Annual National Security Colloquium

Cyber Threats to the U.S. Government and Private Sectors

Tomás Rivera Conference Center
Union Building East
The University of Texas at El Paso
March 18-19, 2015

Welcome!

On behalf of the faculty, staff, and students of the National Security Studies Institute—An Intelligence Community Center for Academic Excellence, I welcome you to our annual national security colloquium. This year we will be examining "Cyber Threats to the U.S. Government and Private Sectors." We have a wonderful assortment of distinguished speakers from academia, the U.S. Intelligence Community, law enforcement, industry, and our student cohort to discuss this critical national security issue, perhaps one of the most important of our time. Over the past several years, cyber threats have risen to the top of the nation's security agenda. As a key tool, strategic enabler, and force multiplier of terrorist groups, criminal organizations, and nation-state adversaries, it represents a supreme challenge to the United States and its allies.

This special event also marks our successful Intelligence Community Centers for Academic Excellence grant proposal earlier this year. This major U.S. Government grant valued at $1.86 million provides tremendous career-enhancing opportunities for our students including immersive strategic language instruction, study abroad, and analytic training to name a few. This grant also positions our academic unit as one of the leading centers for intelligence and security education in the country. Our federally sponsored Intelligence Community Center for Academic Excellence has a long tradition of placing our highly qualified and talented students into critical positions in the U.S. Intelligence Community. We are committed fully to serving UTEP students, the U.S. Intelligence Community, and the nation!

Our success would not be possible without the continuing support of our senior administration, especially Dr. Diana Natalicio, UTEP President, Dr. Patricia Witherspoon, Dean of the College of Liberal Arts, and Dr. Roberto Osegueda, Vice President for Research. I would like particularly to thank Dr. Damien Van Puyvelde for his valuable leadership in organizing this colloquium. Additionally, I would also like to extend my sincere appreciation to Mr. Justin Magee and the Students in Intelligence and National Security for co-sponsoring this event.

Many thanks to all of our participants, stakeholders, and other guests joining us for our colloquium! We hope you enjoy your time on our beautiful UTEP campus.

Go Miners!

Larry A. Valero, Ph.D.
Director, National Security Studies Institute

Colloquium Program

Wednesday, March 18

8:30 – 9:00	Registration and Refreshments
9:00 – 9:10	**Introduction:** Dr. Larry Valero, Director, National Security Studies Institute
	Welcome: Dr. Diana Natalicio, President, The University of Texas at El Paso
9:15 – 10:30	**Keynote Address:** Dr. John Sheldon, George C. Marshall Institute – "The Search for the Mackinder of the Digital Age: A Geopolitical Model for the 21st Century"
10:30 – 11:00	*Coffee Break*
11:00 – 12:30	**Panel: Intelligence and Diplomacy in the Cyber Age**
	Chair: Dr. Damien Van Puyvelde, National Security Studies Institute Discussant: Dr. John Sheldon, George C. Marshall Institute
	Dr. Rich Andres, National Defense University – "Inverted Militarized Cyber Diplomacy"
	Dr. Michael Warner, U.S. Cyber Command – "The Future of Intelligence and Military Power in the Digital Age"
	Mr. Stephen "Scuba" Gary, University of South Florida – "The Evolution of Cyber Intelligence"
12:30 – 14:00	*Lunch Break*
14:00 – 15:15	**Panel: Cyber Threats (I)**
	Chair: Dr. Michael Warner, U.S. Cyber Command
	Mr. Travis Rosiek, FireEye – "The New Normal: Cyber Attacks and Effective Defense in the Modern Era"
	Supervisory Special Agent George Quinlan, FBI – "The Current Cyber Threat Landscape as it Pertains to the U.S. Government and the Private Sector"
	Dr. David Gray, Campbell University – "Cyber Security: Advanced and Persistent Threats to National Security"
15:15 – 15:30	*Coffee Break*
15:30 – 16:30	**Panel: Cyber Threats (II)**
	Chair: Mr. Travis Rosiek, FireEye
	Mr. Jeff Gibson, El Paso County Sherriff's Office – "Cyber Crimes: The Use of Cyberspace for Criminal Purpose"
	Special Agent Michelle Liu, FBI – "Cyber Threats to Higher Education"

Thursday, March 19

9:00 – 10:15 **Keynote Address:** Dr. Derek Reveron, Naval War College – "The Rise of China and the Future of Cybersecurity"

10:15 – 10:30 *Coffee Break*

10:30 – 12:00 **Panel: Cybersecurity**

Chair: Dr. Larry Valero, National Security Studies Institute
Discussant: Dr. Derek Reveron, Naval War College

Dr. Damien Van Puyvelde, National Security Studies Institute – "From Information to Cyber Security: Bridging the Public-Private Divide"

Mr. Kevin Lawrence, Accenture and the Intelligence and National Security Alliance – "The Insider Threat"

Mr. Tomás Armendariz, FBI – "Best Cybersecurity Practices for the Private Sector"

12:00 – 13:30 *Lunch Break*

13:30 – 15:00 **Panel: Training Tomorrow's Cyber Workforce**

Chair: Dr. Sara McGuire, National Security Studies Institute
Discussant: Dr. Larry Valero, National Security Studies Institute

Brig. Gen. (Ret.) Scott Bethel, U.S. Air Force, and Mr. John Wisehunt, Independent Consulstant – "Training Coalitions on Cyber and Intelligence Capability: Building Capability through Familiarity and Relationships"

Dr. Matthew Gonzalez, University of the Incarnate Word – "A 360 Approach to Cyber Security"

Dr. Mario Caire, UTEP Office of Research and Sponsored Projects – "Hands-On Cyber Security Labs for Non-Technical Majors"

Dr. Elbert Basham, Sul Ross State University – "Developing a Cybersecurity Curriculum and Degree"

15:00 – 15:15 *Coffee Break*

15:15 – 16:15 **Panel: Leveraging Cyberspace**

Chair: Dr. Larry Valero, National Security Studies Institute
Discussant: Dr. Michael Landon-Murray, National Security Studies Institute

Mr. Gary Adkins, Intelligence and National Security Studies Alumnus – "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism"

Mr. Sean Curtis, Intelligence and National Security Studies Graduate Student – "Cyber Capabilities of the Developing World: Tuareg Rebels in Northern Mali"

16:15 – 16:30 **Closing Remarks**

Dr. Larry Valero, Director, National Security Studies Institute
Dr. Patricia Witherspoon, Dean, College of Liberal Arts

Speakers and Abstracts

Mr. Gary Adkins, Intelligence and National Security Studies Alumnus – "Read Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism"

This paper is a feasibility study on using targeted cyber attacks to combat terrorism.

Mr. Adkins is currently Special Projects Administrator at the Teachers Federal Credit Union of El Paso.

* * *

Dr. Richard B. Andres, National Defense University – "Inverted Militarized Cyber Diplomacy"

Cyber weapons create an incentive structure for interstate militarized bargaining fundamentally different from conventional or nuclear weapons. According to traditional theory, weapons exist mainly to back diplomatic threats, and military power is the currency of diplomacy. Unlike other weapons, however, cyber weapons generally require secrecy to be effective; announcing their existence removes their ability to cause harm. Thus, they cannot easily be used in militarized diplomacy. In this paper I describe how cyber weapons create an incentive to invert the usual pattern of militarized diplomacy. In this new model, states strike first, taking whatever they can with cyber weapons, then use diplomacy to prevent their opponents from retaliating. The model is illustrated with three brief cases of ongoing instances of inverted militarized cyber diplomacy.

Richard B. Andres is a senior research fellow at the Institute for National Strategic Studies and full professor at the U.S. National War College. His work focuses on national security strategy and particularly cyberspace. Previously, he was Associate Professor of Security Studies at the School of Advanced Air and Space Studies. Dr. Andres has held a number of posts in government including Special Advisor to the Secretary of the Air Force and Special Advisor to the Commander of Air University (24 schools, colleges and think tanks). Dr. Andres specializes in developing national security strategy and has led teams of general officers and senior executives developing strategy for the White House, Chief of Staff of the Air Force, Commandant of the Marine Corps, the Office of the Secretary of Defense, several combatant commands, and other civilian and military institutions. He was awarded the medal for Meritorious Civilian Service by the Secretary of the Air Force and the Joint Unit Meritorious Service Award by the Chairman of the Joint Chiefs of Staff. Dr. Andres received his Ph.D. in Political Science from the University of California, Davis and wrote his dissertation under Randolph Siverson, Miroslav Nincic, Scott Gartner, and Kenneth Waltz.

* * *

Mr. Tomás Armendariz, FBI – "Best Cybersecurity Practices for the Private Sector"

* * *

Dr. Elbert Bassham, Sul Ross University – "Developing a Cybersecurity Curriculum and Degree"

This presentation focuses on steps taken to identify and define the courses comprising the Computer Science Cyber Security Concentration of the Computer Science degree at Sul Ross State University. It will address preliminary research; the NSA/DHS CAE/IAE designation; determining the course levels, names, and descriptions of the courses in the program; the degree plan, and working through the higher education local and state processes. This development is funded with a Title V HSI/STEM grant from the Department of Education.

Elbert Bassham came out of retirement to help build the Computer Science Cyber Security curriculum and degree at Sul Ross State University. He is spearheading the work to obtain the NSA CAE/IAE designation for this degree. He organized a Cyber Security Symposium held on November 13th last year. He has a strong background in institutional research and strategic planning from his earlier employment at Sul Ross. He has experience with data mining from his work subcontracted with the Department of Homeland Security via the North Central Texas Fusion Center.

* * *

Brig. Gen. (Ret.) Scott Bethel, U.S. Air Force, **and Mr. John Wisehunt**, Independent Consultant – "Training Coalitions on Cyber and Intelligence Capability: Building Capability through Familiarity and Relationships"

In the past, our developing U.S. cyber intelligence community was a relatively small group of highly skilled people, who built relationships based on circles of trust. This circle was closed and limited to other U.S. intelligence, communications, and Information Operations personnel. U.S. cyber-operators and crews were based in a few small, secured locations; they knew one another through the dynamics of tight teamwork; and generally executed very focused, limited information campaigns. Some commentators would argue that the U.S. was too protective of its technical solutions. Others were quick to demonstrate the utility of cyber solutions in all levels of warfare — both inside and outside the Department of Defense. Those who advocated for more openness believed there was value in maximum collaboration and sharing the basic tenets of network-based tradecraft. Through a balance of protection and sharing, the U.S. has developed successful coalitions, spanning dozens of member governments and combined command structures. All of these relationships are based on international directives, but they grew and functioned on familiarity, and have been sustained through trust. In the future, coalition building, predominantly through training and joint exercises will be the key to better defense from cyber attack, but more importantly more effective cyber defense. The closer the U.S. can get to its allies, the better protected all will be against the growing source and sophistication of cyber threats to government and industry.

Scott A. Bethel is an Intelligence, Surveillance and Reconnaissance leader with 27 years of education, training, intelligence, cyber, kinetic targeting, and unmanned vehicle operations experience.

Currently, he is the Vice President for Intelligence Education and Training for JMark Services—a Training and Education Company. He is also Senior Vice President for Governmental Affairs at Delta Risk—a Cyber Policy, Strategy, and Operations Company. He is also Visiting Distinguished Practitioner of Intelligence at Angelo State University and pursues a number of community initiatives in San Antonio and San Angelo, Texas.

Brig Gen Bethel is at the center of government and industry solutions for cyber and intelligence training, education, and strategy. His most recent government position was as Vice Commander, Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) where he oversaw the organization, training and equipping of assigned forces to conduct intelligence and cyber operations for the United States Department of Defense. He was the senior operator for the Air Force Distributed Common Ground Station (DGS) and was the Air Force's Senior Targeting Officer. He served as the commander of the 17th Training Wing where he was in charge of the initial training for all U.S. Air Force intelligence and cyber-intelligence personnel. His other assignments include Deputy Director of Operations for Technical Training at the U.S. Air Education and Training Command where he was responsible for all initial skills training of Air Force personnel in all career fields. During his three years in this role, he was responsible for placing more than 100,000 new recruits into the U.S. Air Force fully trained. He has also held various command, staff, and budget positions at all levels including Headquarters U.S. Air Force. Brig Gen Bethel has spoken and published extensively on the topics of cyber and intelligence strategy, policy and operations as well as on strategic thinking and developing leaders.

* * *

Dr. Mario Caire, UTEP Office of Research and Sponsored Projects – "Using Computer Labs to Teach Cybersecurity"

This presentation demonstrates the utility of hands-on cyber security labs for non-technical majors. The labs provide step-by-step tutorials on information gathering, identifying reachable targets, and system intrusion. The objectives are to provide students with training to enhance education and awareness, to expose students to technical aspects of cyber security, to increase interest in the field, and to provide introductory knowledge of cyber security testing and ethical hacking. Two targeted outcomes of the labs are to increase the number of students interested in cybersecurity and to develop students who recognize the need for lifelong learning in this field. The labs utilize various commands and programs available in both Windows and Linux systems. Students are also introduced to remote access tools such as Putty Secure Shell, which enables them to remotely access LINUX servers. Students have been very responsive to these labs and find them interesting and fun. They are encouraged to work in teams to facilitate comprehension and solve problems faster than working alone.

Dr. Caire is a cyber-security researcher and web-based application and database programmer at the Office of Research and Sponsored Projects at The University of Texas at El Paso (UTEP). He is also an adjunct instructor for both the National Security Studies Institute and the Criminal Justice Department at UTEP where he teaches cybersecurity related courses. He received a B.A. degree in Psychology from the University of Texas at Austin in 1992. In addition, he earned an M.S. and Ph.D. in Electrical and Computer Engineering from UTEP in 2003 and 2012 respectively.

* * *

Mr. Sean Curtis, Intelligence and National Security Studies Graduate Student – "Separatist Militancy in Mali: What Cyber Means for the Developing World"

Access to Internet connection can now be found not only in the bustling metropolises of New York and London but also in Internet cafes from Mogadishu to Kano. The effect of growing cyber capabilities across the world for U.S. national security is not limited to major powers such as Russia and China or even to well-established terrorist groups like Al-Qaeda and ISIS. Small rebel groups in rural areas of third world countries across the globe have access to the Internet to create websites and social media accounts. The Internet has thus become a common tool, used by many non-state groups to empower their operations and messages. One group benefitting from Internet access is the Mouvement National de la Liberation de l'Azawad (MNLA), which fights for an independent state in northern Mali. Online presence adds an entirely new dimension to information operations, propaganda, and basic communication for the group, fighting in the rural Sahara. Not since the proliferation of cellular phones in the region and across the continent has a technological advancement like the Internet and associated cyber networks revolutionized the way conflicts are approached and conducted.

Sean Curtis is a Master of Science in Intelligence and National Security Studies candidate at the National Security Studies Institute at the University of Texas at El Paso. Mr. Curtis has research interests in African security, U.S. foreign policy in Africa, and conflict and war studies. Mr. Curtis is currently working on several projects on the topics of extrajudicial assassinations of Rwandan dissidents, the MNLA independence movement in Mali, and U.S. foreign policy toward Horn of Africa states.

* * *

Mr. Stephen "Scuba" Gary, University of South Florida – "The Evolution of Cyber Intelligence"

Cyber Intelligence is one of the newest buzzwords in the cybersecurity community, and different commentators seem to use it in very different ways. A shared understanding of the basic terms and concepts is needed to lay the foundations of cyber intelligence as a discipline of practice and study. Although the word "cyber" can be somewhat ambiguous, the term "intelligence" is probably the greatest

source of confusion. It is easy to equate intelligence with information and to use the terms interchangeably, but in practice they really are quite different. In the cyber domain, data are abundant, information is common, and intelligence is rare. Five years ago, the term "cyber intelligence" was seldom used, but in recent years it has been employed routinely to characterize an approach to cybersecurity and to advocate for new solutions. The moniker, however, is not always used correctly. This paper discusses the conceptual foundations and practical implications of defining cyber intelligence and describes how the field has been evolving so far.

Stephen "Scuba" Gary is an Assistant Professor of Practice in the School of Information (College of Arts and Sciences) at the University of South Florida (USF). He has a background and expertise in intelligence, specifically cyber intelligence. Prior to joining the USF faculty, Mr. Gary developed, and served as Chief of, the Cyber Intelligence Support Element at U.S. Special Operations Command; as a Deputy Division Chief at the National Security Agency/Central Security Service; as Cryptologic Support Team Officer in Charge for the Combined Joint Special Operations Task Force in Iraq; and as an Adjunct Instructor at Joint Special Operations University. He was a highly-decorated career Intelligence Officer and Russian Linguist/Interpreter in the U.S. Air Force, and a Reserve Police Officer for the Biloxi (MS) Police Department. Steve earned a B.S. degree from Regents College and an M.S. in Cyber Operations from the Air Force Institute of Technology. He currently holds a Security+ certification (CompTIA). His academic interests are intelligence, cyber intelligence, cybersecurity, cyber operations, and analysis tools and methods. He does research for and networks with many organizations in the Tampa Bay area. His primary courses of instruction are: Cyber Intelligence and Advanced Cyber Intelligence.

* * *

Mr. Jeff Gibson, El Paso County Sherriff's Office – "Cyber Crimes: The Use of Cyberspace for Criminal Purpose"

The Internet, or cyberspace, is being used to facilitate a myriad of criminal activity. Currently, criminals use it to capture valuable identity data and financial data for use in identity crimes. The monetary loss alone to the private citizen and the financial corporate sector is staggering. It is used to share illegal images of child victims of sexual abuse among sexual predators, and to advertise the illegal prostitution of young men and women. Organized criminal elements use the Internet to communicate, and to gather intelligence on their rivals, and on law enforcement personnel. "Scams" and confidence crimes have enjoyed resurgence with the use of this powerful tool to trawl for victims. As the Internet lacks boundaries or borders (a good part of its allure and power), the capability of law enforcement to investigate these crimes, as well as the prosecutors to bring these offenders to trial, is significantly diminished.

Jeff Gibson is a 23-year veteran of the El Paso County Sheriff's Office. He is a certified instructor, who has had the privilege of teaching federal, state, and local law enforcement officers for more than 20 years. Additionally, he has taught law enforcement related courses at El Paso Community College. Detective Gibson began his career as a corrections officer, and has served as a patrolman and an investigator for the Sheriff's Office. He has been certified in both basic and intermediate computer forensics by the National White Collar Crime Center, and investigated public corruption and financial crimes for almost seven years. He has developed several database applications for law enforcement over the years, some of which are still in use. Detective Gibson is currently serving as a gang intelligence detective with the West Texas High Intensity Drug Trafficking Area Investigative Support Center on an FBI Gang Task Force.

* * *

Dr. Matthew Gonzalez, University of the Incarnate Word – "A 360 Approach to Cyber Security"

This presentation will provide an interdisciplinary approach to designing and developing cyber security curriculum involving various university-wide resources, federal, state, and local level resources, and most of all the voice of the student.

Matthew D. Gonzalez, Ph.D., PMP, is an Associate Faculty member who serves as the Bachelor of Science in Business Administration (BSBA) Coordinator within the University of Incarnate Word's (UIW) Extended Academic Program. Dr. Gonzalez oversees seven concentrations within the BSBA program on ground and online. He specializes, teaches, and conducts research in information technology, leadership, project management, and entrepreneurialism for such universities as Harvard, Temple, Brandeis, and Northeastern.

While working at UIW as an adjunct professor in the evenings, Dr. Gonzalez worked as an IT Developer, Systems Analyst, IT Architect, and IT Project Manager for United Stervices Automobile Association (USAA), a global financial services provider. His lessons learned and successes at USAA in managing $10+ million dollar projects and programs provided him with the necessary experience to pursue multiple entrepreneurial endeavors to include GSI Event Production (2001), and Events Education (2004) where he founded and eventually sold each of the profitable organizations to pursue his doctorate.

Dr. Gonzalez' latest endeavor outside of his teaching profession was launched in 2010 as *M.D. Gonzalez, LLC* focusing on leadership building for new and mid-level managers, and curriculum development/review for organizations and government entities in excess of 100 employees.

Dr. Gonzalez earned his BBA in Information Systems from the University of Texas at San Antonio, MBA from St. Mary's University, Ph.D. in Organization and Management from Capella University, and MIS from Keller Graduate School. Dr. Gonzalez stays active in his community where he serves his Church as an ACTS team member.

* * *

Dr. David H. Gray, Campbell University – "Cyber Security: Advanced and Persistent Threats to National Security"

Cyber security is undoubtedly a most pressing national and international security issue. This presentation will address some of the crucial factors relative to this emerging threat, and focus on key concepts of cyber security. It will conceptualize and operationalize many important dimensions of cyber security, and present an approach and framework to factually, contextually, and strategically assess, and deal with cyber security. Specifically, areas that are addressed include such topics as strategic assessment, risk, costs, attribution and deterrence, as well as, highlights some of the most serious threat actors. An assortment of current and descriptive examples will be provided to illustrate and demonstrate key elements of cyber security. Future forecast and projection of cyber security, combined with coverage of important ramifications, implications and lessons-to-be-learned provide an engaging and fascinating discussion. Finally and most importantly, this research provides a perspective that supports a calculated and disciplined approach to policy formulation and implementation when contending with this important issue of cyber security.

Dr. Gray specializes in international and national security affairs. His expertise includes U.S. and international security and strategic studies; current global security issues; U.S. foreign and national security policy formulation and strategy; intelligence; political violence and insurgency; international terrorism; and international weapons proliferation.

A retired U.S. Air Force officer, Dr. Gray is also a former Foreign Service Officer. He has extensive experience in the national and international security and intelligence communities and has completed

assignments for the United States Departments of Defense, Energy, Homeland Security, Justice, and State, as well as, the United Nations, the Congress and the National Intelligence Council. He also served in a number of overseas assignments in various parts of Europe, Asia, Africa, and the Middle East and has worked with many defense, corporate, law enforcement, security and intelligence organizations and services worldwide.

Dr. Gray has taught graduate and undergraduate courses for more than a dozen universities. Currently, he teaches undergraduate and graduate courses at Campbell University, the University of North Carolina-Chapel Hill, the University of North Carolina-Wilmington, and Norwich University. Previously, he taught graduate international security courses at the University of Denver Graduate School of International Studies and the University of Colorado.

For decades, he has taught graduate and undergraduate courses in international security studies in academe and government. Dr. Gray has taught national and international security and strategic studies courses at the National Defense University, Air University, Naval War College, Joint Forces Staff College, Marine Corps University, JFK Special Warfare Center and School, USAF Special Operations School, USAF Academy, and the Naval Postgraduate School. He has also taught national and international security courses at the Defense Intelligence Agency National Defense Intelligence College, National Security Agency National Cryptological School, National Geospatial-Intelligence Agency National Imagery School, Department of Defense Intelligence Technical Training Center, CIA. Kent School for Intelligence Analysis and several other Central Intelligence Agency and Federal Bureau of Investigation operational education and training centers. He has lectured at U.S. Army Special Operations Command, U.S. Marine Corps Special Operations Command and U.S. Air Force Special Operations Command.

Drawing upon his professional and academic experience, Dr. Gray is a much-sought-after speaker and has published extensively on national and international security topics with special emphasis on International Terrorism and Strategic Intelligence. He completed his undergraduate work at Brigham Young University and holds a doctorate from the University of Southern California. He also finished post-doctoral coursework at Columbia University.

* * *

Mr. Kevin Lawrence, Accenture, and Intelligence and National Security Alliance – "The Insider Threat"

This presentation will provide an overview of the insider threat program with an emphasis on its significance for cleared defense contractors. Particular attention will be paid to the growth of the insider threat program in the cyber community. The presentation will be based on true stories of insider threat cases and statistical data.

Kevin Lawrence is the Director of the Accenture Federal Services (AFS) Intelligence Security Division. In 2006, Kevin took employment with AFS and within his first few months of hire, wrote the AFS' corporate Counterintelligence (CI) and Insider Threat Program (CIITP). The CIITP includes a Cyberintelligence Program, All-Source Analysis Group, and the corporate Incident Response Program. Prior to AFS, Kevin served as the senior strategic planner for CI, to the Strategy and Transformation Directorate to the Counterintelligence Field Activity (CIFA).

In 2006, after 22 years of active duty service, Mr. Lawrence retired from the U.S. Marine Corps as a Chief Warrant Officer. He holds CI credentials from the Marine Corps and the Defense Intelligence Agency (DIA). He is also a trained Offensive Foreign CI Officer, Master Anti-Terrorism Specialist, a Certified Criminal Investigator (CCI), and a certified Intelligence Collection Manager. He has 30 years of experience in the Intelligence Community (IC), ranging from Small Mission Units, to the highest levels of the U.S. Government. Mr. Lawrence has extensive experiences in conducting CI & Human Intelligence (HUMINT) operations, investigations, safeguarding intellectual property,

physical/information security and competitive intelligence collection. He has coordinated, directed, and conducted CI and security liaison efforts with U.S. National and foreign law enforcement, and intelligence agencies worldwide.

Mr. Lawrence served as the Branch Chief to the National HUMINT Technical Collections Division for the Department of Defense (DoD), conducting test and evaluation of current/future technologies on offensive sensitive collection platforms within the scope of real world strategic missions. In 2004, he deployed to Iraq in support of Operation Iraqi Freedom as the Senior Offensive Technical Intelligence Collection (OTIC) Officer. In this capacity, Mr. Lawrence coordinated with national level organizations and agencies in remote and hostile locations in the approval and conduct of all DoD OTIC operations, surveys, surveillance and countersurveillance activities. He provided critical technical equipment/training, fabrication, and CI operational support to DIA, the U.S. Special Forces Groups, and other Government Agencies.

While assigned to DIA, Mr. Lawrence served in the Pentagon as a CI Action Officer to the Chairman of the Joint Chiefs of Staff (CJCS), J2CI Staff Office, the DIA, and the Office of the Assistant Secretary of Defense (C3I). Mr. Lawrence chaired and instructed the DIA Joint CI Staff Officer Course at the Joint Military Intelligence Training Center, where he was also a principal advisor to the Joint Special Operations Task Force (JSOTF) on CI support to Joint Operations. Mr. Lawrence also served as a senior staff advisor for DIA on CI equities at the Federal Bureau of Investigation's Headquarters in Washington DC, following the terrorist attack on September 11, 2001. While assigned to the Pentagon, Mr. Lawrence managed and authored the editing and revision of numerous Joint and DoD CI policies and doctrine, and assisted in the development and the validation of national intelligence collection requirements for the CJCS, DoD and the CI Community, and assisted in the development of the first Joint Interagency Task Force for Counterterrorism.

Mr. Lawrence served in numerous operations across the globe as a CI Special Agent conducting CI and HUMINT activities and operations, such as - Iraq, "Operations Iraqi Freedom"; Southwest Asia, "Operations Desert Storm/Shield"; Africa, "Operations Provide Relief/Restore Hope"; Combined Task Force, "Operation Northern Watch"; Joint Task Force Southwest Asia, "Operation Southern Watch"; International Force for East Timor Multinational non-United Nations Peacekeeping Taskforce, "Operation Stabilize". During the Gulf War in 1991, Kevin was handpicked to debrief the senior Marine Corps Officer held Prisoner of War (POW).

Over the course of his career, Mr. Lawrence has provided classroom instruction and certified over 600 military, DoD and Federal Government persons in Counterintelligence Support to Operations. He also provided instruction on "The National U.S. Intelligence Community" at George Mason University and Trinity Washington University. Mr. Lawrence is a collaborative author to the book *Steeling the Mind: Combat Stress Reactions and Their Implications for Urban Warfare*; published in 2005 by the RAND Corporation. Mr. Lawrence is currently a member to the Intelligence and National Security Alliance (INSA) Homeland Security Intelligence Council (HSIC), and their Cyber Insider Threat Task Force, and collaborative author to INSA's recent white paper titled "A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector." He is currently working as a collaborative author to publish another white paper for INSA, focused on Homeland Intelligence.

* * *

Special Agent Michelle Liu, Federal Bureau of Investigation – "Cyber Threats to Higher Education"

This presentation will provide case studies of FBI investigations that have impacted academia and students. An emphasis will be put on cases of economic espionage and their ties to the academic realm.

* * *

Supervisory Special Agent George Quinlan, Federal Bureau of Investigation – "The Current Cyber Threat Landscape as it Pertains to the U.S. Government and the Private Sector"

This presentation will discuss current cyber threats to the U.S. Government and the Private Sector.

* * *

Dr. Derek Reveron, Naval War College – "The Rise of China and the Future of Cybersecurity"

China's emergence as a great power in the twenty-first century is strongly enabled by cyberspace. Leveraged information technology integrates Chinese firms into the global economy, modernizes infrastructure, and increases Internet penetration, which helps boost export-led growth. China's pursuit of "informatization" reconstructs industrial sectors and solidifies the transformation of the Chinese People's Liberation Army into a formidable regional power. Even as the government censors content online, China has one of the fastest growing Internet populations and most of the technology is created and used by civilians. Western political discourse on cybersecurity is dominated by news of Chinese military development of cyberwarfare capabilities and cyber exploitation against foreign governments, corporations, and non-governmental organizations. Western accounts, however, tell only one side of the story. Chinese leaders are also concerned with cyber insecurity, and Chinese authors frequently note that China is also a victim of foreign cyber attacks— predominantly from the United States.

Derek Reveron is a Professor of National Security Affairs and the EMC Informationist Chair at the U.S. Naval War College in Newport, R.I. He specializes in strategy development, non-state security challenges, intelligence, and U.S. defense policy. He has authored or edited nine books. The latest are *China and Cybersecurity* (co-edited by Oxford University Press, 2015), *US Foreign Policy and Defense Strategy* (co-authored by Georgetown University Press, 2015), and *Cyberspace and National Security* (edited by Georgetown University Press, 2012). Dr. Reveron is a faculty affiliate at the Belfer Center for Science and International Affairs at Harvard University where he co-teaches a course on contemporary national security challenges at the Kennedy School of Government. He received an MA in political science and a Ph.D. in public policy analysis from the University of Illinois at Chicago.

* * *

Mr. Travis Rosiek, FireEye – "The New Normal: Cyber Attacks and Effective Defense in the Modern Era"

This presentation will discuss the evolution of cyber attacks and threat actors, with insights on where exploits are happening today and why. Mr. Rosiek will discuss a current threat landscape that is more complex than ever, with security teams finding it increasingly difficult to prevent, detect, analyze and respond to advanced attacks. Drawing on FireEye's experience with a range of government and industry organizations, this presentation will touch on where we are making progress, and what can be done to address the new and increasingly sophisticated tactics being used by attackers.

Travis Rosiek is the Chief Solutions Strategist in the CTO office supporting Global Government. In this role, he provides technical and executive support to help ensure the FireEye implementation addresses the evolving security challenges that Federal Government organizations face. He also assists in educating customers on the evolving cyber threats, understanding customer requirements, and influencing FireEye solutions. Prior to joining FireEye, Mr. Rosiek was a Principal Cyber Security Consultant at McAfee. Prior to joining McAfee, Travis spent nearly 10 years at the Department of Defense (DoD) in various roles including: management, security architecture, CND analyst, and as an engineer supporting DoD Enterprise Information Assurance programs, CND Operations centers, Incident Response, Red Team, C&A, Metrics, and many others. In addition, he supported several of the COCOMS, services, and agencies to integrate systems and operations in an effort to enable Cyber Defenders to be more effective in defending their networks. Mr. Rosiek received his M.S. in Electrical Engineering, with a concentration

in Information Assurance and Biometrics, from West Virginia University. In addition, he has completed the Executive Leadership Development Program (ELDP) at George Washington University.

* * *

Dr. John Sheldon, George C. Marshall Institute – "The Search for the Mackinder of the Digital Age: A Geopolitical Model for the 21st Century"

Implicit in many analyses of the use of cyber power in international politics and foreign policy is that classical realist geopolitics no longer matter. Even when the term "geopolitics" is used in such analyses it is as though the geography has become unmoored from the political context. While there is undoubtedly a geographical foundation to cyberspace because of its physical infrastructure of computers, cables, and satellites, it is widely assumed that the geographical setting has no relevance to the political use of cyber power by states and non-state actors. This paper argues that while cyberspace shrinks time and space in many obvious ways, the geographical setting still matters in the use of cyber power. Further, with the return of great power competition and its attendant geopolitical tensions, it is argued that cyberspace and its strategic expression, cyber power, will play a critical role in the geopolitics of the 21st century, and therefore any geopolitical model must account for it. The paper concludes by offering some ideas of what such a model might look like, building on the theories of Sir Halford Mackinder and Nicholas Spykman.

John B. Sheldon, Ph.D., is the Executive Director of the George C. Marshall Institute, in Arlington, Virginia; founder and owner of the Torridon Group LLC, a space and cyberspace consultancy; Senior Fellow at the Atlantic Council; and a Senior Fellow in Global Security Studies at the Munk School on Global Affairs at the University of Toronto in Canada.

Prior to his current positions, Dr. Sheldon was Professor of Space and Cyberspace Strategic Studies at the U.S. Air Force's School of Advanced Air and Space Studies (SAASS), at Maxwell AFB, Alabama. For over six years John taught the National Security Space course, and founded, directed, and taught the Intelligence, Information, and Cyberspace course.

A former British diplomat, Dr. Sheldon holds his bachelor and master's degrees from the University of Hull, UK, and a Ph.D. in politics and international relations from the University of Reading, UK.

* * *

Dr. Damien Van Puyvelde, National Security Studies Institute – "From Information to Cyber Security: Bridging the Public-Private Divide"

This presentation will assess the extent to which intelligence contractors pose a risk to information security within the U.S. intelligence enterprise. An examination of the PERSEREC espionage databases and a series of more recent cases of cyber-espionage shows that intelligence contractors have been a relatively frequent target of hostile infiltration, although certainly not a more frequent target than government employees. On the whole, the challenges faced by the U.S. government and its private "partners" in the domain of information security point out the need for better government control of the private sector, and increased public-private cooperation to secure cyberspace.

Damien Van Puyvelde is an Assistant Professor of Security Studies and Associate Director for Research at the National Security Studies Institute at the University of Texas at El Paso. He has worked as a Research Assistant at the Centre for Intelligence and International Security Studies at Aberystwyth University, UK, and Assistant Editor for the journal *Intelligence and National Security*. His main research and teaching interests include Intelligence and Security Studies, issues of democratic accountability, and public-private "partnerships" in the security sector. Dr. Van Puyvelde is currently writing a book on *The U.S. Intelligence Community and the Private Sector*.

* * *

Dr. Michael Warner, U.S. Cyber Command – "The Future of Military and Intelligence Power in the Digital Age"

Every armed conflict today involves the use of digital-dependent weapons and communications, and features opponents striving to use the Internet for communications, recruiting, propaganda, and possibly for frustrating the other side's uses of cyberspace. In addition, Western states rely on networked technology in ways that leave them vulnerable to digital espionage, disruption, and destruction against those networks. This reality has developed despite recent academic debates over whether or not espionage, denial and disruption, and deception in cyberspace can constitute "war." These developments have significant implications. First, there remains considerable disquiet over how to defend and respond to aggressive actions in cyberspace, and the extent to which Western states should be involved in perpetrating such attacks. Second, the extension of power, force, and conflict into cyberspace has called for new forms and tasks for intelligence that will lead to new organizations and conceptions of the discipline. Finally, understanding the future requires a look back over the last century to chart the ways in which Western militaries and intelligence services were shaped by technology and ideology to develop precise, digital means of targeting adversaries in war and opponents at home-and how such means have spread globally.

Dr. Michael Warner serves as Command Historian at U.S. Cyber Command. He has written and lectured widely on intelligence history, theory, and reform, and he teaches as an Adjunct Professor at Johns Hopkins University and American University. His new book *The Rise and Fall of Intelligence: An International Security History* was published by Georgetown University Press in 2014. Essays and volumes include: "Cybersecurity: A Pre-History," *Intelligence and National Security* 27:5 (October 2012); "The Rise of the US Intelligence System," in Loch Johnson, ed., *The Oxford Handbook of National Security Intelligence* (Oxford, 2010); and "Building a Theory of Intelligence Systems," in Greg Treverton and Wilhelm Agrell, eds., *National Intelligence Systems: Current Research and Future Prospects* (Cambridge, 2009).

The National Security Studies Institute – An Intelligence Community Center for Academic Excellence

The National Security Studies Institute is dedicated to the concept of advancing intelligence and security education for the purpose of providing for the national security of the United States. The institute prepares students academically and professionally for the challenges of the current cyber era characterized by increasing speed, complexity, and uncertainty and requiring a deeper understanding of the nexus between culture, technology, and conflict. The institute's aim is to educate our students to be as innovative and adaptable as the constantly evolving security challenges that currently face our nation and allies. The institute provides creative learning experiences that balance both theory and practice. We are a full spectrum educational enterprise comprising synergistic undergraduate, graduate, and research components, and embrace cultural awareness and strategic language proficiency.

Students in Intelligence and National Security (SINS)

Students in Intelligence and National Security (SINS) is an organization that seeks to enhance and enrich the learning experience of both graduate and undergraduate students at UTEP who have an interest in the field. SINS brings together students, academics, and practitioners from the El Paso area and across the globe to engage in educational and professional events for mutual benefit. SINS holds events for students to meet one another and to work more closely with NSSI faculty. We organize events such as recruitment visits, seminars, workshops, and disseminate information about the ever-growing intelligence and national security field.

National Security Studies Institute
An Intelligence Community Center for Academic Excellence
The University of Texas at El Paso

500 W. University Ave.
Kelly Hall, Rm. 218
El Paso, Texas 79968

Tel: (915) 747-5865
Fax: (915) 747-8504