INTELLIGENCE COMMUNITY FORUM

ICF 2019

Intelligence Support for Decision-Makers • June 18–20, 2019

MERCYHURST
RIDGE COLLEGE
OF INTELLIGENCE STUDIES AND APPLIED SCIENCES

Brécourt Academic

GLOBAL WAR STUDIES
The Journal for the Study of Warfare and Weapons, 1919-1945

RIDGE POLICY GROUP

MERCYHURST
UNIVERSITY

501 East 38th Street
Erie, PA 16546

814-824-2000
800-825-1926
mercyhurst.edu

It is my pleasure to welcome all of you to the inaugural Intelligence Community Forum (ICF 2019), hosted by the Ridge College of Intelligence Studies & Applied Sciences at Mercyhurst University in Erie, Pennsylvania, and Brécourt Academic in association with Global War Studies. We trust you will enjoy this valuable learning and networking experience.

Here at Mercyhurst, we like to think of ourselves as pioneers and there are many instances of this characterization that I could share with you. However, for purposes of this forum, I will settle for one.

Mercyhurst pioneered the academic discipline of intelligence studies in the mid-1990s, and today is home to the largest and oldest academic intelligence enterprise in the United States: the Ridge College of Intelligence Studies & Applied Sciences. Named after Erie native Thomas J. Ridge, the first Secretary of the U.S. Department of Homeland Security and two-term Pennsylvania governor, the Ridge College has earned a reputation throughout the world for the quality of its graduates. In fact, our intel alumni work in all 17 federal intelligence agencies and dozens of Fortune 500 companies, assisting corporate and government leaders in making informed decisions.

More recently, as new threats and technologies have emerged, we have leveraged our expertise and reputation in intelligence studies into the fields of data science and cyber security. In addition to developing cutting-edge curricula, we opened a top-flight cyber education center on campus in 2018, enabling us to provide unparalleled, hands-on instruction in today's most dynamic fields.

It is out of this thriving enterprise that we are pleased to host ICF 2019, an international conference bringing together intelligence community professionals, scholars and students to create a vibrant mix of thought leadership and best-practice strategies. We are indeed honored to have Gov. Ridge as our inaugural keynote speaker. He and others will address the theme "Intelligence Support for Decision-Makers."

We trust you will take away an increased knowledge of the practices and partners in this critical field through the many papers, presentations and panel discussions that are planned. It is with great pleasure that I welcome you on board for the first of what we anticipate will be an annual event.

And, as we say at Mercyhurst, Carpe Diem,

Michael T. Victor, J.D., LL.D.
President, Mercyhurst University

Brécourt Academic

GLOBAL WAR STUDIES
The Journal for the Study of Warfare
and Weapons, 1919-1945

Dear ICF 2019 Delegates,

On behalf of Brécourt Academic and Global War Studies, I would like to extend a very warm welcome to all of you. ICF 2019 is the first of what will be an annual conference for the international intelligence community and your attendance and participation are appreciated.

When I first developed the idea for this conference nearly five years ago, I was fortunate to have the support of colleagues Kris Young, Duane Young, and Duncan McGill, as well as their critical intellectual input. The underlying objective of the forum has always been to provide the IC with an annual academic conference that would bring together intelligence professionals from a variety of disciplines—academia, military, government, business, students—to share research, ideas, and methods. It was also important that the ICF be an international event welcoming delegates from many nations.

It has been my good fortune to work with Dean Duncan McGill and his exceptional tea.m. at Mercyhurst University’s Ridge College of Intelligence Studies and Applied Sciences, and I look forward to our continued partnership. As we look toward ICF 2020, we welcome your feedback— critical or otherwise—to help us develop the conference into a must-attend annual event.

Robert von Maier
Publisher and Editor-in-Chief
Brécourt Academic

SCHEDULE

MONDAY, JUNE 17, 2019

Noon – 6 p.m.	Housing check-in	Ryan Hall	Peter Chuzie; Graham Goodwiler

TUESDAY, JUNE 18, 2019

7 – 9 a.m.	Breakfast	Ryan Hall	Tickets in Package
9 – 11:30 a.m.	Conference Registration	Hirt Building Lobby	All delegates check in
9:30 – 10:30 a.m.	Tour #1	Campus and Cyber/Intel	Depart from Hirt Building Lobby
10:30 – 11:30 a.m.	Tour #2	Campus and Cyber/Intel	Depart from Hirt Building Lobby
11:30 a.m. – 1 p.m.	Lunch	Ryan Hall	Tickets in package
12:30 – 1 p.m.	Press Conference	Ed Conf Rm, Hirt 303	Gov. Tom Ridge
1 – 1:20 p.m.	Conference Welcome	Walker Recital Hall	Duncan McGill and Robert von Maier
1:20 – 1:30 p.m.	Speaker Introduction	Walker Recital Hall	Cal Pifer
1:30 – 2:30 p.m.	Keynote Address	Walker Recital Hall	Gov. Tom Ridge
3 – 4:30 p.m.	Strategic Intelligence	Hirt 212	Antony Field
		Hirt 212	John A. Gentry and Joseph S. Gordon
	Historical	Hirt 213	Matthew Walker
		Hirt 213	Jonathon M. House
5 – 8 p.m.	Welcoming Reception		The Roost Pub (Student Union)

WEDNESDAY, JUNE 19, 2019

7 – 8:30 a.m.	Breakfast	Ryan Hall	Tickets in Package
8:45 – 10:15 a.m.	NIU Plenary Session	Walker Recital Hall	Bruce MacKay (Chair), Julie Mendosa, Susan Perlman and Vangala Ram
10:30 a.m. – Noon	Information Management	Hirt 212	Daniel Irwin
		Hirt 212	Hamid Mansouri Rad
	Regional Issues	Hirt 213	Chase Masters
		Hirt 213	Augustin Maciel-Padilla
		Hirt 213	Carl William Strong
	Historical – "Brit-Int"	Hirt 214	Andrew R. English
		Hirt 214	Haley Fenton

Noon – 1 p.m.	Lunch	Ryan Hall	Tickets in Package
1 – 2:30 p.m.	Regional – Asia: Past to Present	Hirt 212	Ralph D. Sawyer
		Hirt 212	Mark Wheeler
	Improving Intelligence	Hirt 213	Fred Hoffman
		Hirt 213	Mary-Beth Moore
	Regional – Middle East	Hirt 214	Samiah Baroni
		Hirt 214	Vangala Ram
		Hirt 214	Matthew Walker
3 – 4:30 p.m.	Terrorism – 1	Hirt 212	Afzal Upal
		Hirt 212	Duane Young
	NIU Graduate Student Cyber Panel	Hirt 213	Christopher M. Hines
		Hirt 213	Meridith Doran
	Historical – "Eisenhower Era"	Hirt 214	Nicholas Dujmovic
		Hirt 214	Jean-Michel Turcotte

THURSDAY, JUNE 20, 2019

7 – 8:30 a.m.	Breakfast	Ryan Hall	Tickets in Package
8:45 – 10:15 a.m.	Intelligence in "Other Than War"	Hirt 212	J. Scott Braderman Piotr Ziemkiewicz
		Hirt 212	Kristina A. Young
	Cyber Panel	Hirt 213	Gregory S. Laidlaw
		Hirt 213	Sarah Freeman
10:45 a.m. – 12:15 p.m.	Historical – ETO	Hirt 213	Sarah Anna-Maria Lias Ceide
		Hirt 213	Elizabeth A. Coble
	Terrorism – 2	Hirt 212	J. Scott Braderman and Maura Reilly
		Hirt 212	Musa Tuzuner
		Hirt 212	M. Afzal Upal
Noon – 1 p.m.	Lunch	Ryan Hall	Tickets in Package
1 – 2:30 p.m.	Methods for Decision-Makers	Hirt 213	Stephen Downes-Martin
		Hirt 213	Christopher Mansour
	Intelligence Education	Hirt 212	Michael Fowler
		Hirt 212	Kathleen Moore
2:30 – 3 p.m.	Closing Remarks	Walker Recital Hall	
3 p.m. – 4 p.m.	AAR session	Hirt 212	

PROGRAM SESSIONS & PANEL ASSIGNMENTS

TUESDAY, JUNE 18, 2019

Welcome & Keynote Address, Governor Tom Ridge - 1:00 - 2:30 PM (Walker Recital Hall)

Strategic Intelligence Panel - 3:00 - 4:30 PM (Hirt 212)

Chair: Robert von Maier, Publisher/Editor-in-Chief, Brécourt Academic & Global War Studies

Antony Field, California State University San Bernardino

Strategic Intelligence: Road to Nowhere?

John A. Gentry, Georgetown University and Joseph S. Gordon, National Intelligence University

U.S. Strategic Warning Intelligence: Debating Its Status

Historical Panel - 3:00 - 4:30 PM (Hirt 213)

Chair: Duane C. Young, National Intelligence University

Matthew Walker, Independent Scholar

Crafting Communities: A Study of Developing Relations Between Non-Governmental and Intelligence Sectors, 1944 - 1957

Jonathan M. House, U.S. Army Command and Staff College

Intelligence Reform in the Eisenhower Administration

WEDNESDAY, JUNE 19, 2019

Plenary Session - National Intelligence University Roundtable - 8:45 - 10:15 AM (Walker Recital Hall)

Bruce MacKay (Chair), Julie Mendosa, Susan Perlman and Vangala Ram

Leading Today's Intelligence Community

Information Management Panel - 10:30 AM - 12:00 PM (Hirt 212)

Chair: Christopher Mansour, Mercyhurst University

Daniel Irwin, Department of National Defence, Toronto (co-author, David R. Mandel, Department of National Defence, Toronto)

Improving Information Evaluation for Intelligence Production

Hamid Mansouri Rad, New Mexico State University

Rhetoric of National Intelligence Writing: A Qualitative Exploration of the Role of Persuasion

Regional Issues Panel - 10:30 AM - 12:00 PM (Hirt 213)

Chair: Susan Perlman, National Intelligence University

Chase Masters (on behalf of William R. Hawkins, Hamilton Center for National Strategy and Brenda J. Ponsford)

Intelligence as Soft Power: The Case of Africa

Augustin Maciel-Padilla, Embassy of Mexico in Belize

Mexico: The New Security Conundrum

Carl William Strong, National Intelligence University

Energy Imperialism: Geopolitical Implications of Russian Pipeline Construction

Historical – "Brit-Int" Panel - 10:30 AM - 12:00 PM (Hirt 214)

Chair: Robert von Maier, Publisher/Editor-in-Chief, Brécourt Academic & Global War Studies Andrew R. English, Independent Scholar

"Prying Eyes": Foreign Spies, War Plans, and the Dawn of British Naval Intelligence

Hayley Fenton, The Ohio State University

"The Oracle of Bletchley": Frederik Winterbotham and the Translation of Technology

Regional – Asia: Past to Present Panel - 1:00 - 2:30 PM (Hirt 212)

Chair: Kristina A. Young, National Intelligence University

Ralph D. Sawyer, University of Massachusetts

Disinformation Theory and Practice in Historic China

Mark Wheeler, 29th Intelligence Squadron, Fort George G. Meade, MD

The Way Xi Moves: Understanding Chinese Behavior in Proper Strategic and Cultural Context

Improving Intelligence Panel - 1:00 - 2:30 PM (Hirt 213)

Chair: Duncan E. McGill, Mercyhurst University

Fred Hoffman, Mercyhurst University

The A2E Integrated Intelligence Model: Integrating Five Types of Intelligence to Improve Organizational Performance

Mary Beth Moore, SAS

Improving Intelligence with AI

Regional – Middle East Panel - 1:00 - 2:30 PM (Hirt 214)

Chair: Benjamin Baughman, Mercyhurst University

Samiah Baroni, National Intelligence University

The Commodification of Islam

Vangala Ram, National Intelligence University (delivered on behalf of Paul Kubik, Signals Intelligence and Advanced Geospatial Intelligence Officer, WA, DC)

Iran: Pariah State, Rogue Nation

Matthew Walker, Independent Scholar (co-author, Hersh A. Hama Karim, University of Sulaimani, Iraq)

The Intellectual Case in Kurdistan

Terrorism Panel – 1 - 3:00 - 4:30 PM (Hirt 212)

Chair: Jacob A. Mauslein, Mercyhurst University

M. Afzal Upal, Mercyhurst University

Grievances are Status Enhancing Myths

Duane C. Young, National Intelligence University

Thoughts on Terrorism in Warfare

NIU Graduate Student Cyber Panel - 3:00 - 4:30 PM (Hirt 213)

Chair: Vangala Ram, National Intelligence University

Christopher M. Hines, National Intelligence University

Supply Chain Risk Management: Viewing ICT Supply Chains as Complex Adaptive Systems

Meredith Doran, National Intelligence University

Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM): A Risk Management Framework to Understand and Reduce Vulnerabilities

Historical – "Eisenhower Era" Panel - 3:00 - 4:30 PM (Hirt 214)

Chair: Todd Clark, Fairmont State University Nicholas Dujmovic, Catholic University of America

Prisoners of the Chicoms: Eisenhower and the CIA-China Dilemma

Jean-Michel Turcotte, JFK Institute for North American Studies/Freie Universität, Berlin

"Observing Communist Soldiers": US Intelligence Policy and the Captivity of North Korean and Chinese POWs, 1950-1953

THURSDAY, JUNE 20, 2019

Intelligence in "Other Than War" Panel - 8:45 - 10:15 AM (Hirt 212)

Chair: Bruce MacKay, National Intelligence University

J. Scott Braderman, U.S. Army War College (co-author, Piotr Ziemkiewicz, Deloitte LLP & 203rd Military Intelligence Battalion, U.S. Army Reserve

Peacekeeping and Stability Activities Lack Intelligence Indicators Leads to Protracted Conflict

Kristina A. Young, National Intelligence University

Thoughts on Asymmetric Warfare

Cyber Panel - 8:45 - 10:15 AM (Hirt 213)

Chair: Christopher Mansour, Mercyhurst University

Gregory S. Laidlaw, University of Detroit Mercy and Charles E. Wilson, University of Detroit Mercy

Enhancing Cyber Security: Applying and Cyber Intelligence Techniques

Sarah Freeman, Idaho National Laboratory

The Challenges of Attribution Within Cyber Space

Historical – ETO - 10:45 AM - 12:15 PM (Hirt 213)

Chair: Jacob A. Mauslein, Mercyhurst University

Sarah Anna-Maria Lias Ceide, University of Naples Federico II

ODEUM Rome – German-Italian Intelligence Collaborations (1945-1956)

Elizabeth A. Coble, U.S. Army - XVIII Airborne Corps and Fort Bragg

Allied Intelligence Leading Up to Operation MARKET GARDEN

Terrorism Panel – 2 - 10:45 AM - 12:15 PM (Hirt 212)

Chair: Duane C. Young, National Intelligence University

J. Scott Braderman, U.S. Army War College and Maura Reilly, Dickinson College

Mitigating Terrorism and Transnational Organized Crime Links: A Focus on Facilitators

Musa Tuzuner, Mercyhurst University (co-author, Mehmet Arican, Homeland Security Consultation LLC)

U.S.-Turkey Anti-Money Laundering (AML) International Cooperation: The Case of Gold Trader Reza Zarrab

M. Afzal Upal, Mercyhurst University

Scientific Fundamentalism and the Need for Meaning

Methods for Decision-Makers Panel - 1:00 - 2:30 PM (Hirt 213)

Chair: Todd Clark, Fairmont State University

Stephen Downes-Martin, U.S. Naval War College

How an Opponent Wargames is an Intelligence Collection Requirement

Christopher Mansour, Mercyhurst University

From Cyber Risk to Cyber Secure

Intelligence Education Panel - 1:00 - 2:30 PM (Hirt 212)

Chair: Duncan E. McGill, Mercyhurst University

Michael Fowler, U.S. Air Force Academy

A Pedagogical Approach to Country Analysis

Kathleen Moore, James Madison University

New Fronts of the Cyber War and Intelligence Education

PANELS & ABSTRACTS

Strategic Intelligence Panel

Antony Field, California State University San Bernardino

Strategic Intelligence: Road to Nowhere?

This paper will explore the reasons why strategic intelligence often fails to make an impact on national security decision-making. Intelligence analysts spend a considerable amount of time producing strategic intelligence assessments and estimates, yet these products are frequently ignored or under-utilized by policy-makers. For example, strategic intelligence reports regarding the terrorist threat posed by Al Qaeda in the 1990s failed to generate a timely response from senior officials who were responsible for counter-terrorism strategy. This paper will argue that strategic intelligence often fails to make impact because there is a fundamental tension between intelligence analysts and policy-makers about what constitutes "useful" national security knowledge. Intelligence analysts are increasingly focused on producing strategic intelligence products that provide methodologically robust, balanced and reasonable judgements about national security threats. This is often at odds with the desire of policy-makers to push forward preexisting national security agendas that are deeply embedded in their political belief system. In this context, strategic intelligence products can be seen as more of a 'hinderance' than a 'help' in the policy-making process. The paper will discuss some potential ways to mitigate this problem and improve the overall impact of strategic intelligence.

U.S. Strategic Warning Intelligence: Debating Its Status

John A. Gentry, Georgetown University and Joseph S. Gordon, National Intelligence University

Strategic warning intelligence in the U.S. intelligence community (IC) is in one of its periodic troughs—underappreciated and without an institutional home. Yet there is unhappiness in some parts of the IC about the lack of emphasis on strategic warning and concern that Director of National Intelligence James Clapper's abolition in 2011 of the position of national intelligence officer for warning and assignment of warning responsibilities to a large group of officials with other duties means that in fact no one is addressing strategic warning. In a recent book (Strategic Warning Intelligence: History, Challenges, and Prospects, Georgetown University Press, 2019), we assessed the state of U.S warning intelligence, identified problems, and recommended corrective measures. In this paper, we will update our book by, primarily, describing debates within the IC in 2018 about strategic warning, identifying the concerns of some senior leaders, and assessing the likelihood of IC restoration of a dedicated strategic warning function in the near term. Source material will include newly available documents and discussions with senior officials, some of whom evidently are willing to speak on the record.

Historical Panel

Matthew Walker, Independent Scholar

Crafting Communities: A Study of Developing Relations Between Non-Governmental and Intelligence Sectors, 1944 - 1957

In the earliest stages of the Pax Americana following World War II, non-government organizations (NGOs) played a prominent role in setting the agenda for America's national interests in the international community. One of the earliest examples of this was the Citizens' Committee for the Marshall Plan (CCMP), calling for direct aid to help rehabilitate Europe following its utter destruction resulting from total war. Established in the fall of 1947, and nearly coinciding with the creation of national security infrastructure brought about by the National Security Act of 1947 earlier that year, the CCMP set out to convince the American public and Congress of the need for supporting President Truman's European Recovery Plan. This bipartisan panel readily identified and relentlessly campaigned to win over a reluctant public to support extending America's presence overseas. The proposed research and paper aims to investigate the paths of the CCMP and newly created Central Intelligence Agency arising from the National Security Act. What was the relationship between the CIA and the Committee? Specific attention will be paid to understanding the approaches taken to NGO formation and influence. Was the CCMP influential to the CIAs understanding of NGOs? If not, what was? Additional attention will examine the relationships between the leading personalities, Dean Acheson and Allan Dulles among others.

Jonathan M. House, U.S. Army Command and Staff College

Intelligence Reform in the Eisenhower Administration

During the presidency of Dwight Eisenhower, numerous special boards or groups influenced the adolescent American intelligence community. The Clark Task Force (1953-55) and Doolittle Committee on Covert Activities (1954) both identified significant issues, especially with the role of Director of Central Intelligence. Building on these observations, Eisenhower appointed the President's Board of Consultants on Foreign Intelligence Activities (PBCFIA), which made a sustained effort to improve the intelligence community between 1956 and 1961. The first chair of the PBCFIA, James Killian, skillfully employed the president's backing to achieve significant changes. These included creation of a unified body, the U.S. Intelligence Board, and greater authority for the DCI and the Director, National Security Agency. After a final panel, the Joint Study Group in 1960, Eisenhower left office convinced that his reforms had failed. In retrospect, however, these reform committees made notable progress in the integration and maturation of American intelligence; the Kennedy Administration reappointed Killian to chair an advisory board, and Eisenhower's efforts contributed to the creation of the Defense Intelligence Agency and the removal of the armed services from the Intelligence board.

Plenary Session - National Intelligence University's Roundtable

Bruce MacKay (Chair), Julie Mendosa, Susan Perlman and Vangala Ram

Leading Today's Intelligence Community

The security environment of the 21st Century is composed of rapidly-changing threats that challenge the processes and mental models of United States intelligence professionals and decision-makers. These threats have implications that span a variety of organizations, including the private and non-profit sectors, government, military, and law enforcement. Success for the intelligence community in supporting decision-makers requires ongoing adaptations and creation of flexible systems. The roundtable discussion will address the need for IC leadership to guide collaborative, adaptive practices in intelligence. It will also touch on leadership principles that can provide the foundations of ongoing development in intelligence organizations.

Information Management Panel

Daniel Irwin, Department of National Defence, Toronto (co-author, David R. Mandel, Department of National Defence, Toronto)

Improving Information Evaluation for Intelligence Production

National security decision-making is informed by intelligence assessments, which in turn depend on sound information evaluation. Recognizing this fact, intelligence organizations have promulgated methods for evaluating source and evidential characteristics. We critically examine these methods and identify several limitations that undermine the fidelity of information evaluation. We argue that these limitations are symptomatic of a deep-seated tendency in the intelligence community to mask rather than effectively guide subjectivity in intelligence assessment. Drawing on the guidance metaphor, we propose that rigid "all-purpose" information evaluation methods be replaced by flexible "context- sensitive" guidelines aimed at improving the soundness, precision, accuracy, and clarity of irreducibly subjective judgments. Specific guidelines, supported by empirical evidence, include use of numeric probability estimates to quantify the judged likelihood of information accuracy, promoting collector- analyst collaboration, and periodic revaluation of information as new information is acquired. We also offer a set of questions to guide information evaluation.

Hamid Mansouri Rad, New Mexico State University

Rhetoric of National Intelligence Writing: A Qualitative Exploration of the Role of Persuasion

Was the August 6, 2001 PDB a warning? Some former CIA analysts believe it was. Yet, President George W. Bush, recognized as an avid intelligence consumer, did not perceive that document as a warning; that is, one could argue that he was not sufficiently persuaded of the severity of the threat that Al Qaeda affiliates were posing to the US homeland. While persuasiveness has been identified as one of the characteristics of effective intelligence products, some intelligence scholars maintain that persuading the policy maker is not the goal of intelligence. Instead, they argue, the goal is to "inform" the policy maker. Many will find this debate intriguing if not important to national security. As a researcher, I have set out to explore the potential role of persuasion in intelligence products using a qualitative design, including a survey and interviews to explore relevant perspectives of former members of the US Intelligence Community. My presentation will place studies and theories about rhetoric, persuasion, and argumentation into conversation with related literature from intelligence studies. My presentation will include preliminary results of this study.

Regional Issues Panel

Chase Masters (on behalf of William R. Hawkins, Hamilton Center for National Strategy and Brenda J. Ponsford)

Intelligence as Soft Power: The Case of Africa

Major changes in the strategic environment in Africa call for a reorientation of America's operational focus. First, U.S. economic ties to Africa have declined substantially. The expansion of domestic production has greatly reduced American need for African oil, the main basis of past trade. This reduces political support for any large investment of money to fund defense or foreign policy initiatives on the continent. Second, China has rapidly increased trade and investment in Africa, built on the old imperialist model of importing oil and minerals in exchange for manufactured goods. Beijing's Belt and Road initiative is aimed at controlling African infrastructure and entangling local states in the Chinese economy. China will leverage development projects for strategic gains. Third, the U.S. National Defense Strategy has elevated American efforts from combating terrorism to competing globally with rival Great Powers, of which China is identified as the most prominent. Therefore, scarce U.S. diplomatic and military assets must be deployed in an asymmetrical and cost effective strategy to prevent Chinese money from subverting African governments and turning them against the United States. The provision of intelligence, training and technical aid (particularly in cyber security) can help African leaders face Chinese expansion by safeguarding their national independence, rooting out foreign corruption, and protecting their people from exploitation.

Augustin Maciel-Padilla, Embassy of Mexico in Belize
Mexico: The New Security Conundrum

The central argument of this proposal is that in the absence of an ordered process to reorganize security structures in Mexico, and in the absence of clarity about the concept of security, the measures the incoming left-wing government inplement to combat insecurity will not be effective unless there is a clear understanding not only of the challenges, but also of the instruments at its disposal to deal with these challenges. The plan of the Andres Manuel Lopez-Obrador administration (MORENA-National Regeneration Movement) about disbanding the Mexican intelligence agency and to create instead a new institution under the Secretariat of Public Security focusing on internal challenges, is just an example of the prevailing confusion. Mexico's increasing international exposure cannot afford neglecting foreign intelligence. This paper will therefore address Mexican intelligence prospects for the future.

Carl William Strong, National Intelligence University
Energy Imperialism: Geopolitical Implications of Russian Pipeline Construction

Russia's 2017 GDP was $4 trillion and 68% came from fossil fuels: i) Natural gas revenues contribute significantly and the EU purchases as much as 24% of its gas from Gazprom, the Russian state-owned gas company; ii) This is significant because Moscow "uses pipeline politics to get its way;" iii) It requires Gazprom to sell to former republics at a cost below market rate because "business priorities are second to political concerns;" iv) and even turned off Ukrainian gas supplies in 2006 following a pricing disagreement. EU dependency on Russian gas constitutes a significant security risk. The Kremlin uses it as a mechanism of economic power and also as a coercive tool within their "hybrid warfare" construct. The purpose of this paper is to explore the evolving implications of that dependency following the construction of the Nord Stream 2 and TurkStream gas pipelines.

Historical – "Brit-Int" Panel

Andrew R. English, Independent Scholar
"Prying Eyes": Foreign Spies, War Plans, and the Dawn of British Naval Intelligence

By the late nineteenth century, Russian Naval Intelligence was considered "the best in the world," and they reportedly knew more about the Royal Navy "than the First Sea Lord of the Admiralty." 1. London responded to this Russian threat by forming its own intelligence cell in 1882, and Britain would now "have vigilant and systematic eyes bent also upon their proceedings." 2. By the late 1880s, the duties of Britain's Naval Intelligence Department embraced "all information relating to maritime matters likely to be of use in war." 3. In St. Petersburg, one general warned the British colonies were not secure. 4. One Hong Kong newspaper observed, "Russia can hardly repudiate a treaty, before the ink is dry." 5. The "Great Game" had generated a momentum of its own.

Hayley Fenton, Ohio State University
"The Oracle of Bletchley": Frederik Winterbotham and the Translation of Technology

The entwining of collection techniques with increasingly sophisticated technology has been a pronounced feature of intelligence development over the last century. Yet, technological leaps can be accompanied by steep learning curves. The Second World War experience of Frederick Winterbotham demonstrated the organizational and communication challenges that accompanied one such advance: the ability to decode intercepted German messages. Winterbotham, himself an observer of the development process that broke the Enigma codes, recognized the communication challenges that accompanied a new and unusually reliable intelligence source. He positioned himself to interface with political and military leadership. To facilitate the acceptance of ULTRA, Winterbotham built relationships and de-emphasized the sophisticated scientific and mathematical principles that had made the breakthrough possible. This rapport built on an understanding of the newly-fashioned decryption machines as a supernatural force. Winterbotham minimized the cultural and geographical distance between code-breaking headquarters at Bletchley Park and field commands by implanting personnel familiar with the project and its security demands. ULTRA changed both the quality and quantity of the intelligence available to political and military leaders, but its effective employment continued to rely upon personal relationships and attitudes.

Regional - Asia: Past to Present Panel

Ralph D. Sawyer, University of Massachusetts

Disinformation Theory and Practice in Historic China

From their inception with the Art of War nominally attributed to Sun-tzu, China's extensive military writings emphasized the importance of disinformation in deceiving and manipulating enemies. In addition to helping maintain secrecy, disinformation played a major role for more than twenty-five centuries in distracting opponents, inducing errors, fostering distorted perspectives, skewing interpretations, balking assessments, concealing authentic communications, and inducing doubt, thereby paralyzing the decision making process. Based on original Chinese language sources, Disinformation Theory and Practice in Historic China elucidates the main theoretical points and provides a brief overview of actual practice in traditional China, including how misinformation was conceived, manipulated, and disseminated in order to achieve these objectives, as well as raise doubt about the validity of observations and the authenticity of intercepted communications. Materials that continue to be assiduously studied in the PRC for lessons and techniques integral to their quest to formulate "military science with unique Chinese characteristics" are emphasized.

Mark Wheeler, 29th Intelligence Squadron, Fort George G. Meade, MD

The Way Xi Moves: Understanding Chinese Behavior in Proper Strategic and Cultural Context

The U.S.-China relationship will be one of the defining features of the rest of the 21st century. To make sense of Chinese behavior and to properly support decision makers, U.S. intelligence analysts must understand the fundamental differences that exist between Chinese and Western strategic thought and perception. China's long and well-documented history of strategic thought provides many ideas that are either unique or hold a distinct level of influence relative to their Western counterparts. The strategic concept, Shi, and the prominent role that stratagems play in Chinese thought, are two prominent examples of this unique strategic tradition. Chinese strategic culture is even built on a strategic model that differs from the "Ends, Ways, Means" model that dominates Western strategic thought. Furthermore, Chinese perception is far more holistic and contextual than perception in the United States. Properly grasping all of these differences is incredibly difficult, not just because all of these differences must be overcome, but also because of the depth and breadth of Chinese strategic culture that form the foundations upon which Chinese strategic thought is built. Nonetheless, to properly contextualize Chinese behavior and intentions, the intelligence community must study these unique ideas in depth.

Improving Intelligence Panel

Fred Hoffman, Mercyhurst University

The A2E Integrated Intelligence Model: Integrating Five Types of Intelligence to Improve Organizational Performance

The A2E Integrated Intelligence Model blends technology and humanity to support strategic decision-making. The A2E model builds upon the Data-Information-Knowledge-Wisdom (DIKW) hierarchy as its theoretical foundation to integrate five different types of intelligence into a unified and coherent framework: Artificial Intelligence (AI), Business Intelligence (BI), Competitive Intelligence (CI), Decision Intelligence (DI), and Emotional Intelligence (EI). Integrating these five types of intelligence into a cohesive framework provides a simple, yet powerful, mental model to help organizational strategists and business executives conceptualize an effective approach to problem-solving. The successful strategy developed by the U.S. consumer electronics retail giant Best Buy in response to the disruption caused by the online retailing phenomenon serves as a case study to illustrate the relevance and efficacy of this model in a real-world business scenario.

Mary Beth Moore, SAS

Improving Intelligence with AI

As technology has rapidly advanced over the past two decades, intelligence analysis has largely remained impervious to technological transformation. Taking a systems approach to embedding AI throughout the intelligence cycle, I will share tangible ways to improve intelligence activities and the quality of analytical output by allowing AI to augment the efforts of human analysts in meaningful ways. This includes dynamic dashboards and Common Intelligence Pictures powered by AI, incorporating predictive analytics from a data science lens into human generated assessments and measuring the impact and quality of intelligence produced. This presentation will discuss different types of AI technology and how each can contribute to more robust analysis to provide leaders with increased accuracy of information, better transparency into processes and stronger situational awareness from which to make decisions.

Regional – Middle East Panel

Samiah Baroni, National Intelligence University

The Commodification of Islam

The Commodification of Islam is a part of everyday life in a contemporary world that should be explored. Whether it resembles a form of Islamic capitalism, a rebellion against the Western form of capitalism, or an attempt to incorporate Western commodities into traditional societies, the Commodification of Islam represents one of the most lucrative markets in the world.

Vangala Ram, National Intelligence University (on behalf of Paul Kubik, Signals Intelligence and Advanced Geospatial Intelligence Officer, WA, DC)

Iran: Pariah State, Rogue Nation

Pariah State, Rogue Nation – these are two of the many platitudes of U.S. foreign policy often used to describe Iran since 1979. The concept of Rogue States took hold during the Clinton Administration1, and the subsequent four U.S. administrations continued using this moniker to describe threatening or menacing nation-states. Simultaneously, multiple books and articles posited that the U.S. is the ultimate rogue nation due to apparent flouting of international norms and use of hard power to bring other nations to heel. In the debate of which nations are (or are not) rogue, little agreement exists about specific actions or policies that constitute the markings of a Rogue Nation, and whether this term is accurate or holds meaning beyond the images conjured in the minds of the citizens whose leaders use this term. Moving one step further, if the international community believes a nation to be rogue, then what are the steps other nation-states can take to bring the "Rogue Nation" back to the international community? This paper will ask these questions about Iran and seek to more precisely define whether Iran is truly rogue, and if so, what are the best ways for the U.S. to engage with Iran.

Matthew Walker, Independent Scholar (co-author, Hersh A. Hama Karim, University of Sulaimani, Iraq)

The Intellectual Case in Kurdistan

After attaining the informal independence of the Kurdistan Region in 1991, the intellectual Kurds were distanced from the center of decision-making, although they had a great role in the liberation movement against the Iraqi authority during 1921 to 1991. In this movement, they had succeeded in spreading the importance of humanity and nationalism to their community and also pushed towards Kurdish independence in 1991. The intellectual case appeared when the Kurdistan regional government was established in 1992. Under the Kurdish rule, Kurdish intellectuals had been kept away from the center of decision-making and were marginalized by Kurdish political parties. The aim of this research is to show the importance of the appearance of the intellectual case in Kurdistan, and examine the reason why Kurdish intellectuals are not part of tor are poorly connected to decision-making in their region. Is this reason related to the Kurdish community and political parties? Or is it traced back to the Kurdish youth themselves who are the root of the problem?

Terrorism – 1 Panel

M. Afzal Upal, Mercyhurst University

Grievances are Status Enhancing Myths

Previously I have argued for using social identity theory (SIT) to better understand terrorism and for designing more effective narratives for countering terrorist propaganda. Social dominance theory (SDO) builds on SIT to explain that high status groups use hierarchy-enhancing myths to maintain and enhance their higher status. This paper argues that lower status groups also use myths (dubbed "status-enhancing myths") in an attempt to raise their status. Many of these myths are expressed in the form of grievances against the higher status group. I illustrate this model using examples of grievances by groups such as Pakistani Jihadist groups against India and Palestinean groups against Israel.

Duane C. Young, National Intelligence University

Thoughts on Terrorism in Warfare

This paper arises from a serious of conversations with colleagues going back at least a decade concerning how the phenomenon of terrorism is perceived both in government and the academy, and consequently, how best to deal with it. Considerable public pronouncements and much ink spilt in government documents and academic publications seems to point to a belief in those circles that perpetrators of terrorist acts are simply criminals who can be dealt with by apprehension, indictment, trial, and incarceration. Such perpetrators are often referred to in government and academic publications and the news media with labels like "terrorist," "terrorists," and "terrorist organizations." Such simplistic labels of terrorism as criminal acts ignore what seems to be a deeper understanding of the problem. Such perpetrators are in fact members of sociopolitical organizations that employ terror as a tactic and terrorism as a strategy to achieve their political objectives. Such groups are, in fact, engaged in waging war against the states and peoples that are the target of their terrorist acts, and the failure of government, the news media, and the academy to recognize that fact is a significant contributor to the failure to defeat such groups. Easy labels like "the war on terrorism" are an oxymoron because one is arguing one can wage a war on a tactic and a strategy, failing to recognize that while one can always oppose one strategy with another, one must ultimately defeat the sociopolitical groups, whether state or non-state actors, who are employing terrorism as a strategy.

NIU Graduate Student Cyber Panel

Christopher M. Hines, National Intelligence University

Supply Chain Risk Management: Viewing ICT Supply Chains as Complex Adaptive Systems

This paper presents a method to improve Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) processes. The paper examines if the application of complexity theory will assist managers in the Intelligence Community (IC) and elsewhere with SCRM management. It examines ICT supply chain problems by employing three case studies from the public and private sectors to depict how the application of complexity theory might have assisted managers. So far, this paper's research indicates that SCRM managers and analysts who study SCRM can improve their decision-making if they think about supply chains as complex adaptive systems (CAS) that can mutate organically and imperceptibility, without warning. This paper intends to propose a framework for managers to handle changes to SCRM ecosystems by developing their own set of tools to increase efficiency and reduce risk. This paper hypothesizes that understanding supply chains as CAS will lead to stronger, more stable and resilient SCRM processes and therefore to increased cybersecurity.

Meredith Doran, National Intelligence University

Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM): A Risk Management Framework to Understand and Reduce Vulnerabilities

Supply chains in the public and private sector have been affected by globalization. It has made the world more accessible by decreasing cost and increasing global connection. However, it has increased vulnerability and risk to ensuring the integrity of a product. The lack of visibility into how technology is developed, manufactured, and supplied challenges the decision maker's ability to procure new equipment. Adversary strategies have evolved from traditional kinetic engagement to asymmetrical effects on the Department of Defense's (DoD) supply chain, and procurement of information communication technology (ICT). This paper provides a risk management matrix for procurement decisions. It assesses China's threat to microelectronic supply chains, the impact of outsourcing manufacturing, and DoD ICT procurement methods. The paper advocates enhanced relationships between government and the private sector, threat awareness, and mitigation techniques to reduce vulnerabilities. Additionally, it includes results of a study of ICT equipment in the U.S. financial sector, and compares the supply chain mitigation techniques with the DoD to understand, decrease, and remove risks to ICT supply chains. The views expressed do not reflect the official policy or position of the National Intelligence University, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

Historical – "Eisenhower Era" Panel

Nicholas Dujmovic, Catholic University of America

Prisoners of the Chicoms: Eisenhower and the CIA-China Dilemma

Dwight Eisenhower won the 1952 presidential election on the expectation that he would best lead America during the Cold War against the worldwide Communist threat. In addition to the large issues—the war in Korea, difficult relations with Communist China, and tensions with Moscow—Eisenhower inherited the smaller matter of two CIA officers shot down and imprisoned by the Chinese late in 1952. This paper will begin juxtaposing the secret CIA flight from South Korea into Manchuria on the very same day that President-Elect Eisenhower left the United States on his secret trip to Korea in fulfillment of his campaign promise to "go to Korea." Beijing actually held more than a dozen Americans, but the affiliation and activities of the two CIA officers—caught in the act of aggressive US operations against the People's Republic—complicated their case. This paper will demonstrate that the Eisenhower administration initially tried to insist that the CIA officers should be treated like other American detainees in China, but later found it expedient to admit tacitly that their case was different—an approach that prolonged their imprisonment. Downey and Fecteau were finally released during the Nixon administration.

Jean-Michel Turcotte, JFK Institute for North American Studies/Freie Universität, Berlin

"Observing Communist Soldiers": US Intelligence Policy and the Captivity of North Korean and Chinese POWs, 1950-1953

This presentation focuses on the treatment of North Korean and Chinese prisoners of war (POWs) during the Korean War. During this conflict, US authorities detained thousands of enemy prisoners in camps. The surveillance of POWs became then an opportunity to collect information from enemy captives. Indeed, different information gathered from prisoners was valuable to American intelligence to evaluate morale of enemy soldiers, to improve security of the detention, and also to understand a "dangerous" ideology. This paper examines these operations and argues that surveillance policy on POWs was shaped accordingly to intelligence efforts to collect, extract, and gather material from what the authority called

"Communist prisoners." This research also explores the case of the 150,000 North Korean and 25,000 Chinese soldiers held as prisoners of war in South Korea between 1950 and 1954, mainly at Koje-do camp. To sum up, this paper explores the practice and method of captivity used against ideological enemies and thus how important surveillance was for intelligence and political warfare. It intends to explain how the intelligence agencies transformed a large volume of information considered as relevant on POWs into practical knowledge pertinent for the detention of war policies, but also for allied war effort.

Intelligence in "Other Than War" Panel

J. Scott Braderman, U.S. Army War College (co-author, Piotr Ziemkiewicz, Deloitte LLP & 203rd Military Intelligence Battalion, U.S. Army Reserve)

Peacekeeping and Stability Activities Lack Intelligence Indicators Leads to Protracted Conflict

The U.S. intelligence community (IC) predominantly focuses intelligence collection and analysis on targeting belligerents which pose a threat to regional stability and development initiatives, which should be aligned with U.S. national security policy and interest. Post Conflict, Failing and Fragile States, and Natural Disaster responses mandate an infinitely nuanced analytical construct devoted to mitigating root causes of conflict and enhancing the populations' support and trust in the Host Nation government. This paper will address the challenges facing the IC in utilizing traditional collection strategies and analytic models in an ineffectual attempt to provide insightful and relevant assessments to decision makers in a peacekeeping and stability activities (PSA) environment. PSA intelligence support might be more beneficial if focused on assessing capacity building initiatives and their effects on popular support for the host nation government. PSA indicators will assess the cumulative effects of development projects have on each stability activity. This paper will attempt to answer: Will focusing collection in a PSA environment not only enhance capacity building and legitimacy efforts, but also reduce U.S. engagement time in those conflicts?

Kristina A. Young, National Intelligence University

Thoughts on Asymmetric Warfare

This paper encapsulates a series of discussions many of my colleagues and I have had over the years as we wrestled with this rather amorphous concept—"asymmetric warfare." Our students find it most frustrating as they try to frame "asymmetries" in such a way as to satisfy a demanding senior decision-maker, providing certainty in an otherwise uncertain field. Despite 30 years of books, journal articles, and studies, there remains a considerable divergence on the definition of asymmetric warfare. From a military intelligence perspective, this is problematic as the concept lacks a viable lexicon with a concomitant lack of doctrine and analytical frameworks with which to frame the problem. This paper offers another, perhaps simpler, definition of asymmetric warfare, not as a "silver bullet," but as a conceptual starting point for a deeper and more tailored analysis in support of the warfighter and senior decision-maker.

Cyber Panel

Gregory S. Laidlaw, University of Detroit Mercy and Charles E. Wilson, University of Detroit Mercy

Enhancing Cyber Security: Applying and Cyber Intelligence Techniques

This paper proposes the application of cyber threat intelligence to enhance cybersecurity and information assurance in the U.S. Currently, the nation, the public and private sectors, and American citizens are under attack by a growing community of transnational criminal organizations, a cadre of sophistication cyber criminals and a host of nonstate actors. The core of these attacks manifests themselves in the form of three-prong assaults, consisting of cybercrime, cyberterrorism and cyberwarfare. To effectively counter these attacks, this paper recommends an innovative approach for enhancing cybersecurity by fusing cyber forensics, data mining, and advanced analytic techniques into a comprehensive operational model. By addressing the education of cyber defenders as well as providing guidelines for the effective employment of an integrated cyber intelligence framework, the model will improve the operational cybersecurity capabilities of all enterprises and individuals operating in the cyber space environment.

Sarah Freeman, Idaho National Laboratory
The Challenges of Attribution Within Cyber Space

In December 2015, three Ukrainian regional electrical utilities experienced a disruptive cyber attack resulting in an outage for nearly 250,000 people. Although the events on December 23rd only lasted for four hours, they emphasized the challenges of government response following cyber attacks against critical infrastructure. Deterrence strategies in related fields (i.e., chemical attacks and terrorist events) are based on the premise that the global community can define appropriate and acceptable norms of behavior and, in the event that these norms are breached, that assigning attribution for the attack is possible and can be achieved quickly. However, cyber attacks present unique challenges for attribution, namely, that the origin and motivation of cyber attacks can be distorted, cyber weapons can be stolen and re-purposed, and false flag operations are possible. Additionally, the cyber ecosystem is complex with government programs drawing from a variety of third party programs and developers. Given the complexity of the cyber domain, new approaches are needed to respond to these attacks, establish international norms, and develop deterrence strategies. This paper aims to identify the unique challenges of attribution within the cyber space and proposes recommendations for intelligence analysis within these constraints.

Historical – ETO

Sarah Anna-Maria Lias Ceide, University of Naples Federico II
ODEUM Rome – German-Italian Intelligence Collaborations (1945-1956)

If much of Western Germany's intelligence history has been researched, some aspects still remain in the dark. That's in fact the case of the so-called "ODEUM Rome," the Italian base of the unofficial German post-war intelligence agency Organisation Gehlen. Founded in 1946 by US Army Forces and a former German Wehrmacht official, the Gehlen Organization passed under the CIA's supervision in 1948 and went on to be one of Federal Germany's three official secret services in 1956. The existence of an intelligence bureau tied to the Gehlen Organization and based in Rome is proven by a series of CIA documents. It has recently been estimated that ODEUM Rome was created around 1948/1949, but this has yet to be confirmed. As a matter of fact, nothing or little is known about the Gehlen Organization's anti-communist activity in Italy shortly after World War II and its collaboration with the Italian intelligence agencies on that matter. I therefore intend to present a research briefing of my ongoing studies for my Ph.D thesis which will focus on this still unknown chapter of intelligence history.

Elizabeth A. Coble, U.S. Army - XVIII Airborne Corps and Fort Bragg
Allied Intelligence Leading Up to Operation MARKET GARDEN

With German forces on the run in northwestern Europe, Allied forces were staged to enter Germany in late summer 1944. Both Field Marshal Bernard Montgomery and Lieutenant General George Patton clamored to be given the priority of effort. General Dwight Eisenhower chose Montgomery's Operation MARKET GARDEN as the plan for action. With mission success, the German Ruhr industrial heartland would be within easy reach. But the operation failed. Between 17 and 26 September 1944, there were 17,000 Allied casualties including 80 percent of the British 1st Airborne Division. It took six more months before Allied forces accomplished the final task of the planned operation. Was a lack of Allied intelligence about German forces in the operations area partly at fault for this failure? This paper will examine primary sources to determine what intelligence was available to inform senior Allied leaders about German force disposition in the area of operations before the operation. This will include all source intelligence, signals intelligence (SIGINT), human intelligence (HUMINT), and imagery intelligence (IMINT), reporting as well as diaries, memoirs, and autobiographies from Allied senior leaders.

Terrorism – 2 Panel

J. Scott Braderman, U.S. Army War College and Maura Reilly, Dickinson College

Mitigating Terrorism and Transnational Organized Crime Links: A Focus on Facilitators

The Department of Defense views non-uniformed combatants as terrorists, and counters the network by eliminating senior leaders. Terrorist organizations maintain their operational funding and logistical support by leveraging Transnational Organized Crime (TOC) black market connections. This paper will focuses on the importance of identifying and targeting "facilitators" that directly or indirectly enable and assist illicit operations. The paper will compare and contrast existing criminal and strategic intelligence analytic methodologies and mitigation principles for countering terrorist and TOC networks. The goal is to develop a common collection and analytic model for criminal and strategic intelligence analyst to develop collaborative finished intelligence products to mitigate the nexus between TOC and terrorist elements by targeting facilitators. The paper will incorporate case studies of two illicit businesses—human trafficking in Spain and antiquity trafficking in Syria- to identify patterns and roles of facilitator behaviors across criminal networks, in order to develop a set of early warning indicators. This paper will attempt to answer: How does the analytic methodology and intelligence collection strategy to mitigate a political insurgency differ from that of a criminal insurgency?

Musa Tuzuner, Mercyhurst University (co-author, Mehmet Arican, Homeland Security Consultation LLC)

U.S.-Turkey Anti-Money Laundering (AML) International Cooperation: The Case of Gold Trader Reza Zarrab

This study aims to discuss the ineffectiveness of international cooperation between US and Turkey against Iranian international money laundering efforts. Iran has had great ambitions of being a regional power along with seeking nuclear power. However, the sanctions imposed on Iran by the US and other Western countries were obstacles on their way towards achieving this goal. Thus, Iran declared an economic jihad to eliminate the severe economic consequences of the imposed sanctions, and Turkish-Iranian Reza Zarrab, who himself is a son of a smuggler, crafted and executed an international ML scheme to get money into Iran. This study will explain how this Money Laundering (ML) scheme was executed through the vulnerabilities of Turkish AML regime/system. It will also examine the driving factors for the ineffective international cooperation between the United States and Turkey both before and during the trial of Reza Zarrab. Finally, based on our findings and the Financial Action Task Force (FATF) general recommendations we will craft country specific recommendations for how to improve current Turkish-US AML cooperation and Turkish AML cooperation with other international actors.

M. Afzal Upal, Mercyhurst University

Scientific Fundamentalism and the Need for Meaning

While fundamentalism has been suggested as one of the drivers of intergroup conflict and terrorism, it is not well understood as to why some believers develop an overly zealous attachment to their belief system while others do not. Recently, a number of psychologists have proposed that differences in people's motivations (e.g., need for a consistent and coherent meaning system and people's need to feel that they can control their environment) may account for these differences. While the use of the term "fundamentalism" to refer to an unwavering attachment to a set of irreducible religious beliefs has become widely accepted leading to thousands of publications in the scientific literature as well as the popular press, its usage to refer to an overly zealous attachment to a non-religious belief system is more recent but its popularity also appears to be growing. Despite a growing interest in scientific fundamentalism, little work done to date to empirically study people's overly zealous attachment to a scientific worldview. This paper will review empirical studies conducted to better understand the notion of scientific fundamentalism.

Methods for Decision-Makers Panel

Stephen Downes-Martin, U.S. Naval War College

How an Opponent Wargames is an Intelligence Collection Requirement

The answer to "How does an opponent wargame?" supports decision-makers when deterring, preempting, or reacting to conflict. How opponent decision-makers wargame during peacetime, i.e. the methods, techniques, and styles of gaming used, and the beliefs and psychological biases of the players, gives us insight into how opponent decision makers might operate during conflict. This is in addition to the scenarios, systems, and concepts they game which one can credibly infer from the political, economic, and military environments. Since studying the performance of individual decision-makers during real life planning and conflict tells us something about how those decision-makers might behave in future conflicts, then how they behave during wargames should tell us something about how they would perform during the future conflict that they are currently wargaming. Studying the wargaming approaches of an opponent or ally and the wargame performance of selected military and political leaders should be an intelligence collection requirement. In this presentation, I propose an analytic framework for answering the wargame intelligence question based on the "Purpose of the Wargame" and the "Characteristics of the Wargamers" for each identified opponent group that "does wargaming," and propose methods for avoiding such collection on oneself.

Christopher Mansour, Mercyhurst University

From Cyber Rick to Cyber Security

Living in this digital economy with a plethora of smart devices and an abundant amount of data exposes individuals, organizations, and businesses to multiple threats. Today's organizations are being attacked daily by numerous threats starting from phishing, spyware, and trojans, reaching to ransomware which have cost organizations billions of dollars in losses and recovery. This is not to mention the legal repercussions and sanctions due to privacy regulations such as the GDPR. In the presentation titled "From Cyber Risk to Cyber Secure," you will be introduced to different types of attacks and their consequences on individuals and organizations. You will also be introduced to easy steps that you can take in order to secure yourself and your organizations in the cyber space and mitigate the risks.

Intelligence Education Panel

Michael Fowler, U.S. Air Force Academy

A Pedagogical Approach to Country Analysis

This paper resides in the overlap between Military Intelligence, Security Studies, and Intelligence Methods and Data Analysis. Too often, unconstrained intelligence research results in an overwhelming amount of data that is not useful to the decision maker. This article presents a pedagogical approach to teaching country and organizational analysis and associated centers of gravity (COG) for operational planning. COG analysis is arguably one of the most difficult analytic concept to apply. While students can easily memorize the various definitions, they struggle to describe potential centers of gravity when given real-world situations. Student analysts excel at collecting data but struggle to put it into context. They can gather background data on countries and organizations but students frequently struggle to analyze this data through the paradigm of the specific problem that they are trying to solve. This leads students to rely upon overly simplistic rules of thumb on clichés to identify COGs which, in turn, jeopardizes operational planning.

Kathleen Moore, James Madison University

New Fronts of the Cyber War and Intelligence Education

Cyber warfare is taking on a new front as both organized and singular threats to national security leave Surface Web and move to the anonymous areas of Dark Web. Security analysts and law enforcement professionals face unique challenges in targeting, tracking, and analyzing this dynamic and multi-faceted technological environment. Myths and misconceptions about this area of the World Wide Web lead many universities to discourage the formal study of the Dark Web, and most leading Intelligence and National Security programs do not offer technical instruction in this area. This work will address the myths and offer a proposed educational framework for Cyber Security instructors wishing to inform and train future analysts in this critically underserved area.

Brécourt Academic Author's Guidelines

The deadline for ICF 2020 delegates to submit a paper is November 15, 2019.

We are in the process of updating and completely revising our "Author's Guidelines" and the new version will not be available for some time, but the following will provide a few of the basics.

As for word count, anything between 8,000 and 15,000 words is acceptable, and feel free to take as much space as you require for footnotes, which can be used for sources and supplementary text (all notes must be footnotes; not endnotes). Generally, at least 60% of the sources cited in the footnotes must be primary source material, unless other arrangements have been made with the editor.

The manuscript should be single-spaced, with double-spacing between paragraphs (do not indent the beginning of paragraphs). Please submit the manuscript via email and attached as a Word document. Also, it would be helpful to refer to a recent issue of *Global War Studies* to get a sense of the journal's editorial style regarding footnote citations for books, articles, etc. (eg. always use p. or pp. for all page number references and, when initially cited, all book titles must be complete, including the subtitle). And, of course, all material must be original and not previously published in any form.

Initial book citations should be in the following format: Winston S. Churchill, *The Second World War*, Vol. IV, *The Hinge of Fate* (London: Cassell, 1951), p. 81; James Neidpath, *The Singapore Naval Base and the Defence of Britain's Eastern Empire, 1919-1941* (Oxford: Clarendon Press, 1981), pp. 174–78.

After the initial citation, books should be in the following format: Churchill, Second World War, Vol. IV, pp. 125–32; Neidpath, Singapore Naval Base, p. 183.

Archival references must be in descending order. Following are two examples of descending order (see below):

Example 1) The National Archives, London (hereinafter TNA), ADM 223/688, Essay by Grand Admiral Dönitz on the war at sea, 24 September 1945.

Example 2) TNA, ADM 223/172, Note on E-boat Operations in the English Channel, January–May 1944.

You may use Ibid., but not op. cit.

Ships should be referred to as follows: Early the next morning, *Bismarck* was located. (NOT: Early the next morning, the *Bismarck* was located.)

The article should be divided into sections, each with its own heading, with the first section labeled **Introduction** and the final section labeled **Conclusion**. *Do not use sub-sections or sub-headings.*

Use a single space between sentences (do not double-space between sentences).

All maps, graphs, and tables should be sent separately—not embedded in the text—with each as a separate file. PNG is the preferred file format. Place a marker (Insert Table 1 here) in the text to indicate where the map, graph, or table is to be positioned. Copyright information must be provided for all maps, graphs, and tables.

Also, please include (as a separate Word document) a one-paragraph abstract of 170 words or less. The abstract should provide a brief summary of the article's purpose, scope, and objectives and communicate to the reader the article's results and/or conclusions. We will also need a list of 8–10 of the article's keywords.

REGISTERING YOUR DEVICE ON THE MERCYHURST NETWORK

The registration of your computer or network enabled device for use on the Mercyhurst network will occur when you first attempt to access the internet on the Mercyhurst campus. All PCs (laptops and desktops) and other network enabled devices must be registered through the Bradford Campus Management system to provide internet access while on the Mercyhurst campus.

Username: eventsguest

Password: Lakers1926

Instructions on Registering your Computer on Bradford Campus Manager

Step 1: Connect your PC to the Mercyhurst Network

- Make sure you are connected to the network using either wireless or wired – do not connect both to do the registration.
- If using wireless, make sure you connect to LakerVapor.
- If using wired make sure you have a Cat5e Ethernet cable and plug it into the DATA Wall Jack – if you have wireless connectivity on your computer do not connect to LakerVapor when you plug in the wired connection.

Step 2: Registration Process

- Double-click your Internet Explorer/FireFox icon to open your browser.
- Your browser will be automatically directed to the Mercyhurst Network Registration pages.
- Read the Acceptable Use Policy / Code of Conduct.
- After you read the policy and if you agree to it, click on the Accept button.
- Select the Next >> button.
- Select the "Guests" Start>> button.
- On the Welcome/DOWNLOAD page:
- Enter your Guest UserName, Password, and Reason for Visit.
- Select the Download button.
- Successful notification will appear when you are registered. Wait the designated 70 seconds for the registration to complete before browsing.

HOUSING INFORMATION

Here is important information you should know about living at Mercyhurst this summer.

Please excuse our appearance as we are still in the process of cleaning and completing maintenance in our residence halls and on campus. There is always an Assistant Director (AD) on call who can help if you are facing an issue/have housing concerns.

IMPORTANT PHONE NUMBERS:

Residence Life (Main) 814-824-2422	Maintenance 814-824-2273
Police and Safety 814-824-3911	AD "on duty" 814-824-3889

GENERAL RULES:

The rules, regulations, policies, and the Student Conduct Code apply over the summer. The Student Handbook, including the Conduct Code, is available online at ***handbook.mercyhurst.edu***

- Quiet Hours are from 10 p.m. to 8 a.m. during the week and from midnight to 11 a.m. on the weekends. We look at these hours for summer guests as "Courtesy Hours."
- Open Containers of Alcohol are not permitted outside apartments (including stairwells, laundry rooms, etc.).
- Dumpsters are located near each building, please do not leave your trash in the hallway.
- No pets are allowed!
- No candles/incense are permitted!
- No smoking or use of tobacco products in and around campus property. We are a tobacco-free campus!
- If you have a maintenance emergency (after 4:30 p.m. Mon-Fri or on Sat/Sun), please call Police and Safety for help.
- When you go to leave campus, please drop your key off at Police and Safety, located at the bottom of McAuley Hall.

We hope you enjoy your stay!

Residence Life and Student Conduct Office
Egan Hall 323
814-824-2422 • *reslife@mercyhurst.edu*

NOTES

NOTES

Carpe Diem 1926

MERCYHURST
UNIVERSITY

mercyhurst.edu