A Primer on the AI and Cybersecurity Landscape in 2018, and What May Come Next: Technology, Ethics, & Policy

Executive Short Course

May 1, 2018
100 MARYLAND AVENUE, NE
SUITE 510
WASHINGTON, DC 20002
### Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00-9:30 a.m.</td>
<td>Registration</td>
<td>Suite 510, Fifth Floor, United Methodist Building</td>
<td></td>
</tr>
<tr>
<td>9:30-9:45 a.m.</td>
<td>Introduction</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>Kiron Skinner</strong>, Director, Institute for Strategic Analysis, Carnegie Mellon University</td>
</tr>
<tr>
<td>9:45-10:45 a.m.</td>
<td>Cyber Security Doctrine</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>Baruch Fischhoff</strong>, Howard Heinz University Professor, Departments of Social &amp; Decision Sciences, and Engineering &amp; Public Policy, Carnegie Mellon University</td>
</tr>
<tr>
<td>10:45-11:30 a.m.</td>
<td>Major Components of AI systems</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>Andrew Moore</strong>, Dean, School of Computer Science, Carnegie Mellon University</td>
</tr>
<tr>
<td>11:30-12:30 p.m.</td>
<td>Major Components of Cyber Warfare</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>Bill Scherlis</strong>, Director, Institute for Software Research, Director PhD Program in Software Engineering, School of Computer Science, Carnegie Mellon University</td>
</tr>
<tr>
<td>12:30-1:30 p.m.</td>
<td>Roundtable Lunch Break</td>
<td></td>
<td>Buffet served in conference room prior to lunch roundtable</td>
</tr>
<tr>
<td>1:30-3:00 p.m.</td>
<td>Advanced Cyber Autonomy</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>David Brumley</strong>, Bosch Security and Privacy Professor, Director CyLab, CMU Security and Privacy Institute, Electrical and Computer Engineering, Carnegie Mellon University</td>
</tr>
<tr>
<td>3:00-4:00 p.m.</td>
<td>Legal, Ethical, and Policy Issues for Autonomous Systems for National Security</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>David Danks</strong>, Department Head, Department of Philosophy, L.L. Thurstone Thurstone Professor of Philosophy and Psychology, Carnegie Mellon University</td>
</tr>
<tr>
<td>4:00-4:10 p.m.</td>
<td>Closing Remarks</td>
<td>Conference Rooms 1 and 2, First Floor</td>
<td><strong>Kiron Skinner</strong>, Director, Institute for Strategic Analysis, Carnegie</td>
</tr>
</tbody>
</table>
Parking and Transportation
Course Location

Our office is in the United Methodist Building at 100 Maryland Avenue NE, Washington, DC 20002. Parking is extremely limited around the building, so we suggest taking advantage of a taxi or the Metro (the office is approximately a 10-minute walk from both the Capitol South and Union Station stops). If you prefer to drive, there is hourly parking available in the public garage at Union Station.

The course will be taught in Conference Rooms 1 and 2. The conference rooms are located on the first floor of the United Methodist Building to the left of the elevators. Registration and the reception will be held in Suite 510, the Carnegie Mellon Offices. To access this office, you will take the elevator to the 5th floor, the suite is directly in front of either elevator.

Street Location:

100 Maryland Ave. NE
(Directly on the corner of First St. NE & Maryland Ave. NE)
Washington, DC 20002

Front of building and entrance:
Directions from Union Station Metro to the United Methodist Building (Visual on Following Page)

Union Station

1. Head

2. Walk for 157 ft

3. Take the stairway down to the 1st floor
   - Take the stairs

4. Walk for 213 ft

5. Head south toward Union Station Dr NE

6. Turn left onto Columbus Circle Northeast/Columbus Monument Drive Northeast
   - Continue to follow Columbus Circle Northeast

7. Slight right to stay on Columbus Circle Northeast

8. Continue onto First St NE

9. Turn left onto Maryland Ave NE

100 Maryland Ave NE
Washington, DC 20002
Directions from Capitol South Metro Station to United Methodist Building (Visual on Following Page)

Capitol South Metro Station
355 First Street Southeast, Washington, DC 20003

↑ Head north on First St SE toward C St SE
0.4 mi

↑ Turn right onto Maryland Ave NE
171 ft

100 Maryland Ave NE
Washington, DC 20002
Instructors
David Brumley is the Bosch Security and Privacy Professor at CMU, the Director of CyLab, the CMU Security and Privacy Institute, a Professor in ECE with an appointment in CS, and a founding member and academic advisor for a world ranked competitive hacking team. His research interests include all areas of security, with a specialization in software security. Prof. Brumley received his Ph.D. in Computer Science from Carnegie Mellon University, an M.S. in Computer Science from Stanford University, and a B.A. in Mathematics from the University of Northern Colorado. Brumley's honors include a United States Presidential Early Career Award for Scientists and Engineers (PECASE) from President Obama, a 2013 Sloan Foundation award and numerous best paper awards. Brumley's security startup ForAllSecure won the DARPA Cyber Grand Challenge that tested fully autonomous full-spectrum attack and defense cyber reasoning systems.
Dr. David Danks is Professor of Philosophy & Psychology, and Head of the Department of Philosophy, at Carnegie Mellon University. He is also an associate/adjunct member of: the Center for the Neural Basis of Cognition (CMU); the Center for Advanced Study of Language (Univ. of Maryland); and both the Department of History & Philosophy of Science and Center for Philosophy of Science (Univ. of Pittsburgh). He has received a James S. McDonnell Foundation Scholar Award, as well as funding from the NSF and NIH. Before arriving at CMU, he received an A.B. in Philosophy from Princeton University, an M.A. and Ph.D. in Philosophy from University of California, San Diego, and was a Research Scientist at the Florida Institute for Human & Machine Cognition.

His interests largely fall at the intersection of philosophy, cognitive science, and machine learning, using ideas and frameworks from each to inform the others. His primary research is in computational cognitive science: developing fully-specified computational models to describe, predict, and most importantly, explain human behavior. The fullest expression of that work can be found in his book, Unifying the Mind: Cognitive Representations as Graphical Models (2014; The MIT Press). More recently, his research has turned towards the role of humans in cyber-systems, with a particular emphasis on ethical challenges and opportunities during cyber-conflicts. He has published widely in philosophy, psychology, and computer science.
Andrew W. Moore is the fifth dean of the School of Computer Science at Carnegie Mellon University. He began his new role Aug. 18, 2014. A member of the CMU faculty since 1993, Moore’s appointment as the new dean of SCS marks a homecoming of sorts for the professor of robotics and computer science. He has been on a leave of absence from CMU since January 2006, when he opened the Pittsburgh office of Google Inc. While at Google, Moore has led projects to improve user experiences in advertising and shopping and to help combat fraud.

In October 2011, while continuing to serve as leader of Google’s Pittsburgh office, Moore was named vice president of engineering of Google Commerce, where he became responsible for developing new products and services.

Moore’s tenure at Google Pittsburgh has been characterized by the office’s rapid growth both in size and importance. Google Pittsburgh started with just two employees in a rented office on the CMU campus. It now includes more than 275 employees in 140,000 square feet in East Liberty’s Bakery Square development, located just a few miles from Carnegie Mellon. Work being done at Google Pittsburgh includes everything from the company’s signature search engine to shopping, advertising and the Android mobile platform.

Moore’s research interests broadly encompass the field of “big data”—applying statistical methods and mathematical formulas to massive quantities of information, ranging from Web searches to astronomy to medical records, in order to identify patterns and extract meaning from that information. His past research has also included improving the ability of robots and other automated systems to sense the world around them and respond appropriately.

From 2002 to 2005, Moore served as co-director of the Biomedical Security Center at the University of Pittsburgh, and along with Michael M. Wagner and Ron M. Aryel, he was editor of the Handbook of Biosurveillance, a guide to detecting and fighting outbreaks of communicable diseases in real-time.

In 2005, Moore was named a Fellow of the Association for the Advancement of Artificial Intelligence (AAAI) for his significant contributions to machine learning, data mining and statistical artificial intelligence, as well as for his role in transferring those technologies to industry and government.

A graduate of the University of Cambridge, where he studied mathematics and computer science, Moore was born in Bournemouth, U.K., Jan. 15, 1965, and began his career working
for Hewlett-Packard’s Bristol research lab. He returned to Cambridge in 1986 to earn his Ph.D. in computer science.

Moore spent three years as a post-doctoral researcher at the Massachusetts Institute of Technology before joining the CMU faculty. From 1995 to 2001, Moore served as co-founder and chief technology officer of a small, Pittsburgh-based consulting company specializing in data mining technology. He received a doctorate from the University of Cambridge in 1991 and joined the CMU faculty in 1993 following two years of post-doctoral research. In 2005, he was elected a fellow of the American Association for Artificial Intelligence. Andrew lives in Pittsburgh with his wife, Mary, and two children, William and Lucy.

Moore succeeds Randal Bryant, who will return to the CMU faculty after serving as dean since 2004.

**Education**
University of Cambridge, B.S., mathematics and computer science
University of Cambridge, Ph.D., computer science
William L. Scherlis is a Professor of Computer Science at Carnegie Mellon. He is director of CMU’s Institute for Software Research (ISR), one of seven academic departments in the School of Computer Science (SCS). ISR research and educational programs relate to software engineering, cybersecurity, privacy engineering, network analysis, mobility, systems assurance, and other topics. ISR is home to two PhD programs and six professional Masters programs. Scherlis founded the PhD Program in Software Engineering in 1999 and directed it for more than a decade. During 2012 and early 2013 he was the Acting CTO for the Software Engineering Institute, a DoD FFRDC at CMU. Dr. Scherlis joined the Carnegie Mellon faculty after completing a Ph.D. in computer science at Stanford University, a year at the University of Edinburgh (Scotland) as a John Knox Fellow, and an A.B. magna cum laude at Harvard University in applied mathematics.

Scherlis’s research focuses on techniques and practices for software assurance. His project emphasizes issues of scalability, composability, usability, and judicious use of fragmentary specifications, with a focus on the development of techniques to verify safe concurrency, information flow, and other properties that tend to defy conventional testing and analysis. Some of the technologies are commercialized through a Carnegie Mellon spinoff; these versions have been applied to larger systems such as Hadoop, the SE for Android framework, and Java system libraries including java.util.Concurrent.

Scherlis is principal investigator for the Carnegie Mellon / NSA Science of Security Lablet, which encompasses a diverse set of research efforts in multiple departments and colleges at CMU and also several collaborating academic institutions that address cybersecurity technical challenges related to composition and usability. He is principal investigator for a number of other efforts including a Systems Engineering Research Center (SERC) task focused on Systemic Assurance. He was previously the principal investigator for the Carnegie Mellon / NASA High Dependability Computing Project (HDCP), in which CMU led a collaboration with five universities (MIT, USC, U Wash, U Md, U Wisc).

Scherlis interrupted his early career at CMU to serve at Defense Advanced Research Projects Agency (DARPA) for six years, departing in 1993 as an SES-4. While at DARPA his responsibilities related to research and strategy in software technology, computer security, information infrastructure, and other topics. He was involved in the initiation of the high performance computing and communications (HPCC) program (now NITRD) and, with Pethia, Squires, and Druffel, in creating the concept of operations for CERT-like organizations, hundreds of which are now in operation world-wide.
Scherlis has testified before Congress on software rejuvenation, on innovation and information technology, and on roles for a Federal CIO. He chaired the National Research Council (NRC) study committee on defense software producibility, which recently released its final report *Critical Code: Software Producibility for Defense*. He served multiple terms as a member of the DARPA Information Science and Technology Study Group (ISAT). He also chaired a NRC study on e-government, and has led or participated in other national studies related to cybersecurity, crisis response, analyst information management, Ada, and health care informatics. He has been an advisor to major IT companies and is a founder of two Carnegie Mellon spin-off companies, Panopto and SureLogic. He has served as program chair for a number of technical conferences, including the ACM Foundations of Software Engineering (FSE) Symposium and the ACM Symposium on Partial Evaluation and Program Manipulation (PEPM). He has more than 80 scientific publications. He is a Fellow of the IEEE and a lifetime National Associate of the National Academy of Sciences.
In addition, Professor Skinner is a Distinguished Fellow at CyLab, a cyber-oriented research center associated with the College of Engineering, and holds courtesy faculty positions at CMU’s Heinz College and the Institute for Software Research, an academic department in the School of Computer Science. She has also taught political science courses at Hamilton College, Harvard University, and the University of California, Los Angeles. At Stanford University’s Hoover Institution, Professor Skinner is the W. Glenn Campbell Research Fellow and a member of the Arctic Security Initiative, the working group on the Role of Military History in International Conflict, and the Shultz-Stephenson Task Force on Energy Policy.

Professor Skinner is an award-winning and best-selling author. Her coauthored books Reagan, In His Own Hand (2001) and Reagan, a Life in Letters (2003) were New York Times best sellers. Reagan, In His Own Hand won the Hoover Institution’s Uncommon Book Award and was serialized in the New York Times Magazine on December 31, 2000. Reagan, A Life in Letters was selected as one of the best books of 2003 by the Los Angeles Times, was Time magazine’s cover story on September 29, 2003, and was the subject of a September 29, 2003, editorial written by the New York Times editorial board. The Strategy of Campaigning: Lessons from Ronald Reagan and Boris Yeltsin (2007), a book Professor Skinner coauthored with Serhiy Kudelia, Bruce Bueno de Mesquita, and Condoleezza Rice, was excerpted on the opinion page of the New York Times on September 15, 2007. A frequent contributor of opinion essays, Professor Skinner has written for CNN.com, Forbes.com, Foreign Policy.com, National Review Online, the New York Times, the Wall Street Journal, and the Washington Post. She also regularly provides scholarly commentary on national and international television and radio programs.

Other academic activities in which Professor Skinner is engaged include serving as an associate editor of Telos, a leading humanities journal, and as the general series editor on Ideology and American Politics for Palgrave Macmillan. Professor Skinner is a co-chair of the Securities and Democratic Exceptions working group for the Social Science Research Council’s Anxieties of Democracy program.
Among Professor Skinner’s numerous awards are the Truman Scholarship for the State of California (1979); *Glamour* magazine’s Top Ten College Competition for Women (1981); Harvard University’s Sidney Matz Prize for excellence in advising undergraduates (1989); Delegate to the Bellagio “New Faces” Conference sponsored by the Arms Control Association and the International Institute for Strategic Studies (1989); University of California President’s Postdoctoral Fellow (1996-98); Olin Foundation Faculty Fellowship (1999-2001 and 2001-2002); BMW Transatlantic Forum Fellow (US and Germany, 2004 and 2005); and Kennedy Middle School Hall of Fame (Redwood City, California, 2005).

Professor Skinner’s government service includes membership on the Eisenhower Commission’s Legacy Committee of historians (2002-03); the US Defense Department’s Defense Policy Board as an adviser on the Iraq and Afghanistan wars (2001–07); the Chief of Naval Operations’ Executive Panel (2004–15); the National Academies’ Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security (2009–11); and the National Security Education Board (2004–11). In 2010, Professor Skinner was appointed to the advisory board of the George W. Bush Oral History Project. She served as a foreign policy surrogate for the Bush-Cheney reelection campaign in 2004; a senior foreign policy adviser to Speaker Newt Gingrich during his presidential campaign in 2001–07; and a senior foreign policy surrogate to Governor Mitt Romney’s presidential campaign in the fall of 2012. In 2015-16, she was a member of the foreign policy team for Senator Rand Paul during his presidential bid. Professor Skinner served on Pennsylvania Governor Tom Corbett’s Advisory Commission on African American Affairs from 2012 to 2015.

Professor Skinner serves on a number of boards including the American Australian Council in Washington, DC; the Atlantic Council of the United States in Washington, DC; Grove City College in Grove City, PA; Propel Schools in the Pittsburgh area; Saint Vincent College in Latrobe, PA; and the US Global Coalition’s Pennsylvania Advisory Committee. Professor Skinner is a life director of the Atlantic Council in Washington, DC, as well as a life member of the Pacific Council on International Policy in Los Angeles and the Council on Foreign Relations in New York City.

Professor Skinner holds MA and PhD degrees in political science and international relations from Harvard University and undergraduate degrees from Spelman College and Sacramento City College. She received an honorary doctor of laws degree from Molloy College, Long Island. In her leisure time, she enjoys hiking in California’s foothills and mountains.