU 안보연구소 행정관

Dr Patryk Pawlak is Brussels Executive Officer at the EU Institute for Security Studies (EUISS). In this capacity, he is responsible for inter-institutional relations and coordination of cybersecurity projects. With over ten years of experience in research and policy support projects, he currently manages a team working on a 'Cyber Capacity Building Toolkit' for the European Commission. Patryk's work on cybersecurity capacity building and cyber diplomacy has appeared in several peer-reviewed journals and edited volumes. He is the editor and author of the EUISS report "Riding the digital wave", which analyses the impact of cyber capacity building on human development. Since June 2016, he is a member of the Advisory Board of the Global Forum on Cyber Expertise. Patryk holds a PhD in Political Science from the European University Institute in Florence.

Appointed Discussant | 지정토론자

Fan Gaoyue 판 가오위에

Senior Research Fellow, China Strategic Culture Promotion Association, China
중국 전략문화촉진회 선임연구원

Gaoyue FAN, retired senior colonel, is now a senior research fellow and project director at the China Strategic Culture Promotion Association and a guest professor at the Collaborative Innovation Center for Security and Development of Western Frontier China, Sichuan University. He used to be a research fellow, deputy director, director and chief specialist at the PLA Academy of Military Science (AMS) in Beijing. His research interests include US military affairs, international security and cooperation, international arms control and disarmament. He studied at Jilin University and the Southwest China Normal University where an MA in British and American English Language and Literature was conferred on him. He was trained at PLA National Defense University for a year, and studied as a visiting scholar at the University of Pennsylvania for a year and as a residence WDS-Handa Fellow at the Pacific Forum CSIS for half a year. He had served as an infantry man, staff officer and English instructor before he came to AMS. He has published two dozens of books, such as Iraq War: the First War That Is Characterized by Information Age, Joint Operations and Joint Training of the US Armed Forces, The US Special Forces, about 50 study reports and 230 articles.

Plenary Session 4

Moderator | 사회자

Abdulla Salem Alkaabi 압둘라 살렘 알카비

Head, Publications Department, Emirates Center for Strategic Studies and Research, UAE
UAE 전략문제연구소 공보부장

Mr. Abdulla Salem Alkaabi currently holds the position of Head of the Publications Department, the Emirates Center for Strategic Studies and Research (ECSSR), Abu Dhabi. Prior to that, he served as Deputy Director General for Scientific Research Affairs, Head of the Library Department, Head of the Department of the Director General's Office, Head of the Recruitment Section and Head of the Monitoring Section at the Media Department. Mr. Alkaabi represented the ECSSR on the Executive Team for the National Identity Index, which was affiliated with the UAE Prime Minister's Office. He also represented the ECSSR as a member of the Consultative Academic Council for Zayed University, UAE. In addition, he participated in many conferences, forums and workshops in the UAE, the Arab region and the rest of the world. He is a specialized writer in international affairs, particularly concerning the Arabian Gulf and Middle East regions.

Presenter | 발제자

Nicolas Regaud 니콜라스 르고

Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces, France
프랑스 국방부 국제관계전략본부장 인도 – 태평양 특별대표

Dr. Nicolas Reguad serves as Special Representative to the Indo-Pacific of the Directorate General for International Relations and Strategy, French Ministry of Armed Forces. He was Assistant Defence Policy Director since September 2008. He was also an advisor for Asia-Pacific at the Policy planning staff of the ministry of foreign affairs and senior research fellow at the Centre for International Relations & Strategy of the University Paris I Panthéon-Sorbonne (1989-1992), Head of the Asia desk at the Directorate for Strategic Affairs of the Ministry of Defence (1992-1993), Attaché for defence equipment at the French Embassy in Tokyo (1994-1996), a visiting research fellow at the Japan Institute for International Affairs in Tokyo (1996-1997), and Assistant to the deputy director in charge of regional affairs at the Directorate for Strategic Affairs of the MoD (1997-2000). Dr. Reguad was deputy director in charge of strategic export control and international crisis and conflicts at the General Secretariat of National Defence (SGDN). Dr. Regaud was a fellow of the 57th session of the Institut des Hautes Etudes de Défense Nationale in 2004-2005.

Presenter | 발제자

Mohd Kamarulnizam Abdullah 카마룰니잠 압둘라

Professor, Department of International Affairs, School of International Studies-COLGIS, University Utara, Malaysia

말레이시아 우타라 대학 국제정세학과 교수

Dr. Kamarulnizam Abdullah is a Professor in National Security at the Department of International Affairs, School of International Studies-COLGIS, Universiti Utara Malaysia. His main research areas are on political violence, religious militancy, and national security issues that pertinent to Malaysia and the Southeast Asia region. Currently, he is a panel consultant to the Japan's Ministry of Foreign Affairs on Southeast Asian's Religious Moderation Program (2016-2019), and Timor Leste's Institute of Diplomatic Studies on the Academic Training Program for the Diplomats (2015-2018). He is also an expert panel member for the National Formulation of Homeland Security, Ministry of Home Affairs Malaysia committee (203-2015); and for the Revision of the National Defence Policy, Ministry of Defence, Malaysia (2016); member of the Malaysia's Council for Security Cooperation Asia-Pacific, (CSCAP) (since 2013); expert panel for the Washington-based Council for Asian Terrorism Research (2008-2011); Executive Committee for the Malaysia's Professorial Council for Politics, Security and International Affairs (since 2012).

Appointed Discussant | 지정토론자

Juraev Farrukh 주레브 파루크

Leading Researcher, Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan

우즈베키스탄 대통령직속 지역전략연구소 선임연구원

Mr. Farrukh Juraev is leading researcher at Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan. He has experience in law enforcement bodies. He is a graduate of Tashkent State University of Law. He has a master's degree in the field of system analysis. He is an expert on digital diplomacy, digital economy, information security, domestic and foreign policy issues of the state. He is the author of a number of scientific publications on such topics as the phenomenon of digital diplomacy in the international relations, importance of analytical activity in the system of international relations, the role of the Mahalla institution in strengthening the social and economic prosperity of the country's population and interethnic harmony and much more, published in Uzbekistan and foreign countries.

Appointed Discussant | 지정토론자

Jang Ji-hyang 장지향

Senior Research Fellow, ASAN Institute for Policy Studies, Republic of Korea
한국 아산정책연구원 선임연구원

Dr. Ji-hyang Jang is a senior fellow in the Middle East and North Africa (MENA) Program at the ASAN Institute for Policy Studies. Dr. Jang also serves as a policy advisor on Middle East issues to South Korea's Ministry of Foreign Affairs. Previously, Dr. Jang taught comparative and Middle East politics at Seoul National University, Yonsei University, Ewha Woman's University, and the Hankuk University of Foreign Studies. Her research interests include political Islam, Islamic finance, comparative democratization, terrorism, and state-building. Dr. Jang is the author of numerous books and articles, including The Arab Spring: Will It Lead to Democratic Transitions? (with Clement M. Henry (eds.), Palgrave Macmillan 2013) and a Korean translation of Fawaz Gerges' Journey of the Jihadist: Inside Muslim Militancy (Asan Institute 2011). Dr. Jang received a B.A. and M.A. from the Hankuk University of Foreign Studies and her Ph.D. in political science from the University of Texas at Austin.

Special Session 1

Moderator | 사회자

P.K. Singh 피케이 싱

Director, United Service Institution, India
인도 USI 소장

LT GEN (ret.) P. K. Singh has served the Director of the United Service Institute (USI) of India since January 2009. He was commissioned as a 2/LT in the Indian Army in 1967 and retired as C-in-C (Army Commander) in 2008. He is a member of the Governing Council of the Indian Council of World Affairs and member of the International Advisory Board of the RUSI International, London. He commanded a Brigade in Nagaland/Manipur, an Infantry Division (RAPID)' during Op Parakram, a Corps in Punjab and the South Western Command. He took over as Director of the United Service Institution of India in January 2009. He is a member of the Governing Council of the Indian Council of World Affairs, New Delhi, and also member of the International Advisory Board of the RUSI International, London.

Presenter | 발제자

John Louth 존 루스

Director, Defence, Industries and Society, Royal United Services Institute for Defence and Security Studies, UK
영국 왕립합동국방안보연구소 국방산업사회연구소장

Prof. John Louth is a senior research fellow and director for defence, industries and society at the Royal United Services Institute for Defence and Security Studies. He served as an officer in the Royal Air Force for sixteen years before working as a consultant and programme director extensively throughout the defence and energy sectors. Prof. Louth has also worked as a senior adviser to the European Defence Agency on the development of pan-European procurement policies and practices. He supervises PhD students at the University of Roehampton Business School in London. He is also a specialist adviser to the House of Commons Defence Select Committee and a senior defence and security business adviser to Avascent. He sits on the European working group looking at defence capabilities, technologies and budgeting across the member-states of the European Union.

Presenter | 발제자

Maxim Shepovalenko 막심 셰포바런코

Deputy Director, Centre for Analysis of Strategies and Technologies, Russia
러시아 전략기술분석센터 부소장

Mr. Maxim Shepovalenko is the deputy director of the Centre for Analysis of Strategies and Technologies (CAST) since 2015. He is a former Russian Navy officer, Captain 2nd Rank / Commander (Ret.). He served with the Northern Fleet, and thereafter, with the Main Naval Staff. After retirement, he majored in the finance industry. He also worked for the Rosoboronexport, the Russian state agency for export of defence technology solutions. His principal areas of interest are (i) defence procurement, (ii) sensors, weapons and munitions, (iii) strategic mobility assets, and (iv) medium- and low-intensity conflicts. He edited 'The Syrian Objective' ('Syriysky Rubezh' in Russian, 2016) study by CAST, as well as contributed to a number of other CAST monographs.

Appointed Discussant | 지정토론자

Reifqi Muna 레이프키 무나

Researcher, Center for Political Studies, Indonesian Institute of Sciences, Indonesia
인도네시아 과학원 정치학센터 연구원

Dr. Riefqi Muna is a researcher at Centre for Political Studies, Indonesian Institute of Sciences (LIPI) Jakarta. He is currently a member of National Working Committee on Indian Ocean Rim Academic Group of Indonesia. He was also a National Security Vising Fellow at National Security College, Australian National University and a National Security Vising Fellow (NSVF) at National Security College, Australian National University. His area of interest is security policy and defence studies. He obtained his PhD from Faculty of Defence and Security, Royal Military College of Science (RMCS), Cranfield University, UK Defence Academy, Shrivenham (2009), and Master in Defence Studies (MDefStu) from Australian Defence Force Academy (ADFA) UNSW, Canberra (1995).

Appointed Discussant | 지정토론자

Shim Hyun-chul 심현철

Professor, Department of Aerospace Engineering, Korea Advanced Institute of Science and Technology, Republic of Korea
한국 과학기술원 항공우주공학과 교수

Prof. David Hyun-chul Shim is an Associate Professor at KAIST, Korea. From 1993 to 1994, he was with Hyundai Motor Company, Korea. From 2001 to 2005, he was with Maxtor Corporation in USA as Staff Engineer. From 2005 to 2007, he was with University of California Berkeley as Principal Engineer. In 2007, he joined the Department of Aerospace Engineering, KAIST, Daejon, Korea, as an Assistant Professor and now he is a tenured Associate Professor. He served as Director of Center of Field Robotics in KAIST Institute from 2012-2015. From 2013, he has led the project planning for nation-wide UAV deployment with Korean government. He is now Director of Civil RPAS Research Center funded by Korea Ministry of Land, Infrastructure and Transportation and also Director of Intelligent UAV Laboratory funded by ADD. He is serving as an advisor for Remotely Piloted Aircraft System Panel in International Civil Aviation Organization (ICAO) since 2015. He is also serving as a Global Future Council specialized in AI & Robotics group of Economic Forum since 2016.

Special Session 2

Moderator | 사회자

Jean-Pierre Maulny 장 피에르 마울니

Deputy Director, French Institute for International and Strategic Affairs, France
프랑스 국제전략연구소 부소장

Dr. Jean-Pierre Maulny is the deputy director at the French Institute for International and Strategic Affairs (IRIS). He holds a Master's degree in Defence Studies and a Master's degree in public law, and was a member of the 31th session of the Centre des Hautes Etudes de l'Armement (CHEAr). Between 1997 and 2002, he was advisor to the chairman of the French National Assembly's Defence and Armed Forces Committee. At IRIS, Jean-Pierre Maulny is in charge of matters related to defence policy, CSDP and NATO, arms industry and arms sales. He has published extensively on the subject. He is the author of « La guerre en réseau au XXIe siècle : Internet sur les champs de bataille » a book dedicated to the US network Centric Warfare doctrine. He consults for the French ministry of defence, the European commission and the European Defence Agency on defence matters.

Presenter | 발제자

Margaret E. Kosal 마가레트 코살

Professor, Sam Nunn School of International Affairs, Georgia Institute of Technology, USA
미국 조지아공과대학교 샘 넌 국제대학원 교수

Dr. Margaret E. Kosal is a Professor in the Sam Nunn School of International Affairs at Georgia Institute of Technology. She was recently appointed faculty in the Parker H. Petit Institute for Bioengineering and Bioscience at Georgia Tech. Her research explores the relationships among technology, strategy, and governance. She is also the co-founder of a sensor company, where she led research and development for real-world applications. Previously, Kosal has served as a Senior Advisor to the Chief of Staff of the U.S. Army and as Science and Technology Advisor within the U.S. Office of the Secretary of Defense (OSD), in addition to other consulting. She is the recipient of multiple awards including the Office of the Secretary of Defense Award for Excellence, 2015 CETL/BP Faculty Teaching Excellence Award; and the 2012 Ivan Allen Jr Legacy Award. Recently, she was appointed Editor-in-Chief of the journal, Politics and the Life Sciences.

Presenter | 발제자

Teng Jianqun 텅 지옌췬

Director, Department for American Studies, China Institute of International Studies, China
중국 국제문제연구원 미국연구소장

Dr. Jianqun Teng is the Director of the Department for American Studies and a senior research fellow at China Institute of International Studies (CIIS). He has worked at CIIS since he was discharged from active military service in September 2004. Dr. Teng served in the PLA for 25 years, first in the Navy (1979-1992) and later in the Academy of Military Science (1992-2004). He was the editor-in-chief of the Academy of Military Science journal World Military Review and also an assistant research fellow there. Dr. Teng has published several dozens of articles on the issues of arms control, disarmament, and nonproliferation, in addition to authoring several reports and books. Dr. Teng received his BA in English language and literature from PLA Naval Communication College in 1983, his MA in military science from PLA Academy of Military Science in 1995, his MA in South Asian area studies from School of Oriental and African Studies (SOAS), London University in 1999, and his PhD degree in international relations from Peking University in 2006.

Discussant | 토론자

Tran Viet Thai 트란 비엣 타이

Deputy Director-General, Institute for Foreign Strategic Studies, Diplomatic Academy of Vietnam, Vietnam
베트남 국립외교원 외교전략연구소 부소장

Dr. Tran Viet Thai is currently the Deputy Director-General and Director of the Center for Regional and Foreign Policy Studies, Institute for Foreign Policy and Strategic Studies, Diplomatic Academy of Vietnam (DAV). He finished his Ph.D in International Relations at DAV and got his Master of Public Policy (MPP) at the National Graduate Institute for Policy Studies (GRIPS), Tokyo, Japan. He used to serve as secretary to the Foreign Minister of Vietnam, a China specialist at the Foreign Policy Planning Department, Ministry of Foreign Affairs of Vietnam and had two postings in China (Beijing and Guangzhou) before working as a researcher at DAV since 2011. At present, he is also a regular commentator on international issues on the national television system of Vietnam.

Discussant | 토론자

No Hoon 노 훈

President, Korea Institute for Defense Analyses, Republic of Korea
한국 국방연구원장

Dr. Hoon No is currently a president research fellow at the Korea Institute for Defense Analyses (KIDA). He Joined the KIDA in 1982, served as the Director of the Division of Force Development Studies, the Director of the Office of the Planning and Coordination and the Vice President. of the KIDA. He was on leave of absence from the KIDA for his governmental service Ministry of National Defense as a Senior Policy Advisor to Defense Minister from 2006 to 2007. Dr. No holds various advisory posts, including Blue House, Ministry of National Defense, Ministry of Security and Public Administration and etc. He has published books and articles on Defense Policies, Military Strategy, Force Planning and Defense Reform. He received his B.S. and M.S. from the Seoul National University. He holds a Doctor of Management Science from the University of Iowa in 1990.

Closing Ceremony

Moderator | 사회자

Kim Changsu 김창수

Research Fellow Emeritus, Korea Institute for Defense Analyses, Republic of Korea
한국 국방연구원 명예연구위원

Changsu KIM is currently a Research Fellow Emeritus of the Korea Institute for Defense Analyses (KIDA) in Seoul, Korea. Since he joined the Institute in 1985, Dr. Kim has served on such posts as Chief of Japan Studies Division, Chief of Regional Military Affairs Division, Chief of US Studies Division, Chief of International Conflict Studies Division, and Director of the Center for Security and Strategy. Also, he has been involved in many international security and defense forums, including the Shangri-La Dialogue, the Xiangshan Dialogue, and the Seoul Defense Dialogue (SDD), an annual track 1.5 dialogue hosted by the ROK Ministry of National Defense.
He is the author and co-author of numerous KIDA reports and English books and articles on the ROK-US alliance and the USFK, US defense and military strategies, Northeast Asian security affairs, ROK-US-Japan trilateral security cooperation, and multilateral security cooperation on WMDs and transnational threats.

SDD Special Experts Group
SDD 특별 전문가 그룹

JAPAN

Ueki Chikako 우에키 치카코

Professor, Graduate School of Asia-Pacific Studies, Waseda University, Japan
일본 와세다대학대학원 아시아태평양연구과 교수

Prof. Chikako Kawakatsu Ueki is a Professor of International Relations at the Graduate School of Asia-Pacific Studies (GSAPS) at Waseda University. Her areas of expertise include International Relations and Security in East Asia with a special focus on U.S.-Japan-China relations. She has written extensively on issues concerning threat perception in a unipolar world, transformation of international relations after the Cold War, and issues relating to security problems in East Asia. Prior to joining GSAPS, Dr. Ueki was Senior Research Fellow at the National Institute for Defense Studies, Japan Ministry of Defense; Visiting Scholar at Peking University; and Staff Writer for Asahi Shimbun. She served as a member of the Prime Minister's Council on Security and Defense Capabilities (2009) and was a Research Affiliate at Security Studies Program, Massachusetts Institute of Technology (2012-2015).

MACAU

You Ji 요우지

Professor, Department of Government and Public Administration, University of Macau, Macau
마카오 마카오대학교 정부행정학과 교수

Prof. Ji You is a professor of international relations and the head of the Department of Government and Public Administration at the University of Macau. He is author of four books, including China's Military Transformation and The Armed Forces of China, and numerous articles. Among them are "Xi Jinping and PLA Centrality in Beijing's South China Sea Dispute Management", China: An International Journal, Vol. 15, No. 2, 2017; "Sino-US "Cat-and-Mouse" Game Concerning Freedom of Navigation and Overflight", Journal of Strategic Studies, Vol. 39, No. 5-6, 2016; "China's Indo-Pacific Strategy", Asian Policy, No. 22, July 2016 ; "China's National Security Council: Evolution, Rationality and Operations", Journal of Contemporary China, Vol. 25, No. 96, 2016; "Managing conflicts in the Korean Peninsula: a Challenge to China's National Security", The Bulletin on Korea Studies, Vol. 30, 2017; "Managing the South China Sea Dilemma: China's Strategy and Policy", in Lowell Ditmmer and Ngeow Chow Bing (eds.), Southeast Asia and China: a Test in Mutual Socialization, World Scientific, 2017. Prof. You is on the editorial board of eight academic journals including The China Journal, Issue and Studies, and Journal of Contemporary China.Massachusetts Institute of Technology (2012-2015).

SINGAPORE

William Choong 윌리암 충

Shangri-La Dialogue Senior Fellow for Asia-Pacific Security, IISS, Singapore
싱가포르 IISS 샹그릴라대화 아시아태평양안보 선임연구원

Dr. William Choong is Shangri-La Dialogue Senior Fellow for Asia-Pacific Security at the IISS. He helps run the annual Shangri-La Dialogue and contributes to research on regional security issues such as the South China Sea territorial disputes and Japan's evolution into a 'normal' power. He has had a lengthy career with Singapore's main English-language newspaper, the Straits Times, where he was Senior Writer responsible for opinion pieces and editorials, focusing on defence, diplomacy and US policy in Asia. He wrote his PhD at the Australian National University (2005–2009) on US–China deterrence.Writer for Asahi Shimbun. She served as a member of the Prime Minister's Council on Security and Defense Capabilities (2009) and was a Research Affiliate at Security Studies Program, Massachusetts Institute of Technology (2012-2015).

FRANCE

Alice Ekman 앨리스 에크먼

Head of China Research, Center for Asian Studies, French Institute of International Relations, France
프랑스 국제관계연구소 아시아연구센터 중국연구부장

Dr. Alice Ekman is the Head of China Research at the Center for Asian Studies of the French Institute of International Relations (IFRI) and is currently visiting research fellow at the Asan Institute for Policy Studies in Seoul. She specializes in China's domestic and foreign policy, and also conducts research on the Korean peninsula. She is currently a member of the EU committee of the Council for Security Cooperation in the Asia Pacific (CSCAP) and Senior Associate Analyst at the European Union Institute for Security Studies (EUISS). She holds a PhD from Sciences Po in International Relations, an MA from the London School of Economics, and is the author of the La Chine dans le Monde (China in the World), to be published by CNRS Editions in France in November 2017. In Seoul, she created and developed the "Hanok Hike", outdoor events gathering officials and experts for informal foreign policy discussions, which are now held on a monthly basis.

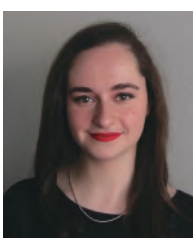
USA

Kevin Shepard 케빈 쉐파드

Defense Policy Specialist, Booz Allen Hamilton, USA
미국 부즈알렌해밀턴 국방정책컨설턴트

Dr. Kevin Shepard is a Defense Policy Specialist with Booz Allen Hamilton, supporting the U.S. Department of Defense commands in Honolulu, advising on the development, coordination, and execution of Korea-related plans, policies, and strategies, as well as theater-wide force posture and military-military engagements. Previously, he served as Deputy Director for United Nations Command-Korea, Combined Forces Command, and U.S. Forces, Korea Strategy Division. He provided significant input to the command's strategic objectives, policy and planning efforts. His portfolio included the ROK, DPRK, China, Japan, Southeast Asian nations and UNC sending states. Dr. Shepard also was a James A. Kelly Korean Studies Fellow at Pacific Forum CSIS, focused on U.S.-ROK alliance issues, and a research fellow with the Institute for Far Eastern Studies, where his primary focus was North Korean foreign policy decision-making and international cooperation for North Korean development.

EU



Zoe Stanley-Lockman 조 스탠리 락먼

Associate Analyst, EU Institute for Security Studies, USA
EU안보연구소 연구원

Ms. Zoe Stanley-Lockman is an Associate Analyst at the EU Institute for Security Studies (EUISS) and a Visiting Research Fellow at the S. Rajaratnam School of International Studies (RSIS). Based in Singapore, she focuses on defence-industrial issues, arms exports, innovation and military capability development. Her research on defence industries covers innovation in the West and nascent defence industrial development around the globe. Prior to joining the EUISS, her experience included working on export controls with the US government and consulting for defence contractors. Zoe holds a Master's degree in International Security with a concentration on Defence Economics from Sciences Po Paris and a Bachelor's degree from the Johns Hopkins University.

SDD 2017 Preparation Office
2017 서울안보대화 준비기획단

Ministry of National Defense, Republic of Korea

- **Choe Hyoung-chan** Director General for International Policy
- **Park Cheolkyun** Deputy Director General for International Policy
- **Yang Seongtae** Director, International Policy Division
- **Ko Youngseol** SDD Coordinator, International Policy Division
- **Son Daun** SDD Public Affairs, International Policy Division
- **Kim Wonjoon** International Cooperation Officer, International Policy Division
- **Lee Woojin** SDD Security Affairs, SDD Secretariat
- **Lim Wonsik** SDD Security Protocol, SDD Secretariat
- **Cho Yonbok** SDD Security Protocol, SDD Secretariat

Global Security Cooperation Center (GSCC) , Hankuk University of foreign Studies

SDD HUFS Secretariat

- **Hwang Jaeho** Director, GSCC
- **Park Jeongjae** Senior Research Fellow, GSCC
- **Lee Donggyu** Research Fellow, GSCC
- **Gu Jasun** Research Fellow, GSCC
- **Won Joooh** Assistant Research Fellow, GSCC

GSCC Advisors

- **Choi Woo-sun** Associate Professor, National Institute of Foreign Affairs
- **Hong Woo-taek** Research Fellow, Korea Research Institute for Unification
- **Lee Jae-hyun** Senior Research Fellow, ASAN Institute for Policy Studies

Supporting Staff

- **Cha Susie**
- **Daniel K. Elder**
- **Jo Eunnara**
- **Jin Shifeng**
- **Kang Nam-jeong**
- **Kim Dongmin**
- **Lee Jae-eun**
- **Lee Sunghyun**
- **Park Ji-youn**
- **Park Han-ye-seul**
- **Pyun Juwha**
- **Shin Jaeseop**
- **Suh So-young**
- **Won Jiyoung**

Contact Information

*** SDD 2017 TF**
Tel 02)748-6307 I Fax 02)748-6319
Email seouldefensedialogue@korea.kr

*** SDD 2017 Secretariat (PCO)**
Tel 02)550-2596 I Email Sdd.office2017@gmail.com

*** Global Security Cooperation Center, HUFS**
Tel 02)2173-2051 I Email . sddhufssecretariat@gmail.com