On the morning of February 24, 2010, at Georgia Tech’s Wardlaw Center, the Director of National Intelligence Centers of Academic Excellence gathered panel speakers from the Intelligence Community to discuss the present threat to cyber security in the United States. The Colloquium was designed especially for students who might want a career in intelligence or national security. Welcoming remarks were made by Kenneth J. Knoespel, Roy George, and Lenora Gant to begin the seminar. In attendance were GT professors, alumni, and students; and intelligence experts both in government and the private sector.

Conference participants:

Mustaque Ahamad  
Professor, College of Computing; Director, Georgia Tech Information Security Center

Lenora Gant  
Director, Office of the Intelligence Community Centers of Academic Excellence, ODNI

John W. Garver  
Professor, The Sam Nunn School of International Affairs, Georgia Tech

Roy George  
Chair, Computer and Information Science, Clark Atlanta University; Principal Investigator, ODNI Center of Academic Excellence

Seymour (Sy) Goodman  
Professor, The Sam Nunn School of International Affairs and College of Computing; Co-director, Center for International Strategy, Technology, and Policy; Co-director, Georgia Tech Information Security Center

Justin Hastings  
Assistant Professor, The Sam Nunn School of International Affairs, Georgia Tech

Steedman Hinckley  
Senior Analyst, Central Intelligence Agency

Don Jackson  
Director, Threat Intelligence, SecureWorks

Robert (Bob) Kennedy  
Professor, The Sam Nunn School of International Affairs, Georgia Tech

James Kilpatrick  
Coordinator, Director of National Intelligence Centers of Academic Excellence

Aaron Karczmer  
Vice President, Financial Intelligence Unit, American Express

Kenneth J. Knoespel  
Interim Dean, Ivan Allen College; Professor, School of Literature, Communication & Culture, Georgia Tech

Fred F. Manget  
CIA Officer-in-Residence, School of Public and International Affairs, UGA

Margaret (Peggy) Maxson  
National Security Agency; Education Portfolio Manager, Joint Interagency Cyber Task Force, ODNI

Rick Maxwell  
Assistant Special Agent in Charge (ASAC), Atlanta Division's National Security Branch, FBI

Michael Murphree  
Georgia Tech researcher

Jeff Moulton  
Information Operations Lead, Georgia Tech Research Institute

Kara Nance  
Professor and Chair, Computer Science Department, University of Alaska Fairbanks

Christopher Rouland  
CEO and Co-Founder, Endgame Systems

Gary Smith  
College of Cryptology, National Security Agency

Alan Trask  
Senior Program Manager, Office of the Intelligence Community Centers for Academic Excellence, ODNI

Brian Woodall  
Acting Chair and Associate Professor, The Sam Nunn School of International Affairs, Georgia Tech

Neal Ziring  
Technical Director, National Security Agency
Alan Trask, from the Office of the Director of National Intelligence (ODNI), opened with an “Introduction to the Intelligence Community.” He gave the background on the creation of the ODNI: the attacks of September 11, 2001 initiated the longstanding call for major intelligence reform and the creation of a Director of National Intelligence (DNI). Post-9/11 investigations included a joint Congressional inquiry and the independent National Commission on Terrorist Attacks upon the United States (better known as the 9/11 Commission). The report of the 9/11 Commission, in July 2004, proposed sweeping change in the Intelligence Community, including the creation of a National Intelligence Director (NID). On December 17, President Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) into law. The IRTPA created the Office of the Director of National Intelligence to improve information sharing, promote a strategic and unified direction, and ensure integration across the nation’s Intelligence Community (IC). The DNI serves as the President’s principal intelligence advisor; manages the National Intelligence Program (budget); establishes Intelligence Community priorities with clear and measurable goals and objectives; sets direction through policies and budgets; ensures coordination of integration of IC personnel, expertise, and capabilities; provides leadership on IC cross-cutting issues; and monitors IC agency and leadership performance.

The first panel was “Cyber Issues and 21st Century National Security” with Seymour Goodman as moderator and speakers Mustaque Ahamad, Kara Nance, and Neal Ziring

Kara Nance opened the panel by focusing on how we should handle increasingly complex technologies and the threat of attacks aimed at operating systems. By utilizing an International Multidisciplinary approach, we would be able to share information across fields to prevent overlap and increase research and development to create trusted environments in order to protect identity and privacy.

Mustaque Ahamad spoke on the “Age of Pervasive Information: Cyber Security Challenges and Opportunities.” Dr. Ahamad’s main question asks, “what are we to do with the vast amount of information that’s out there?” He touched on the growing sophistication of cyber security threats posed by nation state actors. Dr. Ahamad also highlighted the challenge of creating a denial of information attacks, which would limit our ability to exploit pervasive information. He explained three relevant projects currently being tested at Georgia Tech: ALPACA (a distributed user-centric system for organizing information online); Converging Infrastructure Security Lab (explores security challenges for emerging communications technologies); and Cleanse (a project to develop an analysis and detection framework to secure the internet against large scale and coordinated layer-8 attacks by botnets or future compromises).

Neal Ziring spoke about cyber issues and the concern of the National Security Administration (NSA) with cyber defense and its implications for national security. Mr. Ziring highlighted the fact that the U.S. depends heavily on cyber networks for our infrastructure and that exploitable vulnerabilities and weaknesses will always exist in our computer networks. Nations exploit cyber space for national advantages, and under the concept of the “new normal” the U.S. is always under attack. Mr. Ziring argued that cyber defense needs to be a strategic activity, not a tactic, and that our traditional security measures are not adequate. The NSA has goals of becoming timely, adaptable, and strategic in utilizing a three-part strategy: Protect, Defend, and Hunt. Cyberspace is a lawless wasteland that operates in a system of anarchy. It is a haven for criminal and terrorist activity which Mr. Ziring suggests can be deterred by having an “active defense” that would provide risks for the attacker.

Sy Goodman relayed that the DNI, under former Director Dennis Blair, in the 2010 annual security assessment to Congress, described the far-reaching impact of the cyber threat. Mr. Blair further explained how the IC plays a vital role in protecting and preserving our nation’s cyber interests and the continued flow of cyber information.
The next panel was entitled “Intelligence and the Private Sector” with Jennie Lincoln as moderator, and the speakers Chris Rouland, Jeff Moulton, and Aaron Karczmer.

Jeff Moulton started the panel with his discussion on Privacy vs. Intelligence. Mr. Moulton argued that there must be a balance between privacy and the need for intelligence, and that there must be some technological and political safeguards. Citizens need to be ensured of their rights to have medical records confidentiality, genetic privacy, RFID, and protection from data profiling. Today, with the extensive use of biometrics, video surveillance, wireless tracking, and the increased acts of identity theft, there is a stronger need for privacy protection for individuals.

Aaron Karczmer spoke about American Express and its Financial Intelligence Unit. It was established in 2007 and is tactically and strategically responsible for surveillance of money laundering and terrorist financing Mr. Karczmer stated that their goals included assessing risks and monitoring controls in order to understand products, how they should be used, and their vulnerabilities. They also try to define strategy and drive implementation of enterprise level investigation technology solutions.

Lastly, Chris Rouland discussed his company, Endgame Systems, and its relevance to Cyber ISR. He briefly went over the company’s structure and stated goals and objectives. Mr. Rouland also talked about the importance of the private sector interfacing with the government in cyberspace.

The luncheon speaker was Margaret Maxson of ODNI. Her talk was on the National Cyber Security Initiative and why cyber security is the most serious economic and national security challenge of the 21st century. Due to the multiplication of technologies worldwide, we face enormous challenges because of the speed and expansion of technological change. Our adversaries maintain a persistent and pervasive presence in our government networks and target our corporate intellectual property which comprises 70% of the world intellectual property. Ms. Maxson also touched on exposure, risk management, infrastructure vulnerability, and how criminal elements, terrorists, and non-state actors currently threaten us. It is no longer sufficient for the U.S. Government to discover cyber intrusions in its networks, clean up the damage, and take legal or political steps to deter further intrusions. We must take proactive measures to detect and prevent intrusions as they happen, and before they can cause significant damage.

The next panel was “Changing National Security Issues in Asia,” moderated by Brian Woodall with speakers John Garver, Justin Hastings, Steedman Hinckley, and Margaret Kosal.

Dr. Garver initiated the panel by talking about the maritime conflicts in East Asia, principally between Japan and China. The Chinese argue that the continental shelf, 200 nautical miles, and the historic sea principles, all support their claims to the territorial rights to the disputed waters between Japan and China. He also discussed the naval arms race in the region, and how the Chinese were aiming to enhance their naval capabilities to provide greater coercive influence among its neighbors. The U.S.-Japanese alliance is countering the Chinese naval build up by trying to better understand the hydraulic structure of the waters in Southeast Asia by mapping the area to gain information to be prepared in case of a naval altercation. Dr. Garver then turned to some of the problems involving the Russian Far East and its relationship to China. Due to the lack of development and infrastructure, the eastern population is decreasing at an alarming rate. A lack of foreign direct investment (FDI) in the region has caused a demographic crisis for the Russians. Dr. Garver suggested that Moscow allow Chinese FDI into the region and also provide migrant workers in order to build and sustain a sufficient working population in the region.

Justin Hastings spoke next about non-state actors and how they are empowered by technology to create vast networks that threaten the security of states. His focus was clandestine transnational networks in Southeast Asia
and the fact that they were embedded in local territories and the affect this had on their behavior. Dr. Hastings contends that due to pockets of non-governability in Asian nations, these networks thrive and flourish without any interference from government authorities. He used the case study of the attempted Singapore Terror Plot to illustrate how non-state networks operate in the region. Dr. Hastings spoke of the challenges of academic research on this subject and how there happens to be a sampling and selection bias in addition to problems of information gathering; most of the time, the only information sources available are textual sources and expert interviews. Another challenge is understanding midlevel intelligence and making it useful analytically.

Steedman Hinckley of the CIA then spoke about the changing of Asia from the Intelligence Community perspective. Mr. Hinckley focused on factors of change in China such as their progressive movement towards creating a more capitalist economy. He also highlighted the changes in the demographics and population in China as it relates to important factors that affect IC operations. Lastly, he touched on the process of urbanization in the region and what future challenges it will pose to the IC.

Margaret Kosal’s talk was entitled “The Strategic Significance of Emerging Technologies in Asia.” The focus was on nanotechnologies and how they pertain to international and domestic security. One question that Dr. Kosal posed was whether or not nanotechnology has any strategic significance and she also provided a chart illustrating the funding overview and trends in investments in nanotech. Dr. Kosal highlighted some key security factors regarding which included deniability and the lack of transparency; vulnerability perception; that there is no single discipline on which to focus; that intent must be balanced with capability; and globalization.

Michael Murphree’s talk, entitled “The Simple Logic of Perceived Madness: China’s Technology Standards,” focused on technology standards and how they work in emerging economies, and specifically, what the standards are in China and their implications.

The last panel to convene was entitled “The 21st Century Intelligence Community Enterprise: Challenges and Opportunities.” Robert Kennedy moderated with speakers John Garver, Steedman Hinckley, Neal Ziring, and Rick Maxwell. Except for Dr. Garver, all of the speakers on the panel are active members of the Intelligence Community.

Dr. Garver recommended some of the skills students would need in order to obtain careers in national security. He said that language and traveling abroad are important and that students should take advantage of intense summer programs in a region of interest in order to immerse themselves into the culture and gain regional awareness. He also suggested military service and that a student’s academic study should include theory, history, and computers.

Steedman Hinckley spoke about challenges to the Intelligence Community and how the CIA is handling their new missions and roles. Mr. Hinckley pointed out that the agency is focusing on tracking dangerous materials and people, and that this is harder today since the level of analysis has moved from the state level all the way down to the tribal level. Mr. Hinckley also noted the importance of students learning strategic languages that would further benefit the IC.

Rick Maxwell talked about the FBI and its role in the IC. He focused on how the FBI has undergone a change from being a more reactive agency (incident driven) in solving crimes to a more proactive agency (dealing with intelligence gathering in order to prevent crimes). Mr. Maxwell stated, “If I have to solve a terrorist attack, I have already failed.” He also noted that one of the FBI’s previous problems was the lack of information sharing with its counterparts in the IC, and that recently they have strived to improve their working relationship with the other agencies to better serve the American people.
Lastly, Neal Ziring talked about the challenges to the NSA. His talk lined up with that of Rick Maxwell in that he believed that the main goal should be the sharing of tradecraft and techniques across the agencies of the IC in addition to improve working together during missions. Mr. Ziring also spoke of the need for a balancing act between tactical and strategic objectives.

Closing remarks were given by Dr. Woodall and Dr. Gant, which concluded the seminar. Dr. Gant told students that she wanted them to help the IC isolate the issues, find and identify the best approaches and strategies, and use measures and metrics as indicators of success. She gave seven points, or secrets, for students to remember.

- The Intelligence Community (IC) tries to create decision advantages and in that regard tries to prevent lawlessness that could adversely impact our freedoms to be American and live the lives we have become accustomed to living.
- IC jobs or careers involve the thrill of the hunt.
- Very seldom does IC encounter the same problem twice.
- The IC is dealing with the new norm which is ever changing and will never again be constant.
- The academic enterprise is needed to help solve the plethora of problems we face today.
- There is a need for checks and balances. We need the new talent which includes the academic community, industry, and NGOs.
- The IC and America want to ensure that cyber security does not become the wild, wild, west.

Dr. Gant closed with a quote from former Director of National Intelligence, Dennis Blair: “We want talent that looks like America and the world. We want diverse talent. We want people who don’t think alike. We want people from different institutions to be involved in our business.” In her own words, “United we serve.”

Following was a reception so that students could network with experts in the IC; for many, this was an opportunity to discuss future employment.