EAST ASIA'S SECURITY CHALLENGES

21-22 January 2018

The Truman Institute for the Advancement of Peace
The Hebrew University of Jerusalem

January 21 | Sunday

09:30-10:00 Gathering and Registration

10:00-10:30 Opening Remarks

H.E. Mr. Koji Tomita, Ambassador of Japan to the State of Israel
Menahem Blondheim, Truman Institute, The Hebrew University
Nissim Otmazgin, Dept. of Asian Studies, The Hebrew University
Galia Press-Barnathan, Dept. of International Relations, The Hebrew University

10:30-12:00 Japan's Regional Security

Chair: Galia Press-Barnathan, The Hebrew University
Ehud Harari, The Hebrew University: *"Japan's Security Challenges in the 21st Century"*
Paul Midford, Norwegian University of Science and Technology: *"Overcoming Security Isolationism: Japan's Promotion of East Asian Security Multilateralism Since 1991"*
Yiftach Govreen, The Hebrew University: *"Closing the Gaps: Transnational Policy Networks in the U.S.-Japan Alliance"*

12:00-13:00 Lunch Break

13:30-15:00 China and East Asia's Regional Security

Chair: Lior Rozenberg, The Hebrew University
Kai He, Griffith University: *"Rethinking China and International Order: A Conceptual Analysis"*
Yitzhak Shichor, The Hebrew University: *"False Alarm: Xinjiang and China's National Security"*
Doron Ella, The Hebrew University: *"Institutional Statecraft with 'Chinese Characteristics': The AIIB as a Case in Point"*

January 22 | Monday

09:00-10:30 Maritime Conflicts and North Korea's Nuclear Dilemma

Chair: Ira Lyan, The Hebrew University
Tetsuo Kotani, Japan Institute of International Affairs (JIIA): "Gray Zone Conflicts in Maritime Asia"
Alon Levkowitz, Bar-Ilan University: *"North Korea's Nuclear Threat in Regional Perspective"*
Or Rabinowitz-Batz, The Hebrew University: *"Four Paths to a 'Strategic Miscalculation' over North Korea"*

11:00-13:00 Cybersecurity and Regional Security: Lessons from East Asia and the Middle East

This panel is in collaboration with, HUJI Cyber Security Research Center (H-CSRC)– Cyber Law Program
Chair: Amit Sheniak, The Hebrew University
Dai Mochinaga, Mitsubishi Research Institute Inc.: *"Key Elements Governing Cyberspace and Security Environment in Japan and Beyond"*
Dayu Kao, College of Police Science and Technology, Taiwan: *"Toward Actionable Intelligence of Private-Public-Partnership (PPP) in Improving Cybersecurity Forensic Investigation"*
Amit Sheniak, The Hebrew University: *"The Israeli Cybersecurity Innovation Ecosystem: The Case of Beer-Sheva Cyber-Park"*
Tamar Berenblum, The Hebrew University: *"Geography Matters: Spatial Dimensions in System Trespassing Incidents"*
Anja Mihr, HUMBOLDT-VIADRINA Governance Platform: *"Public Privacy: The Balance between Freedom and Privacy in Cyberspace"*

13:00-14:00 Lunch Break

14:30-16:00 The Regional Implications of Great Power Competition

Chair: Danny Orbach, Truman Institute, The Hebrew University
Raymond Yamamoto, Aarhus University: *"China and Japan's Economic Engagement in Southeast Asia–A Threat to Regional Security?"*
Galia Press-Barnathan, The Hebrew University: *"Multi-Level Governance- US-ASEAN Counter-Terrorism Cooperation"*
Yoram Evron, University of Haifa: *"The Spillover of Asian Rivalry: Asia-Related Disputes in the Middle East"*

16:30-17:30 Concluding Roundtable: East Asia's Security Challenges and Prospects

Chairs: Nissim Otmazgin, The Hebrew University
Galia Press-Barnathan, The Hebrew University

האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Embassy of Japan
Israel

מרכז פריברג ללימודי מזרח אסיה
The Frieberg Center for East Asian Studies

החוג ללימודי אסיה
Department of Asian Studies

Truman Institute

Conference Organizers:
Nissim Otmazgin and Galia Press-Barnathan, The Hebrew University

For further information and registration:
asia.chair@gmail.com

East Asia's Security Challenges

The Truman Institute for the Advancement of Peace & The Department of Asian Studies
The Hebrew University of Jerusalem, 21-22 January 2018

Sunday January 21, The Truman Institute, Abba Eban Hall

10:00-10:30 Opening Remarks

H.E. Mr. Koji Tomita, Ambassador of Japan to the State of Israel

Nissim Otmazgin, Dept. of Asian Studies and the Truman Institute, The Hebrew University of Jerusalem

Galia Press-Barnathan, Dept. of International Relations, The Hebrew University of Jerusalem

10:30-12:00 Japan's Regional Security

Chair: Galia Press-Barnathan, The Hebrew University of Jerusalem

Ehud Harari, The Hebrew University of Jerusalem

"Japan's Security Challenges in the 21st Century"

Paul Midford, Norwegian University of Science and Technology

"Overcoming Security Isolationism: Japan's Promotion of East Asian Security Multilateralism Since 1991"

Yiftach Govreen, The Hebrew University of Jerusalem

"Closing the Gaps: Transnational Policy Networks in the US-Japan Alliance"

12:00 – 13:00 Lunch Break

13:30-15:00 China and East Asia's Regional Security

Chair: Lior Rozenberg, The Hebrew University of Jerusalem

Kai He, Griffith University

"Rethinking China and International Order: A Conceptual Analysis"

Yitzhak Shichor, The Hebrew University of Jerusalem

"False Alarm: Xinjiang and China's National Security"

Doron Ella, The Hebrew University of Jerusalem

"Institutional Statecraft with 'Chinese Characteristics': The AIIB as a Case in Point"

Monday, January 22, Beit Maiersdorf, Room 405

09:00-10:30 Maritime Conflicts and North Korea's Nuclear Dilemma

Chair: Ira Lyan, The Hebrew University of Jerusalem

Tetsuo Kotani, Japan Institute of International Affairs (JIIA)

"Gray Zone Conflicts in Maritime Asia"

Alon Levkowitz, Bar-Ilan University

"North Korea's Nuclear Threat: A Regional Perspective"

Or Rabinowitz-Batz, The Hebrew University of Jerusalem

"Four Paths to a 'Strategic Miscalculation' over North Korea"

11:00-13:00

Cybersecurity and Regional Security – Lessons from East Asia and the Middle East

This panel is in collaboration with, HUJI Cyber Security Research Center

(H-CSRC) – Cyber Law Program

Chair: Amit Sheniak, The Hebrew University of Jerusalem

Dai Mochinaga, Mitsubishi Research Institute Inc.

“Key Elements Governing Cyberspace and the Security Environment in Japan and Beyond”

Dayu Kao, College of Police Science and Technology, Taiwan

"Toward Actionable Intelligence of Private-Public-Partnership (PPP) in Improving Cybersecurity Forensic Investigation"

Amit Sheniak, The Hebrew University of Jerusalem

"The Israeli Cybersecurity Innovation Ecosystem: The Case of the Beer-Sheva Cyber-Park"

Tamar Berenblum, The Hebrew University of Jerusalem

"Geography Matters: Spatial Dimensions in System Trespassing Incidents"

Anja Mihr, HUMBOLDT-VIADRINA Governance Platform

"Public Privacy: The Balance between Freedom and Privacy in Cyberspace"

13:00-14:00 Lunch Break

14:30-16:00 The Regional Implications of Great Power Competition

Chair: Danny Orbach, Truman Institute

Raymond Yamamoto, Aarhus University

"China and Japan's Economic Engagement in Southeast Asia: A Threat to Regional Security?"

Galia Press-Barnathan, The Hebrew University of Jerusalem

"Multi-Level Governance: US-ASEAN Counter-Terrorism Cooperation"

Yoram Evron, University of Haifa

"The Spillover of Asian Rivalry: Asia-related Disputes in the Middle East"

16:30-17:30 Concluding Roundtable: East Asia's Security Challenges and Prospects

Chairs: Nissim Otmazgin and Galia Press-Barnathan, The Hebrew University of Jerusalem

Conference Conveners

Nissim Otmazgin, Department of Asian Studies & Truman Institute, The Hebrew University of Jerusalem

Galia Press-Barnathan, Department of International Relations, The Hebrew University of Jerusalem

Collaborating Institutions

Established in 1968, **the Harry S. Truman Research Institute for the Advancement of Peace** is the first and largest peace institute in Israel and the wider Middle East, home to over 120 scholars working on issues related to peace studies and conflict resolution in different parts of the world. The Truman Institute offers a dynamic forum for discussing and debating the challenges facing Israelis, Palestinians, and other communities in Israel and the Global South. For further information, please visit: http://truman.huji.ac.il

The Department of Asian Studies at the Hebrew University of Jerusalem is the oldest in Israel and is one of the largest departments in the Faculty of Humanities, home to over 300 students specializing in Japanese, Chinese, Korean, and Indian Studies. The department is characterized by its excellence in research and teaching, and it maintains an environment of cooperation between students and faculty in a wide array of extracurricular activities. To read more about the department, please visit: http://asia.huji.ac.il/en

The Louis Frieberg Center for East-Asian Studies, founded in 2006, is an interdisciplinary forum of researchers at the Hebrew University of Jerusalem, which aims to promote and broaden teaching, research, and discussion of East-Asian related subjects. The center aims to create a space that links the academy and the wider public, where a diverse group of people and scholars can exchange ideas across disciplinary boundaries. To read more about the center, please visit: http://eacenter.huji.ac.il/?id=500

This conference was generously supported by the Embassy of Japan in Israel

Conference Introduction:

East Asia's Security Challenges

Nissim Otmazgin and Galia Press-Barnathan

The Hebrew University of Jerusalem

This conference discussed the challenges to East Asia's security environment. The papers in the conference examined traditional security threats, as well as new threats such as terrorism and cybersecurity. They also examined the existing mechanisms and arrangements (military and institutional buildup, state-to-state alliances, and international organizations), as well as more recent arrangements, and offered varying assessments with regard to their ability to maintain regional stability in the face of multiple challenges. While all the papers presented in this conference touched upon the challenges for regional security, some expressed more warning signs than others.

Conceptually, the conference sought to offer a complex and nuanced assessment of regional security challenges in East Asia. One such theme was the need to examine regional security across several levels of analysis, which are shaped and influenced by domestic factors in key states (Japan, China, Korea, members of ASEAN (Association of Southeast Asian Nations, the US) by specific regional inter-state dynamics that build on historical and current rivalries (e.g. China-Japan rivalry, South-North Korean relations) and by the interaction of the region as a whole and its individual members with extra-regional actors such as the United States, international organizations, and other regions like the Middle East.

A second theme was the need to think about security in a complex manner. Under the title "security," we investigated traditional security threats (physical threats to states' physical well-being) and emerging transnational security threats (terrorism and cyber threats). We also noted that it is impossible to discuss security, both in terms of challenges and strategies, in a narrow military sense and that economic factors are part and parcel of the analysis. Indeed, Japan, and consequently other East Asian states, have been the first to explicitly acknowledge this connection, coining the notion of "comprehensive security."

A third theme that became quite noticeable during the conference pointed to the need to engage in analysis by scholars from different states and perspectives. The conference brought together experts who deal with individual states (Japan, China or Korea), with specific issue areas (e.g. nuclear proliferation or cybersecurity), and with broader security questions regarding international relations (IR). While this was an academic conference made up of academic experts, it became clear that how one studies regional security may vary depending on where one does her/his research and the academic clusters she/he works within. The interaction among scholars from different states served as a very useful reminder of this, and generated fascinating interaction.

Finally, an additional fact was that Israeli scholars also took part in the conference. Their participation, as well as the fact that this conference took place in Jerusalem, offered an added value on several fronts. To the conference itself, it offered a perspective from outside the region that

Asian experts are less familiar with (e.g. the discussion on cybersecurity in East Asia and in Israel). However, at the same time, the conference itself contributed to the strengthening of research and academic discussion of Asian security within Israeli academia, and generated exposure of these important topics to a broader intellectual public of students and scholars. Some of the issues that were discussed in the conference indeed suggest that future comparisons of security challenges and strategies between East Asia and the Middle East may be interesting and useful.

In what follows, we briefly review the papers presented at the conference, based on the issues they addressed. This will be followed by a more detailed account of each paper.

Ehud Harari's paper on Japan's security made a useful distinction between regional and global challenges. The latter are becoming increasingly important given Japan's relatively recent proactive involvement, not only in regional affairs but also in international organizations. However, Harari's paper also emphasized the risk of what he calls the "wild cards" – Trump and Kim Jong-un – as having the potential to initiate unexpected immediate action that will fundamentally change the security situation in East Asia.

Tetsuo Kotani, who, in his paper, emphasized the risk of violent escalation between Japan and China over the Senkaku Islands, flagged another warning sign. As he discusses in his paper, the "gray zones" – maritime territories, which both Japan and China claim sovereignty over – also encapsulate the broader regional rivalry between the two countries. These gray zones increase uncertainty between the two sides, destabilize state-to-state relations, and represent an immediate threat for military escalation. (Imagine what can happen if, for example, a Chinese vessel infiltrating the zone around the Senkaku Islands is gunned down?)

Galia Press-Barnathan's paper focused on terrorism as yet another challenge to regional security, brought to the forefront of the USA’s agenda following 9/11. According to Press-Barnathan, one of the consequences is the growing attention given to terrorism, not only on a national level but also by regional organizations such as ASEAN. This, in turn, facilitates dialogue and cooperation between regional and extra-regional actors. This cooperation, according to her, is nested in broader global governance structures of counter-terrorism activity and highlights an important role of regional institutions like ASEAN and the ASEAN Regional Forum (ARF).

Focusing on Japan, Paul Midford's paper examined the risks to the country's reliance on regional security multilateralism (RSM), which has developed since the end of the Cold War. He, however, argues that the RSM framework is still stable and beneficial to Japan. Equally, Yiftach Govreen's paper argues for the stability of Japan's regional security, focusing on the unofficial role played by individuals to maintain the Japan-US Security Alliance. Building on the network literature in IR, Govreen's paper emphasized the stabilizing role played by networks comprised of individual mediators from both the US and Japan who help bridge divisions in times of crisis.

The papers of Kai He and Doron Ella examined the way China is increasing its involvement and influence in the international arena and considered whether China's international behavior advances a new set of Chinese-oriented IR norms. Kai He argues that China's rising influence will no doubt become a challenge to the international order; nevertheless, how China will challenge the international order remains unknown. He suggests a more elaborate conceptual framework to think about the nature of this challenge. Similarly, focusing on the Asian Infrastructure Investment Bank

(AIIB), Doron Ella argues that while China is willing to adopt institutional norms prevalent in other similar institutions (such as the World Bank and the Asian Development Bank), it is gradually introducing new norms more akin to its political agenda. From their papers, the emerging picture is that China's growing international presence constitutes both a challenge and an opportunity to the regional security order.

Raymond Yamamoto and Yoram Evron examined the emerging rivalry between Japan and China in two different regional contexts: Southeast Asia and the Middle East. Yamamoto's paper describes the emerging competition between Japan and China in providing aid and building economic infrastructure in the countries of Southeast Asia, but argues that this competition should be seen as part of each country's attempt to better its economy and not as a struggle over regional dominance. Evron's paper, on the other hand, emphasizes the spillover of Sino-Japanese rivalry into the Middle East, intensified by China's Belt and Road Initiative (BRI). According to him, this is part of the desire of the two countries to increase their impact beyond the Asian region, and their similar inclination to combine political and economic goals and the means to do so.

Focusing on North Korea, the papers of Alon Levkowitz and Or Rabinowitz suggest that we might be interpreting the country's nuclear strategy wrong. Looking at the various circumstances and contexts North Korea operates within, Levkowitz emphasizes the failure of the six-party talks and questions the usefulness of the US military showoff in deterring North Korea. Similarly, Rabinowitz suggests that North Korea’s harsh statements may have a particular internal logic of their own, which outsiders tend to miss completely. She warns that we tend to see the country's behavior according to experiences and theoretical frameworks developed in other parts of the world, which might not be as relevant for understanding the Korean Peninsula.

Finally, five papers dealt with the issue of cybersecurity, demonstrating the ways in which this newly emerging field of study can be related to the issue of regional security. Dai Mochinaga's paper looked closely at Japan's cyberspace institutional environment and emphasized the potential of cybersecurity to connect different sectors within the Japanese economy; while Da-Yu Kao showed how cybersecurity should be integrated into everyday police work at both national and transnational levels. Amit Sheniak discussed the growing importance attributed to cybersecurity in Israel, and to the process known in IR literature as “securitization.” But more importantly, focusing on a Beer-Sheva cyber park in southern Israel, he emphasized the impact of cybersecurity on generating a national push to promote cybersecurity as an economic growth engine. The papers of Tamar Berenblum and Anja Mihr touched upon a new set of risks brought about by cybersecurity: the delineation of location and space carries risks to victimized computers and system trespassers (Berenblum) and to human rights (Mihr).

The emerging picture is a mixture of risks and challenges where new forces (terrorism, externalization of rivalry outside of East Asia, cybersecurity) are potential threats to East Asia's regional security, but at the same time, "old arrangements" (Japan's reliance on regional security multilateralism and the stability of the US-Japan security alliance) keep it stable. Concurrently, destabilizing sources of concern continue to exist, both in the long term (China's gradual reshaping of the world order) and immediately (North Korea's nuclear threat).

Summary of Papers

Panel I: Japan's Regional Security

Japan's Security Challenges in the 21st Century

Ehud Harari, The Hebrew University of Jerusalem

In this paper, I present a conceptual framework of various dimensions of security challenges, through the Japanese case, with several examples.

Japan today faces numerous challenges, which vary in nature and derive from different causes. The challenges Japan faces are global (those which the whole world is confronted with) and Japan-specific. But the global challenges are the most serious and pressing. Some of modern Japan's long-term challenges (military, food supply, energy, and mineral resources) are historical, spanning from the Meiji period to the present. Another set of challenges, such as the "rise of China," the territorial "gray zones" (e.g. Senkaku and Takeshima), emerged in the postwar and post-Cold War era. Finally, some challenges are linked more directly to the present and the future, namely North Korea's "nuclearization"; the demographic challenge (Should Japan open its gates to foreign human resources, or should she avoid this because such policy might turn out to be a double-edged sword? Instead, could Japan facilitate an increase in the women's labor force participation rate?); technological challenges (nuclear, cyber); and "wild cards" (Trump ("wild" not "trump" card), Kim Jong-un); or other "contingencies."

Moreover, the types of challenges Japan faces can be analyzed from the vantage point of different theories of international relations. One type is structural, a function of the structure of the regional or world system. This is in line with the "realism" variant of IR theory, where state actors compete for power and "balance." According to Japan's National Security Strategy (NSS) report of 2013, the changing balance of power in Asia-Pacific, the rise of China, and the advancement of globalization and technological innovation means “threats, irrespective of where they originate in the world, could instantly have a direct influence on the security of Japan.”

In contrast, other types of challenges are domestically-induced and derive from the choices of the domestic actors. These are best examined through the combined lenses of two other variants of IR theories – "liberalism," where non-state actors, domestic and international, participate; and "constructivism," where values and ideas play a major role.

One such set of challenges emanates from the variants of national identity (small power, regional power, world power, no power, Asian power, Western power, uniquely Japanese power). With regard to these challenges, it is important to mention the role of what Haagstrom and Gustafsson call "identity entrepreneurs." Prime Minister Abe and former Prime Minister Hatoyama are two salient examples of identity entrepreneurs – Abe with his idea of Japan's “proactive contribution to peace,” and Hatoyama's "commitment to Asia."

Another set of challenges that reflect this mix of approaches are those that emanate from a hierarchical view of the world power structure (superiority in relation to Asia; inferiority in relation to the developed "West") and the challenges that Japan faces as a less powerful partner in international alliances. Those include avoiding "entrapment" on the one hand, and "abandonment" on the other, as well as balancing bilateral alliances and multilateral structures of cooperation. A good example of the entrapment concern is the recent right of "collective self-defense" legislation, which reduces Japan's ability to "hedge" its commitments within the US-Japan alliance, i.e. avoiding getting involved in US military operations being unrelated to Japan's security.

The recent inward-looking foreign policy of the Trump administration (withdrawal from TPP – Trans-Pacific Partnership) is an excellent example of the concern over abandonment, and Abe's argument that "collective self-defense" strengthens the US commitment to play a leading security role in the region illustrates one strategy to deal with it. On the dilemma of using multilateral structures, Japan faces the question of how inclusive the multilateral structures should be, and whether they should be "closed," open exclusively to East Asia, or only open to "like-minded"/allies, and therefore, to the exclusion of rivals. Or, should they encourage “open" structures, such as ASPAC (Asia Pacific) or ASPAC + India = IndoPacific? (President Trump's version of Prime Minister Abe's "security diamond").

Japan also faces challenges that derive from its ambitions to carve a security leadership position in Asia. The main dilemma is whether to adopt/adhere to a leadership-from-behind approach: taking initiatives, but letting others get the credit – a residue of Asians' concern about Japan's motives – or to attempt "up-front" leadership.

In this "mixed" bag of challenges leaders matter. Leaders in bilateral or multilateral rivalries or conflicts can turn certain challenges, such as "crises,” into opportunities for cooperation. The ultimate challenge for world leaders would be in a not inconceivable situation where a "crisis" becomes so dangerous and pressing that it is likely to lead to MAD (mutually assured destruction), which is reminiscent of the Cold War.

Nowadays, the pressing and highly dangerous security challenges are global and largely technologically-based: (1) military "hardware" of mass destruction held by states (as in the Cold War) and non-state terrorist organizations; and (2) cyberattack capabilities held by states and individuals for the purposes of mass destruction and/or ransom. In such a situation, leaders in Japan and elsewhere might, nay should, "turn the crisis on its head," so to speak, and cooperate in taking measures to avoid MAD.

Finally, an afterthought with a question mark: It might be useful to apply the so-called "garbage can theory" of public policy change, especially with its argument that solutions define problems, and not the other way around. For example, Japan's adherence to the US-Japan alliance, a solution for Japan, defines new Chinese initiatives (say China's One Border One Road (OBOR) and Asian Infrastructure and Investment Bank (AIIB)) as problems rather than opportunities. I have yet to think about this possibility more deeply, so I leave it with a question mark for future research.

Overcoming Security Isolationism: Japan's Promotion of East Asian Security Multilateralism Since 1991

Paul Midford, Norwegian University of Science and Technology

This paper asks why Japan pursued regional security isolationism during the Cold War, and why it then suddenly ended this isolationism on the cusp of the Cold War's end, embracing regional security multilateralism through the July 1991 Nakayama proposal. This talk focuses on the Nakayama proposal, and the resulting legacy of more than a quarter century since then of Japanese leadership in promoting regional security multilateralism. Japan's initial sudden leadership attempt, in the form of the proposal by Foreign Minister Nakayama Tarō, made at the ASEAN Post Ministerial Conference (PMC), and several additional proposals by Prime Minister Miyazawa Kiichi (one made before the Washington Foreign Press Club in July 1992, another at a CSIS Councilors meeting in Tokyo in October 1992, and a third during a major policy address in Bangkok in January 1993), played a crucial role in introducing regional security multilateralism into East Asia through the establishment of the ASEAN Regional Forum (ARF) in 1994, the first regional multilateral security forum. Japan's consistent championing of regional security multilateralism thereafter also played a crucial role by building on the ARF to create other multilateral security institutions in East Asia. These institutions include the Northeast Asian Cooperation (NEA 3) in 2003, the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) in 2004, the ASEAN Defense Ministers Meeting Plus Dialogue Partners (ADMM Plus) in 2010, and the East Asian Maritime Forum in 2012.

This paper identifies several challenges that Japan's pivot away from security isolationism and toward security engagement and leadership in promoting regional security multilateralism was designed to address. First, in terms of overcoming Japan's postwar reputational problem, the reassurance imperative is the most important factor explaining both Japan's security isolationism during the Cold War and its subsequent active promotion of regional security multilateralism since 1991. By working through regional multilateral security institutions Japan has been able to play a significant direct role in regional security, while simultaneously reassuring other East Asian states that Japan would not again reemerge as a military threat.

This presentation also identifies two other motivations for promoting regional security multilateralism. First, Japan has been able to use security multilateralism to help mitigate its alliance security dilemma of entrapment versus abandonment vis-à-vis the US. Regional security multilateral institutions such as the ARF and the ADMM Plus have in fact played an important role in maintaining US engagement, by attracting annual (or twice annual) visits by US secretaries of state and defense to the region to participate in these meetings, visits that help maintain elite attention focused on East Asian security and help socialize the US to regional security perceptions and culture. Second, Tokyo has used security multilateralism to build new security utilities not provided by the US-Japan alliance in non-traditional security areas. These include developing means for counter-piracy, counter-terrorism, countering drug trafficking, human smuggling, etc., and further developing capabilities for humanitarian and disaster relief operations (HaDR).

Closing the Gaps: Transnational Policy Networks in the US-Japan Alliance

Yiftach Raphael Govreen, The Hebrew University of Jerusalem

Within the context of this conference, the contribution of this paper lies in its focus on the role played by networks within bilateral relations in the management of alliances. It builds on a growing recent body of literature on networks in IR. In the presentation, I focused on the roles of transnational policy networks (TPNs) in bilateral security relations. These networks influence bilateral security policy-making in two ways. One concerns the actual negotiation of bilateral security agreements, using its superior position as a bridge between the decision makers of the two states as a mediating tool for sensitive issues. The other concerns their long-term influence on the perception of the governments on security issues, thus promoting greater congruence and bringing the two states closer to making an agreement on the issue.

I demonstrate the role of TPNs in the creation of the agreement to relocate the Futenma Marine Corps Air Station. This large base is located in the middle of a crowded city on the island of Okinawa, and has been a source of hazard and public unrest for many years. The negotiations on the agreement to move the base started in a disadvantageous position, and were not likely to succeed amid political strife and a period of change in the US-Japan relationship. This case shows that TPNs are a facilitator for an effective mediation mechanism. A well-positioned TPN minimizes zero-sum negotiations between the two states. It offers more transparency between the actors involved, but with less accountability, enabling more flexibility and creativity with policy planning. The positioning, then, allows these plans to go up the chain to the actual policy makers.

While the idea to explore the issue of returning Futenma to Japan was raised and promoted by the highest echelons of both states, most notably Hashimoto Ryutaro, the Prime Minister of Japan, the actual negotiations on the issue were conducted unofficially by lower level officials, without the knowledge of some of their superiors. This group of actors, from both states, formed a transnational policy network, which strived towards a joint goal in an attempt to make the alliance better and stronger, transcending narrow national interests.

The success of the network, demonstrated by the inclusion of the return of Futenma in the official Special Action Committee on Okinawa (SACO) agreement, was possible due to several conditions. The first factor which enabled the conclusion of the agreement was the secretive nature of the negotiations. This enabled the actors of the network to work without the interference of outside sources and interest, and reduced pressures from other actors, especially those from outside the security sphere.

Second was the support of both governments on the issue. This support, or “shadow of hierarchy,” gave the negotiators a better starting point on the issue and created an atmosphere of a joint goal, rather than a zero-sum game. The unofficial status of the negotiations within the network meant that there was less accountability if things failed, enabling the process of negotiations to be more flexible and creative in the possible solutions.

Finally, and most critically, the connections of the network’s actors to high officials in both states was a key element in their ability to move the negotiations to an official status and include them in a bilateral agreement. The core capital of network theories is the position of actors within the network, and this work builds on them. The beneficial position of the actors, as seen through their close connections to high-ranking decision makers on the one hand, and their role as a bridge between the

two states on the other, puts this TPN in an ideal position to affect bilateral security agreements. By utilizing these advantages of policy networks, they succeeded in forming a bilateral agreement on the very sensitive issue of returning Futenma to Japan.

Looking forward, the challenges facing the US-Japan alliance have changed over the years. Some of them are characteristic of the relationship from its onset, while others are relatively new.

US President Trump, promoting a discussion of an isolationist US, creates a challenge for Japan. While the Abe administration has managed to create a good relationship between the two, the unexpected nature of the American president keeps those in charge of the alliance on their toes.

The Japanese reliance on the alliance for security continues the perception that it constantly needs to balance abandonment of the US on the one hand and the risk of entanglement in US wars on the other. This is one of the oldest of Japan's concerns in this relationship. An isolationist US reduces the danger of entanglement, but also feeds the Japanese fear of abandonment.

Beyond the need to maintain a strong relationship, the alliance needs to cope with the threats from Japan's neighbors. The rising Chinese dominance in the East Asian sphere and its growing assertiveness for promoting its goals pose a real challenge for both the US and Japan as individual states and as part of the alliance. The need to project power on the one hand, while not creating a perception of threat within China is a delicate balance, which is not easy to maintain. The North Korean threat is even more eminent, with the US taking a very assertive stance against the leadership.

Proper use of TPNs can reduce tensions and create a closer mind-set between the two allied states. The US and Japanese willingness to improve the relationship can pave the way for the creation of preferable conditions for the work of TPNs. Most importantly, among these conditions is to enable the creation of networks with links to policy makers, in order for them to make an impact on the bilateral relationship.

Regardless of whether TPNs will be used or not, there is no doubt that the ways by which the two states will face these challenges and the means by which they will use the many tools of the alliance to cope with them will affect the direction the relationship will take for years to come.

Panel II: China and East Asia's Regional Security

Rethinking China and International Order: A Conceptual Analysis

Kai He and Huiyun Feng, Griffith University

The rise of China is one of the most defining political events in world politics in the 21st century. Since the 2008 global financial crisis, Chinese foreign policy has become more assertive, as seen from its behavior in the South and East China Seas. In the next decade or two, China's challenges to the existing international order seem inevitable in all aspects. Meanwhile, the Trump presidency in the United States seems to be putting the existing international order at stake by withdrawing from the Trans-Pacific Partnership (TPP), the Paris Climate Accord, and most recently, the United Nations

Educational, Scientific, and Cultural Organization (UNESCO). Interestingly, according to Xi Jinping's Davos speech, China seems to seek leadership in promoting globalization and even protecting the existing international order. Will China be a challenger or a protector of the international order? Will the United States give up its leadership in globalization? Is the liberal international order over with Trump's "America first" presidency? Understanding the new dynamics among China, the United States, and the international order has become an imperative task for both policy makers and academic scholars in Asia Pacific.

Despite the heated debates over China's challenges to the international order and its implications for world politics since the end of the Cold War, scholars seem to talk past each other because of the contestation over the definition of "international order" and the lack of theorization of the mechanism of "order transition" in world politics. For example, while power transition theorists and offensive realists argue that China is a revisionist state aiming to overthrow the current international order, some liberals suggest that China has no reason to do so because it is the largest beneficiary of the current international order. While both arguments seem reasonable and logical, they come to completely different explanations and predictions about the rise of China. The major reason for these two distinct views lies in their different conceptualizations of "international order." While realists use the distribution of capabilities, especially military power, to define "international order," liberals treat the prevailing rules and institutions as the essence of "international order." Although both seem right when sticking to their own definition of "international order," the debate between them becomes fruitless and even confusing due to their different focus on international order.

In addition, there is no doubt that the rise of China will become a challenge to the international order, no matter how we define it; nevertheless, how China will challenge the international order remains unknown. If China uses military means to overthrow the current international order as Germany and Japan did before World War II, which follows the power transition theory, then military conflict between China and the United States might be unavoidable. However, if China relies on multilateral institutions and non-military strategies to challenge some components of the international order, it might not cause conflicts and wars. In other words, what China will do matters for the future of international order.

We engage the China debate from a conceptual and theoretical perspective. First, we suggest three weaknesses in the existing literature: the conflated concept of international order, the less-theorized framework of "order transition," and the oversimplified relations between China and international order. Second, we introduce an integrated definition of international order. Through stratification and categorization, we discuss the three levels of international order: norm-based order, power-based order, and rule-based order, as well as three domains of international order: security order, political order, and economic order. Third, through integrating Gilpin's argument of change in world politics, we discuss three types of "order transition" in world politics: systems transition of normative order, systemic transition of power-based order, and institutional transition of rule-based order. Last, based on our typology of international order in a 3 x 3 matrix crossing the three levels and three domains, we typologize nine dimensions of international order in Asia Pacific.

We conclude that the rise of China will inevitably alter the current international order. Three types of order transition are associated with these three levels of international order. The normative order change will lead to "systems change" in world politics. The power-based order transition will cause "systemic change" among states. The transition of rules-based order is the most dynamic and complicated "interaction change" of world politics.

Through briefly examining the major features of these nine dimensions as well as their relations with China's foreign policy, we argue that China's challenge to the current international order is still limited to the rules-based economic order. China is a strong supporter of the norm-based order, which mainly features Westphalian principles and liberalism in economic development. In the power-based order, China has the potential to challenge US domination, but it has to manage the political influence of other middle and small powers, especially in the political and economic domains.

In conclusion, we suggest that the multidimensional feature of international order technically strengthens the sustainability and resilience of the current international order. China will play multiple roles at the same time – as supporter, reformer, and challenger – in shaping the current international order. More importantly, China's approach to international order should not be seen in isolation. Instead, it is a strategic interaction between China and the outside world. If the outside world, especially the United States, can accommodate China's rise, instead of forcefully containing or denying it, China's challenges to the international order will be well channeled and constrained. It is still too early to predict an inevitable conflict between China and the United States, because the order is too complicated to change and the future of China's rise is still unwritten rather than destined for war.

Institutional Statecraft with 'Chinese Characteristics': The Asian Infrastructure Investment Bank as a Case in Point

Doron Ella, The Hebrew University of Jerusalem

This paper aims to explore what characterizes China's approach towards institutional building in terms of process and design, and how it is distinguished from the manner in which other states, particularly the United States, have approached this issue. Putting special emphasis on the institutional design of multilateral development banks (MDBs), and particularly on the design of the Asian Infrastructure Investment Bank (AIIB), I argue that China is willing to adopt certain institutional design features that it considers as efficient and legitimate from existing MDBs, such as the World Bank (WB) and the Asian Development Bank (ADB), while it also modifies and introduces new features that are consistent with its current interests and normative agenda.

When China established the AIIB, it recognized that it should invest in its performance as a sound financial institution that is both legitimate and efficient. Thus, it included design features that are similar, and sometimes identical, to those that exist and have proved adequate in other MDBs. These include aspects regarding membership and voting rules, subscription allocation, and certain flexibility and enforcement mechanisms. However, China decided to differentiate the AIIB from other MDBs by including modified design features that are intended to advance its interests through the bank's purpose and operations. These include aspects of institutional control, such as having de-facto veto power in certain decisions made by the Board of Governors and Board of Directors, and limiting some of the bank's flexibility provisions. Additionally, China implemented several unique design features that reflect its normative agenda. These include aspects regarding the conditionality of loans, categorization of member states, operation methods of the Board of Directors, and planning and implementation processes of projects. In short, in designing the AIIB, China carried out a "pick and choose" approach, while also showcasing an exercise in institutional innovation.

This paper aims to investigate this dual approach and illustrate how China is forming its own particular way of advancing its interests and spreading its norms through international institutions.

Since President Xi Jinping came to power, China has become more involved in "institutional statecraft," and it did so by advancing the establishment of new economic initiatives, with the goal of modifying and, some would even argue, transforming the current global financial order, which is led by the US and ruled by Western liberal norms (Ikenberry and Lim 2017). It is argued that due to its frustration with US reluctance to grant it more power over decision-making in the International Monetary Fund (IMF) and the World Bank (WB), China decided to try and replace US economic leadership, at least in Asia, where it perceives itself as the most important stakeholder. Already in 1981, Kindleberger argued that the US had resigned or was discharged as leader of the world economy. Although at that time there was no worthy candidate to take its place, today, China signals a growing willingness to replace the US as this leader. China is doing this by establishing new initiatives to rival the Bretton Woods institutions that will accommodate its growing weight in the global economy (Callaghan and Hubbard 2016; Chin 2016; Hai 2016). Therefore, examining how China is designing new international institutions under its leadership is of special importance to the study of current global affairs.

For the purpose of empirically analyzing this paper's argument, a comparison is made between the newly Chinese-established AIIB with the WB and the ADB, emphasizing key patterns of similarity and difference. These MDBs are similar in many aspects, including their general agenda and their declared financial and development goals. However, they also differ in several aspects, including institutional control, as illustrated through the distribution of voting power between members, the allocation of shares, and in regard to the decision-making processes within the Board of Directors. These banks also differ in terms of membership rules and aspects of institutional flexibility, as they apply different categorization mechanisms that generate distinctive practical consequences for their participant member states. Therefore, investigating the factors behind China's decision to differentiate the AIIB from other MDBs in certain design aspects, while adopting other aspects as it sees fit, might shed light on how China currently perceives the role of international and regional institutions and its position in them.

Panel III: Maritime Conflicts and North Korea's Nuclear Dilemma

Gray Zone Conflicts in Maritime Asia

Tetsuo Kotani, Japan Institute of International Affairs

Upholding the rule of law in the East and South China Seas is essential for the stability of East Asia. In reality, however, there is no consensus on the legal basis for maritime boundaries in postwar Asia. There is little incentive for the peaceful resolution of maritime disputes among the regional countries, either. The United States has maintained regional stability by its military power, but the ongoing power shift is changing the regional power balance. As a result, Asia views maritime conflicts and China as the center of these conflicts. However, China has become skilled at operating below the threshold of military conflict by using fishing fleets, coast guard, maritime militia, military ISR activities and exercises, and offshore facilities and platforms.

China attempts to create a “new normal” in the East China Sea by gray zone coercion, while carefully preventing US military intervention under the US-Japan alliance. The situation surrounding the Senkaku Islands is managed by Japan’s own forces (coast guard buildup, military ISR) and a strengthened US-Japan alliance. However, if intrusions into Japanese territorial waters by Chinese fishing boats and civilian and military vessels continue, Tokyo will face pressure to respond with stronger law enforcement countermeasures. In the process, it will have to walk a delicate line to maintain overall military superiority, respond effectively, and control escalation risks.

The situation in the South China Sea remains complex and difficult to manage because the military balance favors China there. Construction on the Spratly Islands and the expansion of facilities in the Paracel Islands by China further shifted the military balance in Beijing’s favor. In fact, the gray zones in the South China Sea remain darker and thicker than those in the East China Sea, but other claimant states and ASEAN have not come up with unified countermeasures to China’s gray zone tactics even after the UNCLOS arbitration ruled that China’s claims and activities in the South China Sea are illegal or groundless. Further militarization of the South China Sea will make it more difficult for the United States to intervene in military conflicts there.

Ultimately, regional actors must formulate more effective responses to Chinese gray zone coercion by reinforcing efforts at internal and external balancing while promoting the rule of law and peaceful dispute settlement. Otherwise, China is intent on reshaping the international rules for trade and security in ways that favor China in pursuit of a Pax Sinica hierarchical regional order with Beijing at the apex.

North Korea's Nuclear Threat: A Regional Perspective

Alon Levkowitz, Beit Berl and Bar Ilan University

North Korea, under the leadership of Kim Jong-un, invested an enormous amount of the national budget and manpower in developing a credible nuclear deterrence vis-à-vis the United States. Pyongyang's final goal was achieved when it launched an Intercontinental Ballistic Missile (ICBM) with a nuclear warhead in early January 2018, overcoming most of the technical issues in a relatively short time. Although the intelligence communities and analysts around the world raise questions about the accuracy of the missile and the re-entry vehicle, from Kim Jong-un's point of view, the credible deterrence was achieved, even if Washington questions it. Kim Jong-un is now challenging the US’s commitment to its Asian allies. The discussions in Japan and South Korea about Washington's willingness to go to war if Pyongyang threatens the East and West Coast of the US raises doubts about the solidness of the US’s commitment. However, under President Trump, the biggest concern in Seoul and Tokyo is that he might initiate a preemptive strike on the Democratic People's Republic of Korea (DPRK) without getting Japan and South Korea's approval.

North Korea has built a very impressive missile industry. The number and variety of missiles that they have developed in the last decade raises questions about the amount of effort they invest in this industry and from where they get the funding and the technological assistance. In order to get more funding for its missile industry, will North Korea increase its missile export to the Middle East and Africa? Or will it start selling missiles to terrorist organizations?

Throughout the years there have been bilateral and multilateral attempts to solve the North Korean missile and nuclear issue. South Korea, under Kim Dae-jung, tried to pursue a liberal economic policy – "The Sunshine Policy." The logic of this policy was to improve the economic relations between North and South Korea in order to increase the economic benefits that Pyongyang would gain from economic cooperation with Seoul. Seoul hoped that Pyongyang's economic incentive would decrease North Korea's incentives to increase military tension in the Korean Peninsula. President Kim Dae-jung had to convince President George W. Bush to support his Sunshine Policy, since the president supported a more hawkish policy towards the DPRK and was not willing to support a policy that would assist Pyongyang's economy.

Another two multilateral mechanisms that were implemented in order to deal with the North Korean issue were the Six-Party Talks and the sanctions implemented by the United Nations Security Council (UNSC). Both mechanisms failed to prevent North Korea from developing long-range missiles and nuclear capabilities. One could say that North Korea was able to maximize the pitfalls of the multilateral mechanism in order to gain time to develop the military capabilities and decrease the sanctions that were imposed on Pyongyang.

President Lee Myung-bak and President Park Geun-hye decided not to pursue the Sunshine Policy towards the DPRK, but instead, decided to pursue a more aggressive policy towards Pyongyang. Despite that, both failed to halt the development of the North Korean missile and nuclear program.

In President Moon Jae-in's pursuit to revise the Sunshine Policy towards the DRPK, he faces a few obstacles:

The tension with China – China opposed the deployment of the US THAAD system in South Korea. Beijing began to impose unofficial sanctions on Seoul in order to convince it to change its policy. President Moon has tried, since his election, to convince Beijing to ease the sanctions.

US new policy – President Trump does not support an appeasement policy towards the DPRK, but wants to increase the sanctions on the DPRK, which may contradict President Moon's policy. President Moon tried to convince Washington not to initiate any military attack on the DPRK in order to allow them to participate in the Winter Olympics.

North Korea – While President Moon might be seen as the most favorable towards North Korea, Kim Jung-un has not responded to any gesture offered by President Moon. Kim is focusing on President Trump, believing that South Korea does not have any leverage on Washington. The beginning of 2018 symbolized the shift towards the South. Once Pyongyang achieved the ICBM goal it was willing to accept Seoul's offers because it served its interests.

The 2018 Winter Olympics served both leaders. Kim Jong-un saw the Winter Olympics as potential for decreasing the sanctions on North Korea without giving up its nuclear or missile capabilities. Kim is willing to offer a "smiling diplomacy" that will gain public support. President Moon hopes that the Winter Olympics was the beginning of a new change in North-South relations. The optimists hope that this will bring the change, while the pessimists think that after the Olympics Pyongyang will return to developing its nuclear and missile capabilities.

Four Paths to 'Strategic Miscalculation' over North Korea

Or Rabinowitz, The Hebrew University of Jerusalem

On September 25, North Korea's foreign minister declared that Pyongyang sees Trump's actions as a declaration of war, and threatened to shoot down US strategic bombers in international airspace. The intensifying crisis surrounding the North Korean weapons program makes the risk of a strategic miscalculation, a situation in which one side misinterprets an action by its rival as a first step towards war, higher than ever before.

Here are four potential paths to miscalculations of varying degrees. All are avoidable.

(1) North Korea could detonate a hydrogen bomb in the Pacific. Kim Jong-un has threatened to test a hydrogen bomb as the next step in his nuclear strategy. South Africa in the 1980s had a similar idea, without the showstopper H-bomb, but the circumstances were somewhat different and the strategy was kept secret.

South Africa had developed a rudimentary nuclear arsenal, fabricating 6½ enriched uranium bombs by 1989. The South African strategy was to try and coerce Washington to come to its aid, should pro-Soviet forces invade it from the north. The strategy was never tested, as President F.W. de Klerk ended the South African nuclear program upon taking office in 1989. But critics of the plan point out that a South African nuclear test might have had the opposite effect at the time, further antagonizing the Reagan administration and expanding the existing rift between Pretoria and Washington over South Africa's apartheid regime.

What would a North Korean H-bomb test lead to? Instead of deterring the United States, it might just be the tipping point leading to a US first strike against North Korea.

(2) Trump's aggressive rhetoric could set him apart from past US leaders. Previous administrations failed to curtail North Korea's nuclear program, passing this "hot potato" down to the Trump administration. But Trump's use of inflammatory rhetoric has emerged as a serious independent concern.

A recent strand of nuclear proliferation studies looks at the importance of a leader's personality, identity, perception, and world view, underlining the importance of a leader's psychological make-up. This type of provocative and aggressive talk may work on the campaign trail, but can be particularly dangerous in the realm of nuclear diplomacy, especially when Trump hurls insults at the "famously thin-skinned" Kim Jong-un. The North Koreans simply "don't get" Trump and are trying to "make sense" of his statements. The danger is that North Korea could misinterpret Trump's statements as an impending first strike.

The importance of beliefs and perceptions is also salient when considering Trump's position and tough talk on another nuclear issue: the Iran nuclear deal. Despite reports that Iran is not in "material breach" of the agreement, Trump's preconceived beliefs about the agreement greatly impact his policy towards it. Trump seems to think that the agreement should be undermined or terminated despite evidence that it is achieving its goal of inhibiting the Iranian nuclear program.

(3) The US could try – and fail – to shoot down North Korean missiles. Since the 1980s, the US has spent about US$ 200 billion on developing the technological capability to shoot down ballistic

missiles. This effort has produced different systems for different missiles, including the Ground-based Midcourse Defense (GMD) interceptors, developed to shoot down incoming intercontinental ballistic missiles (ICBMs); and the Aegis and THAAD systems, developed to shoot down shorter-range missiles. But shooting down missiles is hard to do, and the GMD interceptors are relatively inaccurate.

The THAAD and the Aegis systems have a better test record than the GMD interceptors, but none of the three has been actively used in an actual war. In theory, the US could use the THAAD and Aegis systems to shoot down North Korean "demonstration" missiles launched over the Pacific. But if the interception fails, it could damage US status, causing its allies to lose faith in US security promises, and perhaps lead to new challenges from rivals. Such a failure could also lead to a miscalculation on North Korea's side, if Pyongyang wrongly assumed that the interception was an act of war.

(4) The global media may miss important nuances in North Korean statements. North Korean statements have a particular internal logic of their own, which outsiders tend to miss completely.

In early August 2017, North Korea stated that it was "carefully examining the operational plan for making an enveloping fire in the areas around Guam." Analysts interpreted this as a threat to launch missiles around Guam, targeting the international water surrounding the island.

This threat was bad enough, but the North Koreans were not, in fact, threatening to hit the island itself. Global media reports, however, depicted the North Koreans as threatening the island itself. The difference between the two scenarios is rather acute: one entails North Korean missiles falling outside US territory, and the other depicts them hitting Guam directly.

What is important is that administration officials are getting it right, even if the media don't account for these important nuances. Public concern will not lead to a strategic miscalculation on the part of the US, though it may impact the crisis in two other opposing ways: It can enhance the pressure on the White House to react to further North Korean provocation; or, more likely, it can increase the pressure to find a diplomatic solution.

The more concerning question is whether the Trump administration and the understaffed State Department are equipped to handle the North Korean crisis. US officials are by now skilled at unpacking "Pyongyang speak." Senior officials, like Defense Secretary Jim Mattis and Secretary of State Rex Tillerson, repeatedly stress the focus on diplomatic and economic pressure, rather than the military option, but is this enough to de-escalate the current crisis?

Words alone are not likely to trigger a nuclear exchange, but they can surely lead to further escalation, as we are witnessing now. Each of these four paths is a mere possibility, and none are particularly likely to occur. The North Koreans probably realize that detonating a thermo-nuclear device in the Pacific could lead to war and take Trump's aggressive rhetoric with some grains of salt (despite Pyongyang's declarations to the opposite).

Even if the US tries and fails to shoot down a North Korean missile, war will not automatically break out. But it might, and all these paths underline the importance of prudence and diplomacy and the need for balanced, far-seeing statesmanship. The question is, can Trump and Kim Jong-un deliver the goods?

Panel IV: Cybersecurity and Regional Security – Lessons from East Asia and the Middle East

This panel was organized in collaboration with HUJI Cybersecurity Research Center

(H-CSRC) – Cyber Law Program

Key Elements Governing Cyberspace and the Security Environment in Japan and Beyond

Dai Mochinaga, Mitsubishi Research Institute

Connected information infrastructure promotes economic developments, but, at the same time, incidents could spread across other sectors and states because of their high interdependence. Events in cyberspace are changing the ways in which states, organizations, and individuals interact. Organizations and individuals will be a part of the main political entities in international relations after cyberspace is widespread. Cyberspace affects not only nation-states, but also organizations and individuals. Conflicts between states and multinational IT corporations, secret leakages by individuals, and interference in elections shows a transition of key players.

Cyberspace consists of computers, networks, and digital signals, and the traffic concentration to developed countries shows a correlation between cyberspace and geographical condition. In addition, computers transfer, duplicate, and compile digital signals with little geographical constraint. Geopolitics has studied the impact of geography on international politics and international relations, providing analysis on the power of nation-states with the assumption that organizations and individuals are under the power of nation-states. However, organizations and individuals have become key elements in cyberspace, since they have acquired the capability to directly influence other nation-states, organizations or individuals. For example, Google is more powerful than a small country in terms of the number of users or GDP, and there are disputes with nation-states regarding tax avoidance.

The Impact and Source of Cyber Threats

The major source of the cyber threats has shifted from individuals to nation-states. Until the early 21st century, the major source of the threat in cyberspace was from individuals called "script kiddies," who were motivated by the desire to show off their skills to disrupt things. In the late 2000s, the source shifted to organizations because their motivation for a cyberattack changed to a pursuit of economic gain. The return on investment in cybercrime in 2014 is estimated to be 1425%, so the outcome of a cyberattack is regarded as a financial source for crime organizations.

After 2010, nation-states became part of the cyber threat source with a purpose to not only steal information, but also to disrupt computer systems within a critical infrastructure that includes power plants, water facilities, and railways. The most remarkable cyber threat is attacking political systems with propaganda sponsored by nation-states.

Japanese cybersecurity environment and challenges

Japan is one of the targets of cyberattacks. Incidents in Japan show that attackers carefully choose targets which hold precious information. For example, the Japan pension service was attacked,

resulting in about 1.25 million personal data leaks. In another case, defense-related companies were also targets of cyberattacks. Since their intellectual property is highly valued by other countries, they can take advantage of any vulnerability discovered in high-tech defense equipment.

To handle cybersecurity issues, the Japanese government established the National Information Security Center (NISC) under the cabinet secretariat in 2005. They developed a fundamental strategy on national cybersecurity, establishing a government-wide framework for information security, and an action plan for critical infrastructures. They also promote comprehensive measures taken by central governments.

In 2014, the National Diet passed the basic act on cybersecurity. The act describes the basic principles of national cybersecurity policy and clarifies the responsibilities of the national government, local governments, and other concerned public parties. It also declared the establishment of the Cybersecurity Strategic Headquarters and the reorganization of the NISC to become the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), under direct control of the cabinet. The NISC's new powers include conducting investigations into the cause of serious incidents, requesting mandatory reports from other governmental bodies, and sending formal recommendations to other governmental bodies.

Cybersecurity in Japan consists of a basic strategy and other policies including critical infrastructure protection and technical standards for central government computer systems. The cybersecurity strategic headquarters released a fundamental "Cybersecurity Strategy" in September 2015, which describes the basic principles of cybersecurity issues and the direction of policies until FY2017. The new strategy will be released in 2018. According to the cybersecurity strategic headquarters, the principles for the next cybersecurity strategy will be: (1) future roadmap and threat prediction; (2) toward Tokyo Olympics 2020 and beyond; and (3) identifying issues and deploying solutions.

One of the challenges for Japan is communication with foreign countries. There are plenty of engineers engaged in cybersecurity but not all them have the ability or willingness to communicate in English. It is now a serious issue for operators and engineers to promote cooperation between other organizations overseas.

Another challenge is the lack of knowledge among government senior officials, some of whom believe issues on cyberspace should be handled by technological specialists. However, a nuclear strategy can be created without being a nuclear physicist, because knowledge of physics makes almost no difference in how nuclear weapons are deployed and used. But this is not true in cybersecurity. What can and cannot be done and what strategy is created requires a great deal of technological understanding.

Analytical framework for controlling cyberspace

This paper proposes a new analytical framework that describes the factors controlling cyberspace. The new framework will help to understand the transition of international relations in cyberspace, and will identify the factors that control cyberspace and who can influence those factors. The factors in this framework consist of: (1) technology, (2) policy/industry, and (3) numbers (data, user, market). These factors have a mutually complementary relationship and the key elements (nation states, organizations, and individuals) have different capabilities which affect them.

Issues in cyberspace impact nation-states, organizations, and individuals. For example, sovereignty or norms in cyberspace are classic and current issues in international affairs between nation-states. Additionally, regulations and technological standardization in cyberspace involve nation-states and organizations, including private companies. For example, private companies research and develop technologies used in cyberspace and try to standardize them in the Internet Engineering Task Force. Privacy in cyberspace is one of the issues that has an impact on individuals. The general data protection directive (GDPR), which will come into effect from May 2018 in the EU, will regulate the personal data of all EU citizens. Therefore, issues in cyberspace have a broader impact not only on nation-states, but also on organizations and individuals.

Each factor in the framework has a different combination of key elements. The technology factor is based on the capabilities of individuals and organizations. The contributors of the policy/industry factor are organizations and nation-states. The relationship between the three key players is comprised of the number factor. These factors characterize a transition of international relations in cyberspace. In the 1990s, the US was the only nation with the capability to affect the controlling factors. Since 2000, the situation has changed from US domination to a multipolar system, and the new big player in all these factors is China.

Conclusion

In this paper, I introduce a Japanese cybersecurity environment and a new analytical framework in order to understand the transition of international relations in cyberspace. The new framework identifies the factors to control cyberspace, which show the transition of international relations in cyberspace and how the EU and China will have a great impact on the future of cyberspace.

Toward Actionable Intelligence of Private-Public-Partnership (PPP) in Improving Cybersecurity Forensic Investigation

Dayu Kao, College of Police Science and Technology, Taiwan

Digital forensic science provides scientifically proven methods that can be used to identify, collect, acquire, and preserve digital evidence. Law enforcement agencies (LEAs) need to explore the crime scene, gather digital data in different devices, and find actionable intelligence immediately. Decision makers in both LEAs and security agencies face a continuous need for actionable intelligence to be at hand in order to speed up the investigation or to increase the trustworthiness of relevant forensic findings.

Many international organizations or associations are collaborating and making efforts to combat cybercrime. LEAs are well advised to consider Private-Public-Partnership (PPP) to apply research to real life events for national security or cybercrime investigation. Actionable intelligence is related to the investigation or incident at hand within the wider intelligence mix. LEAs have produced actionable intelligence from criminal investigations to gain knowledge in support of preventing cybercrime or pursuing terrorists. The effectiveness and efficiency of LEAs can be judged in part by the capability to utilize their intelligence collection to access digital devices, support evidence gathering at a scene, collect volatile/non-volatile evidence in a lab, pursue a criminal immediately, and achieve successful prosecutions. The analysis of cybersecurity forensic investigation presents many opportunities for actionable intelligence to improve the quality and value of digital evidence.

The connections among terrorists, cybercriminals, and organized crime groups appear to be on the rise. A promising approach to ensure an efficient and effective strategy is collaborations between various private and public organizations. Security agencies, intelligence agencies, and LEAs can apply similar techniques to advance counter-terrorism measures to keep citizens safe, or to prevent, pursue, protect, and prepare against cybercrime or terrorism.

The Israeli Cybersecurity Innovation Ecosystem: The Case of the Beer-Sheva Cyber-Park

Amit Sheniak, The Hebrew University of Jerusalem

The enhanced innovation speed, the low price of cyber weapons, and the scarcity of a skilled workforce in the public sector has prevented countries from achieving a technological advantage through the traditional way of developing defense capabilities by government agencies, military industries, and intelligence communities. This has led governments to acknowledge the need to defend cyberspace and enhanced collaboration between themselves and the private actors such as universities, entrepreneurs, large corporations, and investors of risk capital.

Studying the policy of states to cultivate national cybersecurity innovation ecosystems is an attempt to connect between two different concepts that are derived from two distinct academic frameworks: (1) The notion of "ecosystems" originated from a business study and refers to different organizational mechanisms designed to transfer scientific knowledge to the industry and connect the "research economy" with the "market economy" (Jackson, 2011). (2) Cybersecurity policy is a new field of technological innovation, security policy, and military and intelligence doctrine whose goal is to foster the defense of different public and private organizations and institutions against computer communication enabled attacks and espionage.

In this paper the main research question examined the effect of cyber innovation ecosystems on the advancement of state power in the cyber-domain. I hypothesized that cyber innovation ecosystems have the potential to contribute to states' international standing in the cyber-domain in two main ways: (1) Advancing technological supremacy by decreasing innovation deficiencies; (2) Elevating international prestige and legitimacy. My research was based on a study of Israel's policy to promote a local cyber innovation ecosystem, focusing on the example of a cyber-park (Gav-Yam Park) in the city of Beer-Sheva.

Initiated in 2014, the park hosts a combination of private and public entities such as local and international high-tech companies, cybersecurity industries, cyber-defense operational units of the Israeli military (IDF) and intelligence agencies, Israel's National Cyber Event Readiness Team headquarters (IS-CERT), and the computer-engineering department of Ben-Gurion University. The Israeli government's decisions (Decision 546 of 2013 and Decision 1815 of 2014) to establish the cyber-park were part of the new Israeli cybersecurity policy that was initiated at the beginning of the decade to enhance the collaboration between the Israeli cybersecurity public sector and the local cybersecurity private sector, by establishing institutions such as the Israeli National Cyber Directorate (INCD) and developing long-term educational programs at both high school and academic levels. This policy signifies a change in the perception among Israeli officials, who were used to categorizing cybersecurity as an issue associated solely with security apparatus, government intelligence, and military institutions.

Therefore, I claim that the Israeli cyber-park can be described as an implementation of a few different ecosystems: (1) The "innovation ecosystem," aimed at promoting technology that will be used to mitigate new cyber-threats; (2) The "security ecosystem," aimed at improving the monitoring of and state responsibility for cyberattacks inflicted on the private sector; and (3) The "international cybersecurity ecosystem," aimed at enhancing the international collaboration between Israel and other like-minded states, while improving its international cyber posture and legitimacy.

This paper highlights the public statements by different professional and political figures who contributed to the construction of a national narrative based on the symbolic nature of the cyber-park, which is considered by many as the flagship of Israel's policy goal of becoming "one of the world's five leading forces in cyberspace." Overall, I stressed the park's importance as a social-political tool, used to reinstate legitimacy of Israel's current cybersecurity policy, while presenting the differences and similarities for other cyber innovation ecosystem policies around the globe.

I concluded with a call for the advancement of more cybersecurity research, which will focus on the soft power dimensions of cybersecurity policy, such as the ties between the private and public sector as a component in the state's ability today to achieve "cyber-dominance." Specifically, I call for comparable research that will lead to a typology of different kinds of cybersecurity ecosystems, as some states focus on innovative R&D, while others cultivate international ties. This call is based on my view, which was forged in accordance with my academic and professional experience, that a better understanding of these dimensions might improve cybersecurity strategy and policy formation.

Geography Matters: Spatial Dimensions in System Trespassing Incidents

Tamar Berenblum, The Hebrew University of Jerusalem

This presentation will focus on the spatial context of hacking while discussing the findings from two research projects and data collected in China and Israel. The investigation focuses on the relationship between topological positions and geographic positions of victimized computers and system trespassers.

The findings support the idea that geography matters. Drawing on the routine activities perspective, the research has found that victim client computers have a role in determining the geographical origins and temporal trends of the attack. Moreover, exploring the hacking network reveals that geography has an effect on the behavior of the attackers as well as the topology of hacking networks. The implications for cyber-criminological theory and research as well as its implications for the ability to assist policymakers in forming effective policies will be discussed.

Public Privacy: The Balance between Freedom and Privacy in Cyberspace

Anja Mihr, Humboldt-Viadrina Governance Platform, Berlin

Public policy for cyberspace is the latest of many claims to govern, manage, regulate or organize the endless and mostly anonymous spheres of cyberspace and the Internet. But how should a space with half the world's population, that is to say around 4 billion 'inhabitants' or users, be governed? Also,

bear in mind that most of those users have no positive experience with the rule of law abating state practice or the public participation mechanism. Whether all governments or multi-stakeholders confirm and rephrase that the international human rights regime, as we know it today, with its multiple human rights norms, standards, and mechanisms, will apply online as well as offline has not made much progress in fostering or protecting the human rights of all of us users thus far.

The existing concept of a human rights-based global public policy might be a way out of the deadlock of multi-stakeholder cyber governance talk. Cyber public policy is based on an agenda and an implementation process that involves private, state as well as non-state actors, irrespective of where they are located or which citizenship they obtain. Migrants, refugees, citizens, companies, and governments alike have the same access to the Internet and share similar responsibilities, and thus can be held accountable, irrespective of their status. This sounds idealistic, but not impossible.

The legal and political framework of cyber public policy is the international human rights law, including the norms of customary international law, which does not need a nation or a state, whether corrupt or democratic, to be valid. It applies to state and non-state institutions, to users, governments, and companies alike. The UN human rights framework as well as the hundreds of regional human rights treaties, such as the European Convention on Cyber Crimes or the UN's Guiding Principles for Business and Human Rights, can all be applied anywhere in the world when protecting human rights, such as the right to human security and privacy, that of freedom of participation and expression, of professional development or education based on gender equity, and access to information or development.

Yet, cyberspace is a borderless public space in which the Internet is a network and a tool that allows different digital devices to connect and communicate. Cyberspace has increasingly been converted into 'one space' in which we move, an online and an offline space at the same time. Therefore, we do not need a new set of specific human rights standards, since the ones we have still apply and can be implemented. However, the main difference between the offline and online space and world in which we move, live, and work is that the online space lacks the justiciability and liability of the actors and institutions that provide the online services that we use. Whereas there is no longer a controversy on whether human rights are valid norms offline as well as online, the controversy now is around the way, the means, and the litigability of these norms and standards when using the Internet and the services it provides. Thus, a global agreement on the procedures of cyber public policy is still to come about, but it does not need a de facto treaty or government-based agreement. Rather, it can be informally agreed upon by the different state and non-state actors and agencies, users, and companies alike, and put into practice.

There is little to no dispute about the fact that national governments, international organizations such as the UN, or regional organizations such as the European Union (EU) or the Organization for American States (OAS) alone cannot safeguard these rights, let alone enforce or protect them. The solution must be a global, transnational governance regime based on human rights norms, good governance and multi-stakeholder principles that involve local, that is to say "server-located," entities that adhere and enforce these standards and protect users' human rights.

Over the last few years, we cyber citizens or users have become more conscious of posting information and data online that might potentially be used against us in international or national law suits, as seen in recent court decisions in Europe, for example. Consequently, it is possible to manage the behavior and to establish a rule of law for cyberspace. The two main avenues to pursue are: (1) To establish a societal and legally binding "cyber constitution"; and (2) To establish global

enforcement and monitoring bodies, such as a global cyber court, multi-stakeholder committees or otherwise rotating, participatory, and transparent governance regimes. This cyber public policy regime would allow for collaborative work with national/domestic and local institutions, i.e. administrative or constitutional courts, NGOs, international organizations or public administrations, to implement and enforce the rights and duties of people moving in cyberspace.

Universal human rights norms and standards or customary international law is the already existing political and legal framework for this public policy regime. Through new technologies cyberspace offers an environment that consists of many participants who have the ability to affect and influence each other. This space is transparent and neutral in its nature but often corrupted, broadened, limited, or censored by the same people or governments who use it, but can, therefore, be held accountable for it too.

The "Internet citizen" space of 4 billion has a "birth rate" of over 30% per annum. If cyberspace were a country, it would be the largest and most populated in the world, albeit one without any constitutions or government, and with no legislative or otherwise democratic decision-making bodies. It has no police or law enforcement mechanism, let alone a protection mechanism for all Internet citizens to safeguard their human rights. Thus, the public policy regime, in which stakeholders govern, is a way out of this lawless situation.

We citizens or companies using the Internet and moving in cyberspace ought to set up common rules, regulations, and laws for users, even in social networks where we "meet" most frequently and which need the most regulation to protect our privacy and other human rights, such as Orkut, Bharatstudent, Renren or Facebook, Baidu or LinkedIn. The UN's Internet Governance Forum (IGF) claims to be finding multi-stakeholder-based global solutions, which include governments, CSOs, businesses, and service providers. Although this forum is still largely focused on security threats such as cyber war and cyber espionage, and thus, how to deal with and control these developments, it recently began to focus on how to uphold human rights online. But since the human rights-based approach in the offline world is still facing major challenges and obstacles, the online approach is too. Thus, the online world only mirrors our successes or failures to implement human rights in the offline world.

Panel VI: The Regional Implications of Great Power Competition

China and Japan's Economic Engagement in Southeast Asia: A Threat to Regional Security?

Raymond Yamamoto, Aarhus University

Until recently, Japan was the dominant actor promoting the growth in the region through bilateral official development assistance (ODA) and through its contribution to the Asian Development Bank (ADB) – a multilateral organization under the presidency of Japan. In 2013, Kitano Naohiro and Harada Yukinori from the Japan International Cooperation Agency Research Institute (JICA-RI) were one of the first researchers to quantify the amount of China's spending on the economic development of other countries. The analysis of Kitano and Harada revealed that China spent US$ 7.1 billion in 2013. Thus, Chinese "foreign aid" ranked sixth in the world in 2013, just behind the United States, Britain, Germany, Japan, and France (Kitano and Harada 2014, 10–11). Although the data was downwardly corrected by Kitano to US$ 5.4 billion in 2013 (adding that spending dropped slightly

to US$ 4.9 billion in 2014) (Kitano 2016, 17), there is little doubt that China is advancing to become the main infrastructure provider in Asia. Its changing position is revealed in the creation of the Asia Infrastructure and Investment Bank (AIIB) in 2016, the first Chinese multilateral development bank with capital of US$ 100 billion and the inclusion of an ambitious infrastructure project connecting Eurasia, labeled the One Belt One Road (OBOR) in the party's constitution in October 2017.

Interestingly, the territorial disputes in the region have been discussed in the context of China's growing infrastructure engagement in Southeast Asia. According to a *Financial Times* article from 2015, "China and Japan are stepping up their battle for strategic infrastructure projects in Southeast Asia amid rising economic competition and tensions over maritime disputes" (Financial Times 2015). The *Yomiuri* adds that China could use the AIIB to build infrastructure for China's People's Liberation Army (Yomiuri 2017, 243–44). Dennis D. Trinidad, a scholar from De La Salle University in the Philippines, believes that "aid has given China the luxury of enhancing its influence and an instrument to promote its strategic interests in East Asia and elsewhere" (Trinidad 2013, 26). In line with this argument, in 2014, Japan's former Vice Foreign Minister and ambassador in the United States, Sasae Kenichiro, accused Beijing of using "mercantile coercion" against neighboring states (Washington Post 2014). Numerous commentators, scholars, and politicians continually argue that China's infrastructure engagement in Southeast Asia poses a threat (Buszynski 2009; de Castro 2013; Chietigj 2016; Shoji 2009; Yoshimatsu 2010). They seem to share the conviction that Asia is entering a new stage of "Geopolitics of Infrastructure" (Trung-Minh 2017), thus reflecting reasoning which emphasizes China's strategy of "unrestricted warfare."

In his presentation, Yamamoto argued that the abovementioned realist views need to be carefully reconsidered for two reasons. The first argument is that most papers representing such views do not acknowledge similar interests of Japan and China. Both countries are primarily interested in supporting the economic growth of the region through economic infrastructure investments. The second factor that often leads to the overestimation of the donor is the perception of Southeast Asia as a passive playing field of external powers. Such views disregard the existing dyadic relationship of the region to Japan as well as China. Moreover, even though the presenter cannot deny that competition exists, he argues that it needs to be understood primarily in economic terms and as a factor resulting in increased efficiency of investments which bring benefits to all involved actors in the region.

Multi-Level Governance: US-ASEAN Counter-Terrorism Cooperation

Galia Press-Barnathan, The Hebrew University of Jerusalem

This paper relates to several central factors that shape both current challenges to East Asian security as well as the potential means of engaging them. More specifically, the paper deals with the challenge of terrorism, which is global, regional, and local, and the efforts at counter-terrorism cooperation. Conceptually, it points to the importance of understanding the interaction between regional states and extra-regional actors, namely the United States. Finally, it focuses on the important role of regional organizations like ASEAN in managing the regional security challenges and in facilitating interaction and cooperation between regional and extra-regional actors.

The paper examines post-9/11 interaction between the US and the Southeast Asian states on counter-terrorism (CT) cooperation. This case demonstrates the importance of a multi-level analysis in order

to understand the workings of regional governance, as well as to understand how the US participates in that process.

The 9/11 attack brought the issue of terror and counter-terrorism to the forefront, at least of the US agenda in its relations with SEA. In November 2001, ASEAN issued the ASEAN Declaration on Joint Action to Counter-Terrorism. This largely symbolic statement was followed in August 2002 with the ASEAN-US Joint Declaration for Cooperation to Combat International Terror. In May 2002, the Philippines, Indonesia, and Malaysia signed a trilateral Agreement on Information Exchange and Establishment of Communication Procedures – an agreement to which Thailand and Cambodia joined in 2003. Additional ad hoc cases, largely of intelligence cooperation, also occurred. In 2004, ASEAN members agreed to the Vientiane Action Program, which established a Mutual Legal Assistance Agreement (MLAA) in criminal matters relating to terrorism, a convention on counter-terrorism, and an ASEAN extradition treaty. In 2007, a landmark Convention on Counter-Terrorism was signed in the ASEAN annual meeting in the Philippines. It was a legally binding agreement that required ratification through national legislation, and that legally required all ASEAN members to adhere to the key international conventions established in the 1970s to thwart acts of terrorism, share early warning information with members on terrorist movements, strengthen the capability to deal with chemical-biological-radioactive-nuclear methods of terrorism, and establish a regional CT database with ASEAN oversight (ASEAN Convention on Counter-Terrorism 2007). The treaty was ratified by all member states by 2013. This is a historic development for ASEAN because it goes against both the great sensitivity in the region to any policies that may challenge the norm of non-intervention, and against the regional tendency to avoid highly legalized and formalized agreements.

US pressure and American conceptions of CT clearly played an important role, both in shaping the global normative framework (UN resolution 1373) and in shaping the agenda of regional discussions (largely in the ASEAN Regional Forum – ARF). However, the US failed in simply transporting its view of CT to the regional level. The US invested efforts to create legal-normative frameworks that would serve as guidelines in a coordinated CT struggle, and to promote specific practical policies. At the same time, regional states differed in their threat perceptions regarding terror, in their normative perspective about terror and CT, and in their capacity to deal with the threat. Consequently, an on-going negotiation, bargaining, and contestation process currently takes place among them through various channels.

The paper examines the global nesting of both American and Southeast Asian CT policies in UN resolutions. It then moves on to examine the CT interests and policies pursued by the US, and in turn, the domestic interpretations of individual states within Southeast Asia regarding the need for and desired nature of CT strategies. It then moves to examine the cross-level interactions surrounding CT, taking place within the ASEAN framework, and especially within the ASEAN Regional Forum (ARF), the one organization that brings together both the US and regional states. An examination of the discussions both at the regional level, within ASEAN (among regional states), and in the ARF and the ARF Inter-Sessional Meetings (ISM) on Counter-Terrorism and Transnational Crime (CTTC) (between regional states and the US and other external powers) revealed different opinions on how CT should be dealt with. Regional norms of non-intervention and comprehensive security, as well as regional domestic constraints, were central in understanding the reactions to American policies. Thus, for example, regional states were concerned about the military-oriented American approach to CT in the aftermath of 9/11, which initially showed complete disregard to the potentially dangerous

implications of such policies for human rights. For all ASEAN states, cooperating on CT was challenging given the dominance of the non-intervention norm. Furthermore, for some of the key regional states like Indonesia and the Philippines, "counter-terrorism" was not a matter of foreign policy as much as a central domestic political issue, since the identified terrorist groups were domestic groups challenging the regime itself. For them, counter-terrorism was counter-insurgency. Consequently, this led to different domestic sensitivities and constraints. These shared regional ideas and concerns were discussed and negotiated via regional ML institutions, leading to policies that reflected compromise.

The increased density of institutionalized interaction on issues related to CT, via the various regional and inter-regional forums, in official meetings, seminars, workshops etc., together with a growing number of examples of actual cooperation (among regional states, and between them and the US or Australia) suggest that American CT norms and practices are being partially localized into SEA, at both the regional and state levels. At the same time, the paper shows that the process of building and contesting the rules and policies that are to guide a global struggle against terror is neither top-down nor bottom-up, but complex and omni-directional. In the process, US CT policy has changed as well.

Finally, beyond the diffusion and contestation of formal norms, the paper focuses on a less discussed dimension: these regional forums also reflect the development of CT practices and serve as arenas for the development of practical cooperation. Within the ARF we find discussions not only about abstract norms but about how to turn them into actual practices (e.g. how to "do" border security) and examinations of "best practices" on various related topics. This is the substance of global/regional governance: state actors interact – directly and via multilateral (global or regional) formal institutions; their interactions include traditional material bargaining (e.g. financial aid for policy reform), as well as normative discussions and attempts at legitimizing and institutionalizing certain ideas; and what they do is to advance normative-legal formal frameworks, as well as the mechanisms that translate laws and decisions into actual practices of governance.

This multi-level examination then reveals several important points. Firstly, while the US is clearly a central actor in designing and managing international CT cooperation, it is operating in a complex web of institutional channels, and its influence is thus constrained. Secondly, in this complex web of institutions and actors, regional institutions like ASEAN play an important role as the arenas that enable regional states to negotiate among themselves a common voice and that provide institutionalized channels for collective engagement with the United States. Thirdly, despite the importance of ASEAN, bilateral negotiations between regional states and the US remain crucial. Fourthly, it was important also to examine the varying (and shared) domestic perceptions of the terrorist threat and of CT, as well as the variations in the capacity of different regional states to deal with these threats. Finally, domestic, bilateral, and regional debates were all framed within the global CT legal framework provided by the UN, suggesting that with all its limitations, the UN framework still serves as an important reference point for regional states and great powers alike.

The Spillover of Asian Rivalry: Asia-Related Disputes in the Middle East

Yoram Evron, University of Haifa

In recent years, the fierce tension between China and Japan, coupled with their growing economic, political, and even military presence in areas beyond East Asia, make it more likely that their rivalry will spill over into other regions. This possibility raises several questions: Does such a spillover actually exist? What are the forces behind it? In what fields does it take place? How symmetric is Sino-Japanese rivalry in regions other than East Asia? And what are the implications of this spillover for China and Japan, the regions in question, and perhaps also the international system? Attempting to provide preliminary answers to these questions, this paper examines Japan's response to China's Belt and Road Initiative (BRI) and its implications for China-Japan relations in regions beyond East Asia. As demonstrated in the paper, the Sino-Japanese interaction concerning the BRI in regions beyond East Asia is closely related to these countries' rivalry in East Asia, thus meeting the precondition of rivalry spillover.

Japan's response to the BRI has been mostly negative. Itself a major investor in infrastructure and other development projects in Asia for decades, Japan regarded the Chinese mega-initiative as a measure intended to increase its rival's political influence in Eurasia and to provide it with abundant economic opportunities there. The possibility that the BRI would enhance China's military presence along the BRI's routes probably worried Japan as well. For these reasons Japan has taken various diplomatic and financial steps to reduce the BRI's impact and to raise its own political influence and economic opportunities in the respective regions. Prominent among them is a joint initiative with India – another Asian rival of China – called the Asia-Africa Growth Corridor (AAGC). Like the BRI, but intended to be of better quality, the AAGC aims to integrate the economies of South, Southeast, and East Asia with Oceania and Africa through a web of ground and maritime routes to promote these regions' development. China's response to Japan's countermeasures is complex, as it sees Japan as a force that can both promote and thwart the BRI. Hence, it is trying to persuade Japan to join it. For its part, Japan, unwilling to lose economic opportunities associated with the BRI, is not turning its back on it, although concurrently it is proceeding with the AAGC initiative, which the US and Australia have recently joined too.

As this case shows, the main forces behind the Sino-Japanese conflict's spillover into other parts of Asia are the two powers' similar intention to increase their impact beyond their region, and their similar inclination to combine political and economic goals and the means to do so. Their form of rivalry, at least in this case, includes contesting investments and infrastructure projects, foreign aid, and the formation of blocs (mainly Japan) with other countries. The implications of the rivalry's spillover are additional sources of tension between China and Japan, but more economic opportunities for regions into which Sino-Japanese rivalry spreads.

Participants (by presentation order)

Nissim Otmazgin is the Chair of the Department of Asian Studies, The Hebrew University of Jerusalem and Associate Director of the Harry S. Truman Research Institute for the Advancement of Peace. He is the author of *Regionalizing Culture: The Political Economy of Japanese Popular Culture in Asia* (University of Hawai'i Press, 2013) and (together with Michal Daliot-Bul), *The Anime Boom in the US: Lessons for Global Creative Industries* (Harvard University Asia Center Press, 2017). He also co-edited (with Eyal Ben-Ari) *Popular Culture and the State in East and Southeast Asia* (Routledge, 2012), (with Sigal Galanti and Alon Levkowitc) *Japan's Multilayered Democracy* (Palgrave, 2014), and (with Rebecca Suter) *Manga and History: Stories for the Nation* (Palgrave-Macmillilan 2016). Email: nissim.otmazgin@mail.huji.ac.il

Galia Press-Barnathan is a senior lecturer in the Department of International Relations, The Hebrew University of Jerusalem. She has published two books: O*rganizing the World: The US and Regional Cooperation in Asia and Europe* (Routledge, 2004) and *The Political Economy of Transitions to Peace* (Pittsburgh University Press, 2009). She has also published articles in leading international relations journals.

Ehud Harari is Professor Emeritus in the Departments of East Asian Studies and Political Science, The Hebrew University of Jerusalem. A political scientist (PhD from the University of California, Berkeley), his teaching, research, and publications focus on Japanese politics, administration, industrial relations, and foreign relations in comparative perspective. He is the recipient of an Imperial Decorations of the Order of the Rising Sun, Gold and Silver Star (from 2002 and 2018).

Paul Midford is Professor and Director of the Japan Program, Norwegian University for Science and Technology in Trondheim. Midford received his PhD in Political Science from Columbia University in 2001. His research interests include Japanese foreign and defense policies, the impact of public opinion on policy, renewable energy and energy security, and East Asian security and multilateralism. He has published over a dozen book chapters, co-edited three books, and published articles in *International Organization*, *International Studies Quarterly*, *Security Studies*, *Pacific Review*, *Asian Survey*, *Japan Forum*, and *International Relations of the Asia-Pacific*. Midford is the author of *Rethinking Japanese Public Opinion and Security: From Pacifism to Realism?* (Stanford University Press, 2011), and the co-author of *The Japanese Ground Self-Defense Force: Search for Legitimacy* (Palgrave, 2017). He is currently completing a book manuscript entitled *Overcoming the Reactive State: Japan's Promotion of East Asian Security Multilateralism*.

Yiftach Raphael Govreen is a PhD student in the Department of International Relations, The Hebrew University of Jerusalem. He is currently completing his dissertation on the US-Japan Security Alliance.

Kai He is a Professor of International Relations at Griffith Asia Institute and Centre for Governance and Public Policy, Griffith University, Australia. He is currently an Australian Research Council (ARC) Future Fellow (2017-2020). He was a post-doctoral fellow in the Princeton-Harvard China and the World Program (2009-2010). His book entitled *China's Crisis Behavior: Political Survival and Foreign Policy* was published by Cambridge University Press in 2016.

Doron Ella is a PhD candidate in the Department of International Relations, The Hebrew University of Jerusalem. His research focuses on China in international organizations. He is the editor of the academic journal *Politika: The Israeli Journal of Political Science and International Relations*, published by the Leonard Davis Institute for International Relations at The Hebrew University of Jerusalem.

Tetsuo Kotani is a Senior Fellow at the Japan Institute of International Affairs. He also teaches at Hosei University and JMSDF Command and Staff College. His research focus is Japan's foreign and security policies, the US-Japan alliance, and maritime security.

Or Rabinowitz is Assistant Professor of International Relations, The Hebrew University of Jerusalem. Her research interests include nuclear proliferation, nuclear history, and Israeli-American relations. Her book *Bargaining on Nuclear Tests* was published in April 2014 by Oxford University Press, and she has since published articles in *International Security*, *Journal of Strategic Studies*, and *Bulletin of the Atomic Scientists*. She holds a PhD awarded by the War Studies Department of King's College London, and an MA in Security Studies and an LLB, both from Tel-Aviv University. She is currently conducting a study on Israel's failure to establish a civilian nuclear infrastructure, funded by the Israel Science Foundation.

Dai Mochinaga is a researcher at Mitsubishi Research Institute, Inc., a Japanese think tank and consulting firm based in Tokyo. He joined the Institute in 2008 and has worked as a consultant for Japanese government projects related to cybersecurity, R&D strategy development, and cryptographic technology evaluation. His research interests include cybersecurity, international relations, and information technology.

Da-Yu Kao is an Associate Professor in the Department of Information Management, College of Police Science and Technology, Central Police University, Taiwan. He is responsible for various recruitment efforts and training programs for Taiwanese civil servants, police officers or ICT technicians. He was a detective and forensic police officer at Taiwan's Criminal Investigation Bureau (under the National Police Administration). With a Master's in Information Management and a PhD in Crime Prevention and Correction, he has led several investigations in cooperation with police agencies from other countries over the last 20 years. He is now the director of the Computer Crime Investigation Lab at the Central Police University and the webmaster of the Facebook group Cybercrime Investigation and Digital Forensics.

Amit Sheniak is a Post-Doctoral Research Fellow at The Hebrew University of Jerusalem, Davis Institute for International Relations, the Truman Institute for the Advancement of Peace, and The Hebrew University Cyber Security Research Center. He is also the cybersecurity policy coordinator of the Israeli Ministry of Defense Political-Military Directorate.

Tamar Berenblum is a Post-Doctoral Research Fellow, Netherlands Institute for the Study of Crime and Law Enforcement, The Hebrew University Cyber Security Research Center, and The Rachel and Selim Benin School of Computer Science and Engineering at The Hebrew University of Jerusalem. She is the Research Director of the Cyber Law Program, Faculty of Law, The Hebrew University Cyber Security Research Center. Tamar's research interests include victimology, sociology of knowledge, cybercrime, and social control. Her doctoral thesis at The Hebrew University of Jerusalem entitled "The Internet as a Sphere of Social Control" examines the Internet

both as a sphere for social control and as a tool for such control over deviant activities. The study focuses on mapping and analyzing online social control practices and the applicability of social control theories and policies in the context of cyberspace.

Anja Mihr is Founder and Program Director of the HUMBOLDT-VIADRINA Center on Governance through Human Rights in Berlin. She has held professorships for public policy, international relations, and human rights at the Willy-Brandt School of Public Policy, Erfurt University and at the Netherlands Institute of Human Rights, University of Utrecht.

Raymond Yamamoto received his PhD from Hamburg University in 2015. From 2015 to 2017, he worked as a Specially Appointed Researcher and as a Part Time Lecturer at Osaka University. In 2017, he was appointed as Assistant Professor at Aarhus University. His research focuses on Japan's postwar foreign policy as well as on the development and security nexus of the Japanese Official Development Assistance.

Yoram Evron is Assistant Professor in the Department of Asian Studies at the University of Haifa. Focusing on China's national security and foreign relations, his research and teaching interests include China's military procurement, arms proliferation, and military modernization, China-Middle East and China-Israel relations, as well as the Asian powers' involvement in the Middle East. He was the founder and director of the China Program at the Institute for National Security Studies. His book *China's Military Procurement in the Reform Era: The Setting of New Directions* was published by Routledge in 2016.