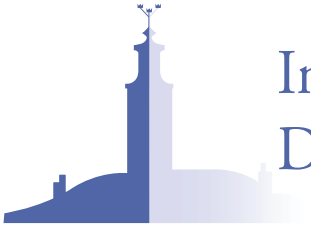
9th AMS-ISDP Joint Conference

Cyber Security: Identifying Threats and Charting a Common Defense

May 24, 2016, Stockholm



Institute for Security & Development Policy

中国军事科学院与瑞典安全和发展政策研究所第9届联合研讨会
The 9th AMS-ISDP Joint Conference

网络安全：识别威胁及构筑共同防御
Cyber Security: Identifying Threats and Charting a Common Defense

中国军事科学院
Academy of Military Science, China

瑞典安全和发展政策研究所
Institute for Security & Development Policy, Sweden

Stockholm, Sweden

May 2016

Contents

This report summarizes the presentations and discussions made during the 9th AMS-ISDP Joint Conference held in Stockholm, Sweden, on May 24, 2016. ISDP would like to thank Jesse Faria, Natasha Ikners, and Maria Rosaria Coduti for contributing to the writing of this report.

© Institute for Security and Development Policy, 2016

Disclaimer:

The opinions and conclusions presented in this report do not necessarily reflect the views of the Institute for Security Development Policy or the Academy of Military Science. All views are the interpretations of ISDP staff alone who are responsible for any inaccuracies presented in this report. The contents of this document may not be quoted or reproduced without the express permission of ISDP.

For editorial correspondence and enquries, please contact Alec Forss at: aforss@isdp.eu

About the Institutes:

The **PLA Academy of Military Science** is a center for military studies and the premier military research organization of the PLA. It answers directly to the Central Military Commission, and also directly receives tasks from the General Staff Department. AMS mainly carries out fundamental research on military science and important issues in defense and armed forces development, drafts and modifying military doctrines, regulations and laws, and provides strategic advice and consultation for military policymakers.

The **Institute for Security and Development Policy** is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security, and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood.

Foreword

The 9th ISDP-AMS Joint Conference was held in Stockholm on May 24, 2016. The theme for this year's conference was Cybersecurity: Identifying Threats and Charting a Common Defense. We are pleased to introduce the summary report from the conference and would like to thank all participants for their contribution toward a successful event.

Cybersecurity has rapidly emerged as one of the most serious non-traditional security challenges. Affecting states, businesses, and individuals alike, it brings policymakers tasked with defence to reconsider technical, legal, and ultimately strategic frameworks of security policy.

The conference brought together academics, diplomats, policymakers, and private sector participants from Sweden, China, Israel, Estonia and the United Kingdom to share their insights and experiences on this critical topic. In so doing, the conference sought to bridge understandings of cybersecurity between different actors and countries as well as how to best tackle the threats emanating from the cyber realm through better international cooperation and coordination.

The conference was divided into four different sessions: the Session One focused on cyber warfare and defense as part of modern military operations, with many countries having established dedicated commands for cyber defense. While regarded as a strategic necessity, these can also possess offensive capacities undermining national and international security. Session Two went on to analyse the criminal use of cyberspace by non-state actors such as terrorist organizations and transnational criminal networks, and what strategies can be employed to defend from such threats. Following on from this, Session Three took as its focus the vulnerabilities of critical information infrastructure and the role of the private sector in cybersecurity relative to governments. The final, fourth session took up the theme of international coordination and cooperation to counter cyber threats. Here participants concluded that better cooperation is indispensable if societies are to adapt technically sound and politically acceptable solutions to cyber security threats.

We are convinced that the reader will find this report informative and illustrative of the range of viewpoints presented and discussed during the conference.

Dr. Niklas Swanström (施万通), ISDP
Major General Liu Renxian (刘仁献 少将), AMS

前 言

军事科学院与瑞典安全和发展政策研究所于2016年5月24日，在斯德哥尔摩共同举办了第九届联合研讨会。今年会议的主题是“网络空间安全：判断威胁和形成共同防御”。我们很高兴地介绍会议报告摘要，并感谢参会人员的努力，使本届联合研讨会得以成功举行。

网络空间安全已经迅速成为非传统安全领域最严重的挑战之一。它影响到国家、商业和个人，也使决策者们重新思考安全政策方面的技术、法律和最终战略构想。研讨会中有来自瑞典、中国、以色列、爱沙尼亚和英国的学者、外交官、决策者及私人部门的人员。他们在会上就一些重要的问题交流思想和经验。通过这样的交流，研讨会为不同国家的参会代表搭建一个理解网络空间安全的桥梁，同时，也为如何更好地加强国际合作与协调，来解决网络领域出现的这些问题而搭建一个桥梁。

研讨会分为四节：第一节主要聚焦现代军事行动中的网络战和防御。很多国家急需进行网络防御，从战略意义上来看，网络防御也可以视为一种破坏国家和国际安全的一种进攻能力。第二节主要分析非国家行为体如恐怖组织和跨国犯罪组织在网络空间中的犯罪行为，以及采取何种战略来防范这些威胁。第三节主要聚焦讨论关键基础设施的脆弱性，以及私人部门在与政府相关的网络空间安全方面所扮演的角色。第四节主要讨论在应对网络威胁方面的国际协调与合作。与会者一致认为，如果整个国际社会要采用技术和政治上都可行的应对网络安全威胁的方法，那么更好的国际合作必不可少。

我们相信，各位读者可以从研讨会论文和讨论中的观点得到有益信息和启示。

中国人民解放军军事科学院 瑞典安全和发展政策研究所所长
刘仁献 少将 施万通 博士

Schedule

08:15 - 08:30	Registration
08:30 - 09:00	Opening session

Hosts

Dr. Niklas Swanström, 施万通
Director of the Institute of Security and Development Policy (ISDP)

Maj. Gen. Liu Renxian, 刘仁献 少将
Deputy Director of Department of Operational Theories and Doctrines, Academy of Military Science, PLA

Keynote Speaker

Dr. Erik Wennerström
Director-General Swedish National Council for Crime Prevention (Brå)

09:00 - 10:40	Session 1: Cyber Defense and Military Operations

Speakers

Wg. Cdr. Gareth Mount:
"UK Military Doctrine: the Challenge Presented by Cyber"
Officer at Development, Concepts and Doctrine Centre, Ministry of Defence, Royal Air Force (U.K.)

Sr. Col. Lu Zhian, 逯志安 大校:
"The Influence of Cyberspace Operations on Future Warfare"
Research Fellow in the Department of Operation Theory and Doctrine Research, Academy of Military Science (AMS), PLA

Dr. Walid Al-Saqaf:
"Towards a Better Understanding of Cyber Security Threats and Possible Actions"
Postdoctoral Researcher at the Department of Media Studies, Stockholm University

10:50 - 12:30	Session 2: Terrorism and Irregular Combatants

Speakers

Dr. Michael Barak:
"Al-Qaeda and ISIS - Case Studies in what is and what should be done"
Senior Researcher at the Institute for Counter-Terrorism; Lecturer at Lauder School of Government Diplomacy and Strategy, Interdisciplinary Center, Herzliya

Maj. Lin Han, 林涵 少校:
"The Challenges and Strategic Options of National Cyber Security"
Assistant Researcher at the Department of Military Political Work of the Academy of Military Sciences (AMS), PLA

12:30-13:30	Lunch break

13:30 – 15:10	Session 3: Private Sector and Critical Infrastructures

Speakers

Mr. Rami Efrati:
"Cyber in Private Sector and Critical Infrastructures-Present Status and Future Trends"
Founder and President of Firmitas Cyber Solutions

Dr. Zhang Ming, 张明 博士:
"China's Practices and Challenges on Critical Information Infrastructures Protection (CIIP)"
Associate research professor at China Institute of Contemporary International Relations (CICIR)

Prof. Katrin Merike Nyman-Metcalf:
"Privatisation of Liability"
Professor and Head of the Chair of Law and Technology at Tallinn University of Technology; Head of Research at the Estonian e-Governance Academy

15:20 – 17:00	Session 4: Policy and International Cooperation

Speakers

Col. Chen Ting, 陈婷 上校:
"Rule of International Law on Cyberspace: China's Positions and Prospects"
Associate Research Fellow at Academy of Military Science (AMS), PLA

Maj. Gunnar Wenngren:
"Personal and/or Organizational Responsibility for Information Security"
Independent Consultant on Information Security; Former Researcher at Swedish Defence Research Agency (FOI) and Swedish Defence Material Administration (FMV)

17:00 – 17:20	Closing session

Sessions

Session 1 — Cyber Defense and Military Operations

China, the United States and Russia are just a few of the increasing number of countries that have established dedicated commands for cyber defense operations. Alternately regarded as a strategic necessity and potential source of international insecurity, these developments are followed with both interest and concern by military planners and security analysts worldwide. This session asks how do we conceptualize the "information war," and what dimensions should we distinguish? Where does cyber warfare fit in the wider scope of military operations? What offensive and defensive capacities can militarized cyber units project?

Session 2 — Terrorism and Irregular Combatants

As a zone of conflict, cyberspace represents a low-cost, highly profitable environment, where perpetrators are less likely to be held responsible for their actions. Irregular combatants, such as transnational criminal networks and terrorist organizations, have seized upon this opportunity to develop new methods of recruitment, logistics and attack. However, definitions of threats, actors and objectives are complex. Session Two examines the latest trends in irregular cyberwar and cyberterrorism. What technological capacities can criminal and terrorist organizations draw upon? What strategies do security services have to prepare against these threats?

Session 3 — Private Sector and Critical Infrastructures

The security of digital infrastructures is of vital importance for the functioning of businesses and national economies. However, confidential information such as industrial and customer data have high economic and strategic value for illicit organizations. Consequently, systems lacking the necessary security mechanisms are often the target of massive security breaches. How are transnational cyber threats reconciled with national jurisdiction? How can policymakers provide adequate support to protect potential private sector targets? What mandate should businesses have to develop powerful non-state cyber security capabilities? How do public authorities best mobilize private cyber security expertise, without sacrificing legitimacy?

Session 4 — Policy and International Cooperation

Over the course of 2015, China's bilateral diplomatic efforts with countries such as the United States, the United Kingdom and Germany have resulted in landmark cyber agreements. However, cyberspace is subject to fast-paced change and transnationally-based threats. This raises the inevitable question: How do we develop the right collaborative tools and institutions for cyber defense? What skills and frameworks should policymakers develop to meet the challenge of cyber security? What are possible solutions to cyber threats through collaboration across political, legal, security, and private sectors?

Hosts

Sweden

Dr. Niklas Swanström, 施万通

Dr. Niklas Swanström is Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Research Fellow at the Johns Hopkins University's Paul H. Nitze School of Advanced International Studies, and Non-resident Professor at Sichuan University. Dr. Swanström has authored, co-authored or edited a number of books, including: Eurasia's ascent in Energy and geopolitics and Sino-Japanese Relations: The need for Conflict Prevention and Management. Dr. Swanström holds a Ph.D. in Peace and Conflict Studies from Uppsala University. He also holds a Licentiate degree from the Department of Peace and Conflict research that examined Chinese foreign policy towards Southeast Asia.

China

Major General Liu Renxian, 刘仁献 少将

Maj. Gen. Liu Renxian is the Deputy Director of Department of Operational Theories and Doctrines, Academy of Military Science, PLA. He was born on Nov. 16th 1962 in Henan Province, and joined the army in 1980. He earned his master degree of law in China University of Political Science and Law and gained his Ph.D. from Beijing Normal University. Since joining the PLA in 1980, he served in succession as an enlisted platoon leader, political instructor in company, secretary in political HQ, judge and President of Military Court, PLA. His main research fields included combat training, revising combat doctrines, non-war military operations, editorial working of Military Journals, in addition to research work.

Keynote Speaker

Sweden

Dr. Erik Wennerström

Dr. Erik O. Wennerström, LL.D., LL.M., is Director-General in charge of the Swedish National Council for Crime Prevention (Brottsförebyggande rådet - Brå) - an agency under the Ministry of Justice, acting as a centre for research and development within the judicial system. He has previously served as Principal Legal Adviser in International Law with the Ministry for Foreign Affairs of Sweden. His academic affiliation is primarily with the University of Uppsala, Sweden. He has a background with the Swedish Ministry for Justice, the European Commission and the Folke Bernadotte Academy of Sweden, and has been an adviser to countries seeking membership of the European Union. Between 2013 and 2015 he was Chairman of the Swedish Government Inquiry on Cyber Security.

Speakers (alphabetical order)

China

Colonel Chen Ting, 陈婷 上校

Chen Ting is an associate research fellow of Academy of Military Science (AMS), PLA. She works in the Department of Foreign Military and as deputy editor-in-chief of World Military Review where she is in charge of designing and editing key columns. She was enlisted as a postgraduate by Shanghai Branch, Nanjing Politics College in 2000 and was conferred a Master's Degree from AMS in 2003. In 2011 she gained a Ph.D. Degree in legal science from Tsinghua University Law School. Her current research focus is on cyberspace security.

United Kingdom

Wg. Cdr. Gareth Mount

Wg. Cdr. Gareth Mount joined the RAF in 1991 and has served at a number of locations in the UK and overseas. He has served at the UK's Permanent Joint Headquarters on two occasions, principally as a targeteer, including during the build up to operations in Iraq (2003). Operational deployments include working with NATO in Afghanistan at Regional Command South (2009) and multiple deployments to the Middle East working alongside the United States – the most recent being with US Central Command in Jordan as the UK liaison officer to a small deployed HQ supporting Operation INHERENT RESOLVE (the Coalition effort against Daesh). Wg. Cdr. Mount has completed the UK's Advanced Command and Staff Course, at the Joint Service Command and Staff College, and holds a Masters Degree in Defence Studies from King's College London.

Sweden

Major Gunnar Wenngren

Major Gunnar Wenngren joined the Royal Swedish Air Force in 1962, where he attained the rank of major, and where he continues to hold the title to this day. Following from his successful military experience, Major Wenngren has spent over a decade working as a computer security manager at Linköping University. This was followed by a role as researcher at FOI, the Swedish Defence Research institute, where Major Wenngren conducted extensive research on Swedish and global cyber security. Major Wenngren has also had vocational experience as a consultant with FMV, the Swedish Defence Materiel Administration.

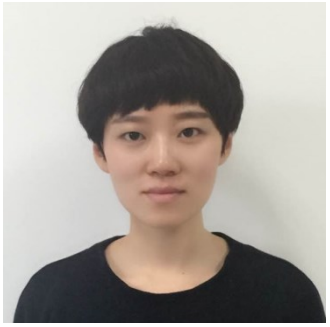
Estonia

Professor Katrin Merike Nyman-Metcalf

Professor Katrin Nyman-Metcalf is Head of the Chair of Law and Technology at Tallinn University of Technology and Head of Research at the Estonian e-Governance Academy. She is furthermore active as an international consultant, working globally primarily in the area of communications law, including ICT regulation, privacy and data protection, media law, e-governance and various cyber issues. Her PhD (Uppsala University, Sweden, 1999) is on the law of outer space and Katrin represents Estonia in the International Relations Committee of the European Space Agency.

China

Major Colonel Lin Han, 林涵 少校



Major Colonel Lin Han is an assistant researcher at the Department of Military Political Work of the Academy of Military Sciences, PLA. She holds a Master's Degree from the National University of Defense Technology, where she graduated in 2011. She was previously a visiting researcher to ISDP in 2013.

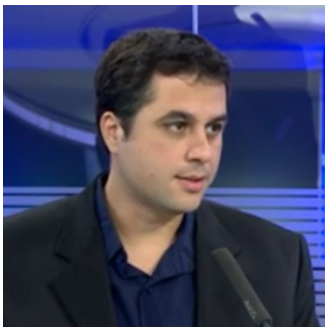
China

Senior Colonel Lu Zhian, 逯志安 大校

Lu Zhian is a research fellow in Department of Operation Theory and Doctrine Research, Academy of Military Science. He is in charge of the Center on Cyberspace Security Research. He has the rank of Senior Colonel and he is still in active duty. He has dual master degrees: the first one being on Joint Campaigns, attained at the Academy of Military Sciences, PLA. The second is on military strategy, from the Rajaratnam School of International Relations, Nanyang Technology University, Singapore. Lu Zhian conducts research in to cyberspace security, whereby his areas of focus are cyberspace operations, as well as cyberspace defense and related issues.

Israel

Dr. Michael Barak



Dr. Michael Barak is senior researcher at the Institute for Counter-Terrorism and a lecturer at Lauder School of Government Diplomacy and Strategy, Interdisciplinary Center, Herzliya. He is Team Leader of the Global Jihad & Jihadi Websites Monitoring Group and Team Research Manager of the ICT Cyber-Desk. Dr. Michael serves as senior researcher of the Social Media Networks in the Arab World research board at The Moshe Dayan Center for Middle Eastern and African Studies (MDS) in Tel Aviv University (TAU). Dr. Barak holds a Ph.D. in Middle Eastern Studies from TAU and specializes in Salafi and Sufi organizations, Global Jihad, Cyber-Terror and Modern Egypt.

Israel

Mr. Rami Efrati

Founder & President of Firmitas Cyber Solutions: a company focusing on providing a unique technological approach for the security of mission-critical infrastructure. An expert in Cyber Technology Strategic Methods, Mr. Efrati is the former Head the Civilian Division of the Israel National Cyber Bureau in the Prime Minister's Office. Col. (Res.) Efrati served in the Israel Defense Forces for over 28 years, commanding positions in Military Intelligence and receiving the Creative Thinking Award. Mr. Efrati also has 18 years of civilian experience and has been involved in entrepreneurial activities with both start-up and established companies in the Cyber-Security, High Tech and Bio-Technology sectors. He is advisory board member of Securonix, an industry-leading platform for security analytics. Additionally, Mr. Efrati is a Senior Cyber Fellow in Yuval Ne'eman Workshop for Science, Technology and Security in Tel-Aviv University, and Associate in the International Institute for Counter-Terrorism (ICT).

Sweden / Yemen

Dr. Walid Al-Saqaf

Dr. Walid Al-Saqaf is a Swedish/Yemeni postdoctoral researcher at the Department of Media Studies, Stockholm University, with a specialisation in ICTs, democratisation and Internet studies. He has a B.Sc. in computer engineering and a PhD in media and communication. His work and research revolve around Internet openness, surveillance, Internet and human rights, cyber security, censorship, and big data. He is a member of the board of trustees of the Internet Society (ISOC), a global organisation based in the United States that provides leadership in Internet-related standards, education, access, and policy while also actively promoting the maintenance of an open, resilient and secure Internet that is accessible to all people around the world.

China

Dr. Zhang Ming, 张明 博士

Zhang Ming is associate research professor at China Institutes of Contemporary International Relations (CICIR). His field of research focuses on cybersecurity, cyber strategy & policy, and social crisis management. Prior to his current position, he served as assistant research professor at the Institute of Information and Social Development, CICIR. From 2009 to 2015, Zhang attended nine rounds of CICIR-CSIS Cybersecurity Track 2 Dialogue held in Beijing and Washington, D.C., as a cybersecurity expert. Zhang holds a Ph.D in International Relations from CICIR, and a law degree from China Foreign Affairs University.

ISDP would like to thank Jesse Faria, Natasha Ikners, and Maria Rosaria Coduti for contributing to the writing of this report.

Institute for Security & Development Policy

Västra Finnbodavägen 2, 131 30
Stockholm, Nacka, Sweden

Tel: +46(0)73-415 0051
Fax: +46(0)8-640 3370

"The challenges of a cyber-world require the co-operation of each sector of the state and society"

Photo: DoD News, licensed under Flickr Creative Commons

U.S. joint service and civilian personnel focus on exercise scenarios during "Cyber Guard 2015" held at Suffolk, Virginia. The exercise involved more than 1000 participants, including active duty Army, Navy, Marines, Air Force and Coast Guard as well as National Guard and Reserve units and personnel. The Cyber Guard 2015 aimed at improving the ability of U.S. forces to defend the Department of Defense's information networks, secure its data, and mitigate risks to its missions.

Keynote Speech

Cyber Security: The Swedish Experience

Erik Wennerström

Dr. Erik Wennerström is Director-General of the Swedish National Council for Crime Prevention

In the keynote speech, Dr. Erik Wennerström outlined the strategic goals and proposals of the Swedish government in facing cybersecurity-related challenges. Some of the most urgent tasks for the Swedish government are to increase the governance and monitoring of cybersecurity to secure communications and enhance the prevention of crime. In particular, Dr. Wennerström argued that the risk management and incident reporting need to be improved in critical sectors like energy, public administration, healthcare, credit institutions, transportation, and internet enablers.

Dr. Wennerström went on to note increased cooperation between private and public sectors towards strategic goals set by the government. He highlighted in this regard the establishment of several cooperation agreements between different Swedish agencies.

In addition to domestic measures, Dr. Wennerström also stresssed that states need to cooperate to protect their security through standardization and confidence-building measures to fight cyberthreats. Responding to questions on current developments in Sweden, Dr. Wennerström asserted that: "you have to act security, it's a management issue and you cannot buy it."

SESSION ONE

UK Military Doctrine:the Challenge Presented by Cyber

Gareth Mount

Wing Commander Gareth Mount is a staff at the Development, Concepts and Doctrine Centre, Ministry of Defence (United Kingdom)

Wg. Cdr. Gareth Mount started his presentation by observing that some concepts of the UK military doctrine have been redefined in order to deal with non-traditional threats emanating from cyberspace. At the same

time, cross and inter-government cooperation is required more and more to prevent conflict and threats materializing; protecting the UK and Overseas from attack in and through cyberspace; and projecting influence and power directly from the UK. Wg. Cdr. Mount focused largely on cyber operations according to UK military doctrine and the different types of operations. He noted that defensive cyber operations can be either passive or active in nature and can be aimed at resolving both defence and security problems, since the distinction between them had become blurred. However, to identify the source of the threat is not an easy task, he argued. Offensive cyber operations require that cross-government departments and agencies (not just the intelligence and security agencies) need to work together to understand the how, what, who and why of a cyber attack in order to attribute it to a specific actor. Moreover, the targeting of such operations entails the integration of physical and informational activities which could result in collateral damage, both intentional and unintentional.

"A deeper understanding of the dependencies involved in cybersecurity is needed both to facilitate universal standards and to effectively face the challenges of cyber threats."

Wg. Cdr. Mount emphasized the factors to secure a successful cyber operation, which must include effective education and training. Cybersecurity is not only a matter of armed forces, but also the vulnerability of critical national infrastructure. What constitutes critical national infrastructure needs to be understood before mechanisms can be put in place to defend it.

Wg. Cdr. Mount concluded that a deeper understanding of the dependencies involved in cybsecurity is needed both to faciliate universal standards and to effectively counter the challenges posed by today's threats in and through cyberspace.

The Influence of Cyber Space on the Future of Warfare

Lu Zhian

Senior Colonel Lu Zhian is Research Fellow in the Department of Operation Theory and Doctrine Research, Academy of Military Science (AMS), PLA

Following on from Gareth Mount's presentation, Senior Colonel Lu Zhian placed emphasis on the importance of defining cyberspace and cybersecurity. He asserted that the two concepts of cyberspace security and cyberspace operations will influence future warfare in a positive way; in so doing, he outlined three reasons. First, the cost of war will decrease as cyberspace operations are characterized by high-time efficiency and high-cost effectiveness. Second, in the future the prevention of new war will be strengthened. In this regard, Lu Zhian noted that forces tend to coalesce

around issues concerning the national political situation and use cyberspace to influence public opinion. As such, he noted, this has an impact on political patterns and foreign affairs. Thirdly, due to "network centric warfare" in which all elements are integrated and operations can be easily coordinated the possibilities to "win" wars in the cyber-era have increased.

> **"The cost of war will decrease as cyberspace operations are characterized by high-time efficiency and high-cost effectiveness"**

He further asserted that the armed forces of the majority of the countries in the world have established their own military information networks. However, while recognizing that such networks guarantee more effectiveness, at the same time they can also create vulnerabilities in the operational systems.

Concluding the presentation, Senior Colonel Lu Zhian stressed the need to accelerate the building of cyberdefense systems by increasing defensive and offensive capabilities in cyberspace. According to Lu Zhian, these actions have not only become an urgent strategic task but also the only way to seize the new commanding height in future informationized operations.

Towards a Better Understanding of Cyber security Threats and Possible Actions

Walid Al-Saqaf

Dr. Walid Al-Saqaf is Postdoctoral Researcher at the Department of Media Studies, Stockholm University

The last presentation in the Session "Cyber Defense and Miltiary Operations" was given by Dr. Walid Al-Saqaf. While noting that he himself was from outside the world of military affairs, he nonetheless stressed that the challenges in a cyber-world require the cooperation of each sector of the state and society. Governments recognize the lack of power they have to govern the cyber-domain alone. However, governments are increasingly required to demonstrate they can be more "open minded" about cyberspace and will need different kinds of knowledge in order to solve defense-related problems.

> **"Governments are increasingly required to demonstrate they can be more 'open minded' about cyberspace and will need different kinds of knowledge in order to solve defense-related problems."**

The main recommendation Dr. Al-Saqaf made

to the political sector was the need to better utilize technical experts from various fields, as well as from academia and civil society. The mass use and penetration of technology implies that "anyone could become a window for a huge attack" and also that "every citizen is responsible for cybersecurity." In concluding, he raised the on-going challenge of defining the cyber domain as it is a multi-layered field with various stakeholders.

Discussion

Discussion raised areas of debate currently underway in Sweden such as regulation of cyberspace in the education sector (elementary and high-schools). The need to improve training for students and families and also for educators to teach students to think critically about cyber matters was pointed out in this regard. The point was further made that the government has recognized the lack of knowledge of the cybersphere at the individual level. Topics of debate also covered the ways in which we must adapt to the new realities presented by a cyber-world which have destroyed old systems of knowledge and created new information systems. As such, cyberspace is important for everyone and promoting security is the duty and responsibility of no one person, entity, or government. Speakers agreed that where the threats of cybercrime and cyberterrorism are markedly increasing the need for international co-operation rather than naming and blaming each other for attacks will be critical to cyberspace security.

"Cyberspace has become a vital platform for terrorist organizations - a low cost, profitable weapon against enemies"

Photo: Andrewww 26, licensed under Flickr Creative Commons

A man wearing a mask associated with Anonymous makes a statement in this still image from a video released in November 2015. The online collective announced to be "at war" with the Islamic State (ISIS) after the Charlie Hebdo attacks in Paris in that same year. The announcement was followed by a crowdsourced initiative to identify ISIS supporters and report their propaganda videos on social media platforms such as Twitter and Facebook. Anonymous also managed to successfully bring down hundreds of ISIS- related websites through distributed denial-of-service attacks.

SESSION TWO

Al-Qaeda and ISIS - Case Studies in What Is and What Should Be Done

Michael Barak

Dr. Michael Barak is Senior Researcher at the Institute for Counter-Terrorism and Lecturer at the Lauder School of Government Diplomacy and Strategy, Interdisciplinary Center, Herzliya

Dr. Michael Barak's lecture offered participants a close analysis of terrorist organizations' current use of cyberspace. Focusing particularly on the cases of ISIS and Al-Qaeda, Dr. Barak looked into the ways in which these two organizations capitalize on cyberspace to attain a variety of offensive, defensive, and operative objectives. He also provided participants with insights on the necessary strategies to prevent and address cases of cyberterrorism.

Dr. Barak started his presentation by stating that cyberspace has become a vital platform for terrorist organizations, as these groups dedicate ever more time and effort to better coordinate their cyber capabilities and knowledge as a low-cost, highly profitable weapon against enemies. Under religious justifications – following the principles of "Electronic Jihad" – terrorist groups such IS and Al-Qaeda attempt to win the "hearts and minds" of potential recruits. They successfully manage to do so, argued Dr. Barak, through multifarious online strategies and platforms. Dr. Barak noted that, today, a complex jihadist online network – encompassing thousands of forums, individual accounts and websites – is used for a number of offensive, defensive and operational purposes, such as to: circulate terrorist propaganda; train new recruits; encourage "lone-wolf attacks"; share strategic information in order to conduct attacks; teach recruits how to build explosive materials; penetrate planes and evade government surveillance; and collect money to fund campaigns.

> **"Cyberspace has become a vital platform for terrorist organizations."**

Following on from this, Dr. Barak offered participants his views on how to better understand, prevent, and tackle cyberterrorist activities. Amongst a number of suggestions, he emphasized the need for countries to support and co-operate with a number of non-state actors such as law firms, banks and internet companies. Dr. Barak also suggested the creation of a new international body that could monitor cyberterrorism. This body, he argued, would supply recommendations, establish international legal measures, and facilitate cooperation between nations against cyber terrorism as a means to maintain stability and prosperity in the international realm.

Thoughts on Counter Cyber-Terrorism

Lin Han

Lin Han is Assistant Researcher at the Department of Military Political Work of the Academy of Military Sciences (AMS), PLA

Major Colonel Lin Han began her presentation by explaining the ways in which terrorist organizations use cyberspace to broaden their impact and reach their objectives. She highlighted three main ways terrorists can threaten and infringe upon global cybersecurity: firstly, they can use websites and social media outlets for both propaganda and communication purposes; secondly, they can attack and potentially take over legitimate websites (the hacking of The Albuquerque Journal's website in 2014 being a case in point); thirdly, they can use the internet as a facilitator of other "traditional" forms of terrorist attacks.

According to Lin, groups such as IS can be more easily achieve their objectives through the use of the internet; compared with traditional terrorism approaches, she argued, cyber terrorism requires fewer people and fewer resources.

Major Colonel Lin proceeded to highlight the ways in which China has dealt with questions of cyber security, and argued that the country has recently designed policies and adopted practices to guarantee a safer cyberspace. She referred to a keynote speech delivered by President Xi Jinping in 2015, in which he identified respect for cyber sovereignty, maintenance for peace and security, promotion of openness and cooperation, and cultivation of a good cyberspace order as the key Chinese principles regarding cybersecurity. Major Colonel Lin argued that, over the last couple of years, the country has enhanced its cyberspace defensive ability, built national response systems for emergency, and fostered professional cyber talents.

> **"Over the last couple of years, China has enhanced its cyber space defense ability."**

Towards the end of her presentation, Major Colonel Lin offered a number of key measures that can help the global community to successfully tackle cyber terrorism on a global scale: the development of a cooperative concept of a "cyberspace community of common destiny"; the design of universally accepted and just rules for cyberspace; and the promotion of the integration of cyber security cooperation mechanisms.

Discussion

One of the questions that was initially presented during the discussion referred to the ways in which international cooperation can help in

the fight against cyberattacks. One of the participants addressed this issue, emphasizing that the lack of an international agreement on how to deal with cyber terrorism is hindering efforts to bring perpetrators to justice. It was also argued that nations should make full use of multilateral platforms such us the UN, as well as consider a universal agreement in which countries would be expected to cooperate during cyberterrorism investigations.

A further question concerned the longevity of terrorist organizations such as IS and Al Qaeda. It was observed by one member of the audience that, despite the fact that much time, energy and money have been spent on the battle against terrorism, the international community is still a long way away from extinguishing it. One of the speakers addressed this issue, noting that groups such as IS often flourish in non-governed areas, which are often plagued by conflict, poverty and instability. Such conditions are the foundation upon which terrorist ideology flourishes and is disseminated. It was also argued that, in order to successfully tackle the issue in question, it is necessary to address more profound socio-economic issues that are endemic in zones of conflict. One participant reiterated the importance of focusing on bottom-up, civil-society based strategies that can offer young and vulnerable people an alternative course to the one presented by extremist groups.
Another participant also took issue with the idea of cyber security now being the main threat, and consequently the main focus for nations in their fight against IS. It was argued that, although it is undeniable that cyber space security has become an integral part of the strategy to battle against terrorism, the main focus should continue to be in defeating the organization on the ground. Expanding on the aforementioned point, one participant argued that IS's territorial control in the Middle East represents a various serious threat to regional and global stability and – through the use of transnational, cooperative military measures – should be dealt with accordingly.

"For the private sector to take cybersecurity more seriously, governments must give incentives to companies to invest in cybersecurity"

Photo: Edgar Zamogilny, Licensed under Flickr Creative Commons

In April 2007, Estonia engaged in a disagreement with Russia over the relocation of the Bronze Soldier of Tallin (pictured above). The decision to relocate the controversial Soviet-era war memorial sparked riots in Tallinn and cyberattacks on Estonian organizations, including the country's parliament, ministries, banks and media outlets. Since this attack, the Estonian government has strived to enhance its cyber security, establishing a Cyber Security Council in 2009 in order to guarantee enhanced security for the country and its citizens, and to promote co-operation between various national and international institutions in matters of cyber space security.

SESSION THREE

Cyber in the Private Sector and Critical Infrastructures- Present Status and Future Trends

Rami Efrati

Rami Efrati is founder and President of Firmitas Cyber Solutions

Mr. Efrati's presentation sought to give an overview of the Israeli experience of cybersecurity with particular regard to the civilian sector. He started by giving a brief history of efforts to coordinate cybersecurity efforts. In 2003, the National Information Security Authority was established under the Israeli internal security ministry with the intention of defending the country against cyber-attacks – a credible threat given Israel's hostile regional neighborhood. In so doing, 25-30 companies were identified as constituting critical infrastructure. However, a key shortcoming was that no-one was responsible for the civilian sector. Nearly a decade later, in 2012, a new organization, the Israeli National Cyber Bureau, was created, which is tasked with coordinating all cybersecurity and working directly under the president. With increased attention accorded to cyber issues, 7 percent of the IT budget is slated for cybersecurity while each ministry will have a dedicated cybersecurity officer.

Mr. Efrati went on to highlight a number of important questions including how to ensure that the national grid is safe and who is certified to deal with cyber issues. He exposed a number of vulnerabilities to critical infrastructure including, among others, banks, energy providers, supermarkets, and transport systems – and that there is a need to increase resilience of so-called SMART cities to cyber-attack. One measure of resilience is the issue of service availability and how quickly, for instance, energy supply can come back online after an attack. In this regard, the Israeli energy ministry has realized the importance of making sure energy companies are made more secure.

> **"By framing the debate on the threat of cybersecurity in terms of potential economic losses to companies, it is more likely for the importance of cybersecurity to resonate with them"**

Mr. Efrati argued that for the private sector to take cybersecurity more seriously there was a need for the government to give incentives to companies to invest in cybersecurity through, for example, making such investments tax-deductible. By framing the debate on the threat of cybersecurity in terms of potential economic losses to companies, he argued that this was more likely for the importance of cybersecurity to resonate with them.

China's Practices and Challenges in Critical Information Infrastructure Protection (CIIP)

Zhang Ming

Dr. Zhang Ming is Associate Research Professor at the China Institutes of Contemporary International Relations (CICIR).

Dr. Zhang Ming's presentation focused on China's practices and challenges regarding Critical Information Infrastructure Protection (CIIP). The first part of his presentation proceeded to outline how the definition of CII has evolved in China starting from the State Council's proposal in 2003 of defining basic information networks (i.e. public telecommunication networks) and critical information systems (including railways, banks, customs, civil aviation, etc.) to the 2015 draft cybersecurity law which defines five types of networks and systems, encompassing the latter two as well as military, government, and large-scale Internet service providers (ISPs). He added that Xi Jinping has at several recent meetings urged the drawing up of regulations and laws on CIIP with it being formally included in China's 13th Five-Year Plan (2016-2020).

The second part of the presentation provided an overview of the CII "landscape" in China. In so doing, he cited statistics to show the explosive growth of Chinese "netizens," websites, and .cn users. At the same time, however, China is also becoming more vulnerable to cyber threats with 24,000 "incident-level" threats to information systems of governments and critical sectors recorded to the end of 2015. He proceeded to outline the responsible departments in China for dealing with CIIP. These include as follows: the Ministry of Information and Technology tasked with supervising the internet and telecommunication industry regarding CIIP; the Ministry of Public Security charged with countering cyber-attacks on CII and sharing information on threats through the National Information Reporting Center; and the Ministry of Foreign Affairs tasked with coordinating international issues on CIIP through the Office of Cyber Affairs.

> **"China is becoming more vulnerable to cyber threats with 24,000 "incident-level" threats to information systems of governments and critical sectors recorded to the end of 2015."**

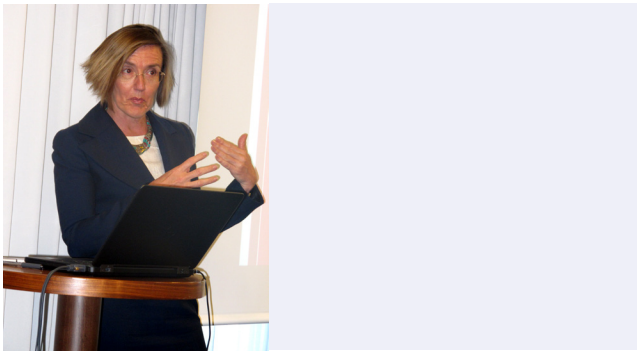
The fourth part of the presentation then went on to highlight the main CIIP mechanisms. This includes a system whereby information security protection is graded according to five levels – with the severity of the grade determining the measures taken by the government. These range from Grade 1 where damage is done to individuals and companies (for which operators are responsible for protection) to Grade 5 where especially serious damage is incurred to national security (in which case a specialized agency is tasked with overseeing the response.) Further-

more, a reporting system has been established by the National Information Reporting Center, including a special reporting platform among 50 critical State-owned Enterprises.

In concluding, Dr. Zhang identified challenges and paths ahead. He identified these to be better coordination among governmental agencies, public-private cooperation, enhanced relations between existing and new mechanisms, and international cooperation on CIIP.

The Private Sector and Critical Infrastructure: The Privatisation of Liability

Katrin Merike Nymam-Metcalf



Katrin Merike Nyman-Metcalf is Professor and Head of the Chair of Law and Technology at Tallinn University of Technology and Head of Research at the Estonian e-Governance Academy.

Dr. Nyman-Metcalf started her presentation by making a comparison between outer space and cyberspace by drawing some similarities but also distinctions between the two. But while cyberspace may differ from traditional sovereign space, she emphasized the applicability of international law and that, ultimately, states are still the main players responsible for activities within that space. Next she sought to clarify the distinction between information security, a term employed mainly by Russia and China, and cybersecurity used by the EU and United States. After proving some definitions of cybersecurity, she sought to characterize its main features – including the absence of physical national borders, no clear borders between public and private, no clear borders between civilian and military, and a borderless environment which directly bears on rules of privacy and anonymity affecting the individual.

She proceeded to highlight the applicability of international law to cyberspace. In this regard, she expressed her opinion that emphasis should lie on properly implementing existing provisions rather than creating many new legal instruments. On the issue of attribution, Dr. Nyman-Metcalf highlighted how perpetrators are difficult to locate with physical location being unimportant and the existence of international networks. Other issues presented included sovereignty over data and licensing.

> **"On the issue of applicability of international law to cyberspace ... emphasis should lie on properly implementing existing provisions rather than creating many new legal instruments."**

The last part of Dr. Nyman-Metcalf's presentation told the story of Estonia's experience of cyber-attack in April-May 2007 which

lasted for about two weeks. This saw DDoS attacks on banks, spamming of news websites, and so on, in what constituted an unprecedented concerted and sophisticated attack. While Estonia turned to Russia under the Mutual Legal Assistance Treaty, assistance was denied. She went on to highlight a number of lessons learnt for cybersecurity from the episode, which include the importance of a comprehensive approach, an inclusive process, that attacks cannot be simply stopped with one kind of (technical) measure, the importance of transparency in reporting breaches, as well as upholding a multi-stakeholder model. Out of the attacks developed the Tallinn Manual on the International Law Applicable to Cyber Warfare, albeit a non-binding, non-official document.

She then went onto outline Estonia's efforts to protect its cyberspace (pointing out that Estonia has one of the most advanced e-governance systems in the world), including the role of private enterprises in being responsible for key components of cyber society and making them key partners, not just subjects, of rule-making.

Discussion

In the discussion session, a question was asked whether such an attack as Estonia experienced in 2007 could occur again. The presenter answered that while there is now better preparedness in Estonia, another similar attack could nevertheless not be ruled out. Another question related to the issue of privacy and getting private companies to share information. It was admitted by one of the presenters that indeed a government could not force the private sector to share information with a lack of trust existing; nonetheless, it was emphasized that there is a clear need to transfer information. In the case of information-sharing in China, it was answered that such sharing is difficult and is currently mostly voluntary. Another presenter argued that breaches of systems are often not reported by the private sector because of the perception that it was "bad for business."

Further questions related to the issue of state responsibility to act as well as definitions of critical infrastructure and the emerging issue of cyber-insurance.

"Cyber security threats have become more serious, extending to criminal networks domestically and internationally"

Photo: National Anthems, licensed under Flickr Creative Commons

During President Xi Jinping's visit to the United States in September 2015 (pictured above), cybersecurity was one of the main topics of discussion with President Barack Obama. During the talks, both leaders committed to identifying and encouraging appropriate norms of state behavior in cyberspace within the international realm. The aforementioned agreement on matters of cyber space was welcomed as an unprecedented historic development between the two superpowers.

SESSION FOUR

Rule of International Law on Cyberspace: China's Position and Prospects

Chen Ting

Cheng Ting is Associate Research Fellow at Academy of Military Science (AMS), PLA, Personal and/or Organizational Responsibility for Information Security

Colonel Chen Ting began her presentation by saying that as the high usage of technology and the importance of cyber networks grows in the twenty-first century, this will challenge existing international and domestic laws to protect and prevent threats. In this regard, Colonel Chen highlighted that the "rule of law" in regulating cyber space is still relatively new. Since the 1990s cyberspace has been largely "self-regulated" in China but domestic governance has gradually been phased in and more recently, from 2010, international regulation has developed through international law.

Colonel Chen proceeded to illustrated China's position on the rule of law in cyber space and the basic approach to governance in two key areas: 1) internationally the United Nations Office for Disarmament Affairs (UNODA) has been a major platform for establishing the normative framework that governs "International Cyber Space Rules"; and 2) domestically through the principle of "national sovereignty" and the balance of individual freedoms with cyber security concerns.

> **"As the high usage of technology and the importance of cyber networks grows in the twenty-first century, this will challenge existing international and domestic laws to protect and prevent threats. "**

China has taken active measures to: improve the domestic rule of law, strengthen policy dialogue /co-operation, and has participated in the drafting of international cyber security laws. For example, China was one of 20 countries included in the Group of Governmental Experts (GGE) responsible for the 2015 UN draft report that has established the norms, rules, and principles regulating the responsible behaviour of states in cyber-sphere. The report also outlines confidence-building measures, international cooperation and capacity building with wider implications to all states. This builds on the Tallinn Manual which provides the basic definitions and principles while the International Code of Conduct in Security has established the implementation of these.

However, she highlighted contentions and contradictions regarding the definition of cyber security and the implementation of a security

framework. A key question is whether "cyberspace" is a domain of the global commons or domestic commons? Colonel Chen suggested a hybrid model to bridge the normative divide. Governance of cyberspace remains in the preliminary stages, she argued, and the difficulties in consistently approaching it, whether from self-defence or through surveillance of threats, remains problematic. As such, Colonel Chen highlighted the need for mutual co-operation and China's strategies through: diplomacy, research on controversial issues, and the adaption of legal norms to strengthen the rule of law.

Personal and/or Organizational Responsibility for Information Security

Gunnar Wenngren

Gunnar Wenngren is an independent consultant on information security

Major Wenngren's presentation emphasized the importance of individual agency in cybersecurity. As he pointed out, the field of cyberspace to the basic and average user has changed dramatically with the development of internet technology over the past two decades. Cybersecurity threats have become more serious and extend to criminal networks both internally and internationally. Major Wenngren highlighted the increase in threats such as: malware (viruses), phishing and spam. Added to this, the storage of personal data and health records has increased the risks to identity theft, one of the fastest growing crimes exploited by criminal networks and facilitated by the black market.

> **"Storage of personal data and health records has increased the risks to identity theft, one of the fastest growing crimes exploited by criminal networks"**

While whistleblowers have called attention to these areas, the broader question is whose domain of responsibility governance falls under? Wengrenn stressed individual behaviour and education of the user is at the core of handling and mishandling of information technology. He subsequently proposed four pillars to shore up individual accountability through: (1) That required data is accessible, in order to enable a quick response in times of need; (2) that this data is both factually correct as well as complete; (3) that data is effectively protected against unauthorized access; and (4) that data is handled and processed in accordance with the law and applicable regulations.

Discussion

Discussions that followed focused on the differences between countries in defining "cyberspace" and how this has implications for the regulation of it through international law. The proposition to divide "cyber space" in the fashion of maritime boundaries was highly contentious but highlighted the difficulties in establishing a basic definition. China maintains that cyberspace is "not a global domain" but rather should be understood as overlapping with domestic and individual rights. Much of cyberspace, as was pointed out, exists in "clouds" and cannot be regulated in the traditional sense of security threats. However, it was suggested that states need not agree on a definition per se but identifying the key areas was more important. Added to this, the private sector will have a more dominant role in the regulation of cybersecurity as most firms such as IBM and Microsoft hold vast stores of commercial data. The most important factor is to build mutual co-operation in the sharing of information and building of trust whether at the individual, domestic, private or international level.