Developing a Normative Framework for Cyberwarfare

October 17-18, 2016

United States Naval Academy
Annapolis, Maryland

Table of Contents:

Purpose:

Welcome to our workshop on the social, ethical, and legal implications on cyberwarfare. As this is quickly-evolving terrain, we hope to reflect the current state of play, as well as to sketch the short- and mid-term future. In these endeavors, we will be aided by a diverse and distinguished group of invited presenters. These presenters have been carefully selected from academia, industry, and government, and bring with them a wealth of expertise and experience.

Unlike many academic workshops, this one is meant to be discussion intensive. Toward that end, presenters have been asked to keep their briefings to approximately fifteen minutes, leaving the rest of the sessions for interaction. To foster these interactions, we will operate under The Chatham House Rule: participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed without their expressed consent.

Acknowledgments:

The conference is organized by Dr. Fritz Allhoff (Western Michigan University/Stanford Law School), Dr. Patrick Lin (California Polytechnic State University), and Dr. Ryan Jenkins (California Polytechnic State University). It is supported by funding from the U.S. National Science Foundation (NSF), under awards #1318126, #1317798, #1318270.

In addition to the NSF, we are grateful for institutional support from the following: California Polytechnic State University, Case Western Reserve University's Inamori International Center for Ethics and Excellence, Naval Postgraduate School, United States Naval Academy's Stockdale Center for Ethical Leadership, and Western Michigan University.

We owe special thanks to Mr. Jonathan Milgrim (Western Michigan University) for administrative support. We also thank Dr. Edward Barrett (Stockdale Center) for co-hosting this event and for logistical support. We further thank Dr. Shannon French (Inamori Center), Dr. Don Howard (University of Notre Dame), and Dr. George Lucas (Naval War College) for continued support and encouragement. Finally, we thank you, our workshop participants, for participating in this event!

Monday, October 17

9:00-9:15	Welcoming Remarks Fritz Allhoff, Western Michigan University/Stanford Law School Arthur Athens, United States Naval Academy

Session 1: Technologies and Methods of Cyberwarfare

9:15-10:00	"Cyber Reconnaissance and Intrusion" Mike Bilzor and Jeffrey Kosseff, United States Naval Academy
10:05-10:50	"'Loud' Cyber Tools for Deterrence" Shawn Turskey, National Security Agency
10:55-11:40	"Machine Intelligence in Adversarial Settings" Patrick McDaniel, Pennsylvania State University
11:45-12:30	"The Present and Future of Cybersecurity" Gene Spafford, Purdue University
12:30-1:30	Lunch

Session 2: Cyberpolicy and Education

1:30-1:45	Welcoming Remarks Chris Inglis, United States Naval Academy
1:45-2:30	"Teaching Cyberwarfare Ethics: Challenges and Opportunities" Lance Hoffman, George Washington University
2:35-3:20	"Cyberwarfare and Trusted Insiders" Michael Theis, Carnegie Mellon University
3:25-4:10	"Civic Virtue and Cybersecurity" Don Howard, University of Notre Dame
4:15-5:00	"Combatting Cyber Risks in a Digitally-Connected Environment" Kirstjen Nielsen, Sunesis Consulting
6:00-9:00	Dinner at Carroll's Creek 410 Severn Avenue (registration required)

Tuesday, October 18

Session 3: Cybernorms and International Law

9:00-9:45	"Constructing Norms for Global Cybersecurity" Duncan Hollis, Temple University
9:50-10:35	"A Comparison of 'Voluntary' Cybersecurity Frameworks" Scott Shackelford, Indiana University
10:40-11:25	"Tallinn Manual 1.0: International Law and Cyberwarfare" Sean Watts, Creighton University
11:30-12:15	"Tallinn Manual 2.0: International Law and Peacetime Cyber Operations" Liis Vihul, NATO CCD COE
12:15-1:15	Lunch

Session 4: Cybersecurity and Cyber Operations

1:15-2:00	"Privacy, Anonymity, and Cybersecurity" George Lucas, United States Naval War College
2:05-2:50	"Protecting Critical Infrastructure from Cyberattacks" Catherine Lotrionte, Georgetown University
2:55-3:40	"Strategic Dimensions of Offensive Cyber Operations" Herb Lin, Stanford University
3:45-4:30	"Terrorism in Cyberspace" David Fidler, Indiana University
4:30-4:45	Closing Remarks Patrick Lin, California Polytechnic State University
6:00-9:00	Dinner at Baroak 126 West Street (registration required)

Session 1: Technologies and Methods of Cyberwarfare

"Cyber Reconnaissance and Intrusion"
Mike Bilzor and Jeff Kosseff, United States Naval Academy
This presentation will discuss various stages of cyberattack from the point of view of the attacker, using virtual machines, including network reconnaissance, network scanning, looking for vulnerabilities, and actual compromise attempts, while explaining what is going on in plain language. At each step, we will discuss the ethical and legal context for that particular attack. This presentation will tangibly bridge the technical aspects of cyberattack and defense with the ethical and legal side. An important part of the discussion will be the challenge of creating rules that are enforceable and legally meaningful, while still giving security researchers the necessary freedom to identify and responsibly disclose vulnerabilities.

"'Loud' Cyber Tools for Deterrence"
Shawn Turskey, National Security Agency
Conventional cyber strategy is to avoid detection and attribution. But if the goal of cyber activity is to deter an adversary's behavior, then cyber attackers should aim to be detected and for attribution to be straightforward. This session will discuss the reasoning behind this kind of "loud" cyberattack; the "big rocks" of cyber, including cyber tools, infrastructure and data analytics; and methods of cyberattack, including the "4D's." This includes exfiltration of sensitive (e.g., commercial or military) data, denying access to the adversary's own systems, destroying found data, corrupting data as a way of deceiving adversaries about the integrity of their own systems, and degrading or slowing access to their data.

"Machine Intelligence in Adversarial Settings"
Patrick McDaniel, Pennsylvania State University
Advances in machine learning have enabled new applications. Autonomous cars, automated analytics, adaptive communication systems and self-aware software systems are now revolutionizing markets and blurring the lines between computer systems and real intelligence. This presentation will consider whether the current use of machine learning in security-sensitive contexts is vulnerable to nonobvious and potentially dangerous manipulation. Here, it examines sensitivity in any application whose misuse might lead to harm—for instance, forcing adaptive network in an unstable state, crashing an autonomous vehicle or bypassing an adult content filter. It explores the use of machine learning in this area particularly in light of recent discoveries in the creation of adversarial samples, and posit on future attacks on machine learning. The talk is concluded with a discussion of the unavoidable vulnerabilities of systems built on probabilistic machine learning, and outline areas for defensive research in the future.

"The Present and Future of Cybersecurity"
Gene Spafford, Purdue University
We have been computing for nearly 60 years and dealing with security problems for nearly that long. Despite great advances in technology and continuing expenditures, the quantity and severity of cyber security incidents have been steadily increasing. We are now experiencing millions of new computer viruses per month, major acts of espionage, and exposure of hundreds of millions of personal records per year. Why isn't the situation better? In this presentation, the speaker will draw on 30 years of experience in computing and study of computer security to draw some conclusions. Starting with a short summary of the current security situation and how we got to it, we will look at a few of the biases and issues that continue to shape how we approach cybersecurity.

Session 2: Cyberpolicy and Education

"Teaching Cyberwarfare Ethics: Challenges and Opportunities"
Lance Hoffman, George Washington University
If nation-states and other actors can agree on acceptable norms for cyberwarfare, educating all stakeholders about these norms will often be done in universities, where users, implementers, and enforcers are trained. They must be given a shared language of discourse and a basic understanding of how computer systems and networks work, as well as explanations of what the norms are, how they affect different stakeholders, the rationale behind acceptable and unacceptable behaviors, when and where the norms apply, and an overview of judicial processes and sanctions. Cyberwarfare ethics demands knowledge and skill sets from many disciplines—technological, administrative, legal, sociological, economic, and more. As a result, professors often must recruit colleagues and experts from outside the university as guest lecturers to do justice to the topic. Introducing ethics or policy topics in university programs reduces time available to cover other material. Academic reward structures often discourage work in new and/or multidisciplinary areas. Thus, bringing the latest knowledge about cyberwarfare ethics to academe poses many challenges.

"Cyberwarfare and Trusted Insiders"
Michael Theis, Carnegie Mellon University
Why do trusted insiders damage or destroy an organization's cyber systems? Who are the people who are the most likely to commit cyber systems sabotage? What are the most common tactics, techniques and procedures? The Carnegie Mellon CERT Insider Threat Center will answer these questions as well as describe mitigation strategies based on their 15 years of empirical research. Armed with this information, an organization can develop and implement socio-technical controls that can prevent, detect, and respond to potential cyber systems sabotage before it occurs. We will also discuss the likelihood that a trusted insider would become a saboteur in response to some of the external pressures being exerted on trusted insiders by the Internet Underground, the Dark Web, and new forms of ransomware.

"Civic Virtue and Cybersecurity"
Don Howard, University of Notre Dame
Questions about cybersecurity live in a space of antiquated and inadequate law, disparate, sometimes overlapping, sometimes conflicting jurisdictions, weak enforcement mechanisms, and weak incentives for international collaboration. Even were notions of civil rights that fit earlier forms of political life capable of adaptation to new technologies of commerce, expression, conflict, and exploration, the means to secure such rights are lacking. This presentation argues that, under these circumstances, the efforts of ethicists, legal scholars, and policy makers are helped by reframing central questions about issues including personal privacy, freedom of expression, the intellectual property claims of individual and corporate persons, and political action in the language of civic virtues as better fitting life in the cyberworld.

"Combatting Cyber Risks in a Digitally-Connected Environment"
Kirstjen Nielsen, Sunesis Consulting
In today's increasingly digitally-connected environment, cyber risks cannot be addressed in isolation. Increasingly, your cyber risk becomes my risk if we are virtually connected (directly or indirectly), and a system's aggregated risk becomes the risk of all component users and contributors. Given the complex nature of cyber risks, no one entity has all of the authorities, capabilities and capacities to effectively address the risk alone. Risk managers must look to build and strengthen a holistic cyber resilience approach. This presentation will describe a resilience approach to combatting cyber risk and offer various activities and capabilities that together can form an entity's resilience toolkit.

Session 3: Cybernorms and International Law

"Constructing Norms for Global Cybersecurity"
Duncan Hollis, Temple University
Calls for new norms to enhance cybersecurity have become ubiquitous, but proponents of new cybernorms have so far focused on content: the behaviors that norms require or prohibit. Little attention has been paid to how new norms actually work. Drawing on extensive social science research, this presentation will discuss the processes by which norms form, spread, and create effects in the world, and shows how those processes ultimately feed back on themselves to shape norms' content. Applying these insights to cybersecurity, it will identify a number of key strategic trade-offs involved in the processes for constructing new cybernorms—trade-offs that may serve as both a caution and guide to those seeking to cultivate such norms.

"A Comparison of 'Voluntary' Cybersecurity Frameworks"
Scott Shackelford, Indiana University
Although there is a spectrum of cybersecurity regulatory frameworks emerging around the world ranging from more state-centric approaches to voluntary initiatives, more and more nations—including the United States—seem to be settling on a bottom-up approach to enhancing private-sector cybersecurity. Emblematic of this movement in the U.S. context is the 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework. This Framework, which is comprised partly of regularly updated cybersecurity best practices, has already been influential in shaping the field of cybersecurity due. However, there has not yet been a thorough examination of the similarities and differences between these various bottom-up approaches and the extent to which they are promoting the harmonization of cybersecurity best practices. This presentation addresses this omission by investigating a subset of national approaches to cybersecurity policymaking highlighting the extent to which they are converging and diverging using the NIST Framework as a baseline for comparison. Such an understanding is vital not only to businesses operating across these jurisdictions, but also to policymakers seeking to leverage the expertise of the private sector in promoting cyberpeace.

"Tallinn Manual 1.0: International Law and Cyber Warfare"
Sean Watts, Creighton University
The presentation will give a brief orientation to law-of-war issues applicable to cyberwarfare. In particular, the presentation will discuss the work of an international group of experts that produced a legal manual on international law applicable to cyberwarfare—the Tallinn Manual. Subjects covered will include how rules applicable to States' resort to force operate in cyberspace, especially the prohibition on the use of force and self-defense. Additionally, the presentation will briefly cover rules applicable to the conduct of hostilities in cyberspace, including questions of applicability, targeting, and the law of neutrality. The presentation will emphasize apparent seems in the law—areas the Tallinn Manual group had difficulty clarifying or on which consensus concerning the state of the law proved elusive. Discussion will explore what the law of war regulating cyber warfare may look like in the future.

"Tallinn Manual 2.0: International Law and Peacetime Cyber Operations"
Liis Vihul, NATO Cooperative Cyber Defence Centre for Excellence
This presentation will give an overview of the genesis of the "Tallinn Manual on the International Law Applicable to Cyber Operations." Completed in two phases in 2009-2016, the Tallinn Manual is an authoritative restatement of the international law that applies to state cyber operations during peacetime as well as those that occur in the context of an armed conflict. In particular, the presentation will introduce some key legal concepts that govern cyber operations undertaken in peacetime that were discussed by the Tallinn Manual's international group of experts. These include issues of state sovereignty in cyberspace, legal attribution of cyber operations to states, and the legal analysis of cyber espionage under international law. Finally, the presentation will give a brief overview of the various specialized regimes of international law that further regulate state activities in cyberspace.

Session 4: Cybersecurity and Cyber Operations

"Privacy, Anonymity, and Cybersecurity"
George Lucas, United States Naval War College
State-sponsored hacktivism has problematized the defense of privacy in the aftermath of hacks of the Office of Personnel Management and Yahoo. It is difficult to fault one's own security forces for invasions of privacy when they are engaged in provision of preemptive self-defense against such attacks. But the preventive security, as the Snowden revelations demonstrated, seem likewise to threaten privacy. Perhaps there is no protecting of privacy of citizens that does not involve the compromise of their privacy for the sake of their greater security of even more serious breaches of that privacy by others. That paradox may be resolved, however, if the preventive self-defense in question is guarded by "soft-law" provisions that commit defenders to the protection of their own and allies' privacy, at the expense only of their anonymity, so as to make them less vulnerable to more serious breaches by adversaries who have no regard whatever for their dignity and welfare.

"Protecting Critical Infrastructure from Cyberattacks"
Catherine Lotrionte, Georgetown University
According to Director of National Intelligence James Clapper, both the U.S. telecommunications and electric grid face escalating cyber threats from foreign adversaries with advanced cyber capabilities. The effective cyberattacks against the Ukraine power system on December 23, 2015 serve as an example of potential threats to state critical infrastructure. The topic of what states may legally do in response to harmful cyberattacks against their critical infrastructure has become a national security issue. Indeed, the issue highlights some of the most important modern questions related to cyber operations and the role of international law in regulating state behavior and maintaining international stability. This presentation will examine the issue of a state's legal authorities to act to protect its critical infrastructure from cyberattacks and evaluate how the inherent right of self-defense could be applicable in such cases compared to a "plea of necessity" invoked by a victim state to excuse what would otherwise be unlawful actions in order to protect the state's critical infrastructure.

"Strategic Dimensions of Offensive Cyber Operations"
Herbert Lin, Stanford University
In a speech releasing the Department of Defense (DOD) cyber strategy in 2015, Secretary of Defense Ashton Carter noted that one mission of the DOD is "to provide offensive cyber options that, if directed by the President, can augment our other military systems." Because they are relatively new to the DOD arsenal, the use of cyber weapons challenges doctrine and strategy developed for kinetic weapons. This presentation will highlight several important strategic dimensions of using cyber weapons, including deterrence, retaliation, counterforce and countervalue targeting, escalation dynamics, rules of engagement, private sector-led operations, and what from U.S. nuclear strategy might inform cyber operations.

“Terrorism in Cyberspace”
David Fidler, Indiana University
Just as terrorism has become a major national security issue, the terrorist threat is prominent in cybersecurity and cyberspace policy. Governments worry about terrorist cyberattacks and are struggling to address how terrorists exploit cyberspace to spread propaganda, recruit and radicalize individuals, and raise funds. This presentation analyzes international law in connection with potential terrorist cyberattacks and terrorist use of cyber technologies for other purposes. Current international law is not well positioned to support responses to terrorist cyberattacks, but the lack of such attacks to date undermines incentives for states to develop international law against this threat. In terms of terrorists using the Internet and social media for propaganda, radicalization, recruiting and fundraising, the crisis caused by the Islamic State’s online activities has not created consensus strong enough to support a prominent role for international law in countering cyber-facilitated terrorism.

Presenter Biosketches

Michael Bilzor, CDR, Ph.D. is Chair of the Computer Science Department at the United States Naval Academy, where he teaches classes in cybersecurity and artificial intelligence, among others. His primary research interest is in cybersecurity, particularly malware detection and classification, and he currently serves as Officer Representative to the USNA competitive cyber team, the Information Warfare Group. He served as a Naval Flight Officer in F-14s and F/A-18s from 1995-2005 and holds a Ph.D. in computer science from the Naval Postgraduate School.

David Fidler, J.D. is the James Louis Calamaras Professor of Law at Indiana University. He is also an Adjunct Senior Fellow for Cybersecurity with the Council on Foreign Relations, an Associate Fellow with the Centre on Global Health Security at the Royal Institute of International Affairs (Chatham House), a Senior Fellow at the Indiana University Center for Applied Cybersecurity Research, and a Fellow with the Pacific and Asia Society. He is also on the Roster of Experts that advises the Director-General of the World Health Organization under the International Health Regulations (2005). He serves as Chair of the International Law Association's Study Group on Terrorism, Cybersecurity, and International Law. He earned a J.D. from Harvard Law School and a B.C.L. an M.Phil. from Oxford University.

Lance Hoffman, Ph.D. is the Distinguished Research Professor of Computer Science and Director of the Cyber Security Policy and Research Institute at The George Washington University. He developed the first regularly-offered university course on computer security and is the author or editor of five books that captured the state of cybersecurity and privacy at various times between 1973 and 1995. His 1999 study of encryption products explored the effect of the U.S. export control regime that he later presented before Congress. His leadership included pioneering workshops on Internet voting, cybersecurity educational competitions, and workforce development; the institutionalizing of the ACM Conference on Computers, Freedom, and Privacy; and the development of courses that focused on e-commerce security, information policy, and cybersecurity and governance as the field broadened. He initiated and still leads a CyberCorps scholarship program that has produced dozens of cybersecurity experts with degrees in at least ten majors who have gone on to work for dozens of different government agencies.

Duncan Hollis, J.D., M.A.L.D. is James E. Beasley Professor of Law at Temple Law School and a Senior Fellow at Melbourne Law School. He is editor of the award-winning *Oxford Guide to Treaties* (Oxford University Press, 2012) as well as a series of articles on securing cyberspace, including (with Martha Finnemore) "Constructing Norms for Global Cybersecurity," *American Journal of International Law* (forthcoming). He is part of a team headed by research scientists from the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory (CSAIL) that was awarded a U.S. Department of Defense Minerva Grant for inter-disciplinary analysis of norms and governance in cyberspace. Professor Hollis is a Non-Resident Scholar at the Carnegie Endowment for International Peace, an elected member of the American Law Institute, and (beginning in 2017) a member of the Inter-American Juridical Committee, one of the principal organs of the Organization of American States.

Don Howard, Ph.D. is the former Director and a Fellow of the University of Notre Dame's Reilly Center for Science, Technology, and Values and a Professor in the Department of Philosophy. A Fellow of the American Physical Society, and Chair of APS's Committee on International Freedom of Scientists, Dr. Howard is an internationally recognized expert on the history and philosophy of modern physics, especially the work of Albert Einstein and Niels Bohr. He has been writing and teaching about the ethics of science and technology for many years. Co-editor of the recent collection, *The Challenge of the Social and the Pressure of Practice: Science and Values Revisited* (University of Pittsburgh Press, 2008), Dr. Howard led NSF-funded workshops on science and ethics at Notre Dame for physics students, is currently PI on an NSF-EESE research ethics grant, and has taught courses on topics ranging from the moral choices of atomic scientists during World War II and the Cold War, to the ethics of emerging weapons technologies and robot ethics. Dr. Howard earned his Ph.D. in philosophy from Boston University.

Jeff Kosseff, J.D., M.P.P. is an Assistant Professor in the United States Naval Academy's Cyber Science Department. Professor Kosseff is a lawyer who he teaches cybersecurity law and policy. His research focuses on cybersecurity evidentiary issues, public-private cybersecurity partnerships, cybercrime, cyberwarfare law, and the intersection of cybersecurity and free speech. Professor Kosseff received his J.D. from Georgetown University Law Center, and a B.A. and an M.P.P. from the University of Michigan.

Herb Lin, Ph.D. is Senior Research Scholar for cyberpolicy and cybersecurity at the Center for International Security and Cooperation and Research Fellow at the Hoover Institution, both at Stanford University. In addition, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee. He received his Ph.D. in physics from the Massachusetts Institute of Technology.

Catherine Lotrionte, J.D., Ph.D. is the Director of the CyberProject in the School of Foreign Service at Georgetown University. At Georgetown she founded the CyberProject in 2008, focusing on the role of international and domestic law in recent and emerging developments in the proliferation of weapons, technology and threats. In 2002 she was appointed by General Brent Scowcroft as Counsel to the President's Foreign Intelligence Advisory Board at the White House, a position she held until 2006. Dr. Lotrionte holds an M.A. and a Ph.D. from Georgetown University and a J.D. from New York University and is the author of numerous publications. She currently serves on the World Economic Forum's Global Agenda Council on Cybersecurity, the Center for Strategic and International Studies Cyber Policy Task Force, the CFR-sponsored Independent Task Force on Defending an Open, Global, Secure, and Resilient Internet, and the CFR-sponsored Independent Task Force on U.S. Policy Toward North Korea.

George Lucas, Ph.D. is currently the Vice Admiral James B. Stockdale Professor of Ethics at the United States Naval War College. He is a Visiting Professor at the Reilly Center for Science, Technology & Values at Notre Dame University, and Professor Emeritus at the United States Naval Academy. He is currently President of the International Society for Military Ethics. Dr. Lucas is author most recently of: *Military Ethics: What Everyone Needs to Know* (Oxford University Press, 2016); *Ethics & Cyber Warfare* (Oxford University Press, 2017), and Editor of the *Routledge Handbook of Military Ethics* (2015). His forthcoming book is entitled *Beyond Clausewitz: the Role of Ethics in Military Strategy in the 21st Century* (Routledge).

Patrick McDaniel, Ph.D. is a Distinguished Professor in the School of Electrical Engineering and Computer Science at Pennsylvania State University, co-director of the Systems and Internet Infrastructure Security Laboratory, and Fellow of IEEE and ACM. He is also the program manager and lead scientist for the Army Research Laboratory's Cyber-Security Collaborative Research Alliance. His research centrally focuses on a wide range of topics in security and technical public policy. Prior to receiving his Ph.D. at the University of Michigan, Dr. McDaniel was a software architect and project manager in the telecommunications industry.

Kirstjen Nielsen, J.D. is currently the founder and President of Sunesis Consulting, LLC, a security management consulting firm, and the Chair of the World Economic Forum's Global Agenda Council on Risk and Resilience and a Senior Fellow at the Center for Cyber and Homeland Security. She is also a credentialed risk expert and serves as a civilian expert for NATO and on various cyber advisory boards. Previously, Ms. Nielsen was commissioned to serve as Special Assistant to the President and Senior Director for Prevention, Preparedness, and Response on the White House Homeland Security Council. Ms. Nielsen graduated from the Georgetown University School of Foreign Service and from the University of Virginia School of Law.

Scott Shackelford, J.D., Ph.D. is an Associate Professor at Indiana University where he teaches cybersecurity law and policy, sustainability, and international business law. He is also a Senior Fellow at the Center for Applied Cybersecurity Research, a Visiting Scholar at Stanford Law School, and a Term Member at the Council on Foreign Relations. Dr. Shackelford has written more than 100 books, articles, and essays. He is also the author of *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press, 2014). Both Dr. Shackelford's academic work and teaching have been recognized with numerous awards, including a Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, and the 2015 Elinor Ostrom Award.

Eugene Spafford, Ph.D. is a Professor of Computer Sciences at Purdue University, and is the founder and Executive Director Emeritus of the Center for Education and Research in Information Assurance and Security (CERIAS). His research and education over three decades has contributed to many of the technologies used in modern computing system protection. Dr. Spafford's current research interests are in information security, cybercrime, software engineering, professional ethics, and security policy. Dr. Spafford is a Fellow of the ACM, AAAS, IEEE, (ISC)2, is a Distinguished Fellow of the ISSA, and has received many other awards for service, scholarship, and education.

Michael Theis uses his 25 years as a Counterintelligence Supervisory Special Agent supporting the U.S. Intelligence Community along with his 30 years of concurrent computer systems engineering experience to aid the CERT© Insider Threat Center further its research and development of socio-technical controls to prevent, detect, and respond to insider threats. He is also a Senior Member of the Technical Staff at the Software Engineering Institute (SEI). Previously, Mr. Theis was the first-ever Cyber-Counterintelligence Program Manager for the National Reconnaissance Office, where he served as the Chief for Cyber-CI investigations and operations for over six years. In 2006, he was named one of the Premier 100 IT Leaders in the nation by COMPUTERWORLD Magazine. Mr. Theis is a frequent keynote speaker at government, private industry, and academic conferences, where he is a recognized thought leader for insider threat, cyberspace intelligence, and security issues. He has also guest lectured at Harvard University and the Massachusetts Institute of Technology on the challenges and opportunities of modeling human behavior in cyberspace.

Shawn Turskey, M.S. has been executive director of the United States Cyber Command (USCYBERCOM), the highest-ranking civilian, since 2014. Additionally, as the lead for Cyber Tools and Capabilities Development under the Secretary of Defense Cyber Strategy, he drives strategic and technical innovation that enables and equips the cyber warrior to conduct operations. During his 29 years with the National Security Agency (NSA), he spearheaded several missions in the Directorates of Signals Intelligence, Information Assurance and the NSA/Central Security Service Threat Operations Center. Mr. Turskey's background spans a breadth and depth of technical and operational leadership across NSA's cyber components. He is a Certified Information Systems Security Professional and earned a Master of Science in National Security Strategy from the National War College. Mr. Turskey also holds B.S. and M.S. degrees in Electrical Engineering.

Liis Vihul, M.A., M.Sc. is a senior analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence. She is the project manager and managing editor of the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." Ms. Vihul runs the international law training programme at the NATO Cyber Defence Centre, serves as a member of the Estonian delegation at the United Nations Group of Government Experts, and is the CEO of Cyber Law International, a firm that provides international law consultancy and training. Ms. Vihul holds an M.A. in law from the University of Tartu and an M.Sc. in information security from the University of London.

Sean Watts, J.D., LL.M. is a Professor of Law at Creighton University Law School, a Senior Fellow at the Lieber Institute for Law and Land Warfare at the United States Military Academy at West Point and a Senior Fellow with the NATO Cooperative Cyber Defence Center of Excellence in Tallinn, Estonia. He also serves as an Army JAG Reservist at the U.S. Strategic Command. He was a member of the group of experts that produced the Tallinn Manual on International Law Applicable to Cyber Warfare as well as the second, forthcoming edition of that work. From 2009-2012, he served as a defense team member in *Gotovina et al.* at the International Criminal Tribunal for Former Yugoslavia. Prior to teaching, Professor Watts served 15 years as an active-duty Army JAG Corps officer and as an armor officer in an Army Tank Battalion.

Grant Team Biosketches

Keith Abney, M.A., A.B.D. is a Senior Lecturer in the Philosophy Department and a Senior Fellow at the Ethics + Emerging Sciences Group at California Polytechnic State University, San Luis Obispo. His research includes work on warfare and the cyber debate, just war theory and the use of autonomous weapons, human enhancement in the military, demarcating science from non-science, moral status and sustainability, astronaut and space ethics, patenting life, robot ethics, and other aspects of the ethical implications of emerging sciences and technologies.

Fritz Allhoff, J.D., Ph.D. is a Professor in the Department of Philosophy at Western Michigan University and a Fellow in the Center for Law and the Biosciences at Stanford Law School. He received his Ph.D. in philosophy from the University of California, Santa Barbara, and his J.D. from the University of Michigan Law School, where he graduated magna cum laude. Following law school, he clerked for the Honorable Chief Justice Craig Stowers of the Alaska Supreme Court. Dr. Allhoff is the author of *Terrorism, Ticking Time-Bombs, and Torture* (University of Chicago Press, 2012), as well as co-editor of the *Routledge Handbook of Ethics and War: Just War Theory in the Twenty-First Century* (2013) and *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press, 2016). His popular work has been featured in Slate, The Atlantic, and The Huffington Post. Dr. Allhoff is also a founding member of the Asia Pacific Chapter of the International Society for Military Ethics (APAC-ISME) and serves on the editorial board for the International Committee of Military Medicine (Switzerland).

Shannon Brandt Ford, Ph.D. (c) is President of the Asia Pacific Chapter of the International Society for Military Ethics (APAC-ISME). He was previously a Research Fellow at the Centre for Applied Philosophy and Public Ethics, Charles Sturt University, where he led a research project on the ethics of cybersecurity. Before that, Mr. Ford spent 10 years as a Defence Strategist and Analyst with the Australian Department of Defence. He is completing his doctorate at the National Security College with the Australian National University. Mr. Ford was recently awarded a contract with the Australian Army Research Scheme to write a report that examines "Emerging Weapons Technologies: Political, Ethical and Legal Dilemmas."

Ryan Jenkins, Ph.D. is an Assistant Professor of Philosophy and a Senior Fellow at the Ethics + Emerging Sciences Group at California Polytechnic State University, San Luis Obispo. His interests include military ethics and the ethics of emerging technologies, including cyberwarfare, autonomous vehicles, robots, algorithms, and autonomous weapons. He is currently co-editing two books on military ethics and robot ethics, both for Oxford University Press.

Patrick Lin, Ph.D., is Director of the Ethics + Emerging Sciences Group at California Polytechnic State University, San Luis Obispo, where he is an Associate Professor of Philosophy. He is also affiliated with Stanford Law School's Center for Internet and Society, University of Notre Dame's Emerging Technologies of National Security and Intelligence Initiative, Australia's Centre for Applied Philosophy and Public Ethics, and the World Economic Forum's Global Future Councils. Previously, he held academic appointments at Stanford's School of Engineering, United States Naval Academy, and Dartmouth College. Dr. Lin is well published in the ethics of emerging technologies—including robotics, cybersecurity, AI, human enhancements, nanotechnology, and more—especially their national security implications. He is the lead editor of *Robot Ethics* (MIT Press, 2012), among other books and articles. He has provided briefings, testimony, and counsel to the U.S. Department of Defense, CIA, United Nations, UNIDIR, National Research Council, Google, Apple, and many other organizations. He earned his B.A. from the University of California and his Ph.D. from the University of California at Santa Barbara.

Neil Rowe, Ph.D. is Professor of Computer Science at the United States Naval Postgraduate School where he has worked since 1983. He has a Ph.D. in Computer Science from Stanford University. His main research interests are in data mining, digital forensics, modeling of deception, and cyberwarfare.

Bradley J. Strawser, Ph.D. is an Assistant Professor of Philosophy in the Defense Analysis Department at the United States Naval Postgraduate School, and a Research Associate at Oxford University's Ethics, Law, and Armed Conflict Center. He works primarily on the ethics of war, military ethics, just war theory, and related issues. He recently published *Binary Bullets: The Ethics of Cyberwarfare* (Oxford, 2016) with Fritz Allhoff and Adam Henschke. His newest book, *The Bounds of Defense: Killing, Moral Responsibility, and War* is forthcoming from Oxford University Press.

Registration:

Conference registration is free, but space is limited. Please email us with registration requests.

Venue:

The conference sessions will be held in the Naval Academy Club. Registered conference attendees will be listed with the Naval Base guard stations. Walk-in access is available at Gate 3, and vehicle access is available at Gate 8 (map). Complimentary shuttle service will be available to and from the conference hotel at designated times.

Banquet:

The conference banquet will be held at Carrol's Creek Café, located at the Annapolis City Marina, 410 Severn Avenue #100, Annapolis, MD, 21401 (map). Complimentary shuttle service will be available to and from the restaurant. Please email us with any dietary restrictions.

Hotel:

The conference hotel is the Loews Annapolis Hotel, located at 128 West Street, Annapolis, MD 21401 (map). The conference rate is $136.73/night; registration is available through the hotel portal.

Travel:

Annapolis is serviced by—in decreasing order of convenience—Baltimore/Washington International Airport (BWI), Reagan National Airport (DCA), and Dulles International Airport (IAD). There is also Amtrak service from New York to Baltimore Penn Station and BWI. Transportation from Baltimore and Washington, D.C. varies in time and price depending on time of day.

Baltimore/Washington International Airport. Super Shuttle is approximately $39 for a shared ride. Annapolis Taxi Service is approximately $50. Uber prices vary from as low as $30 to as high as $120 depending on time of day and service choice.

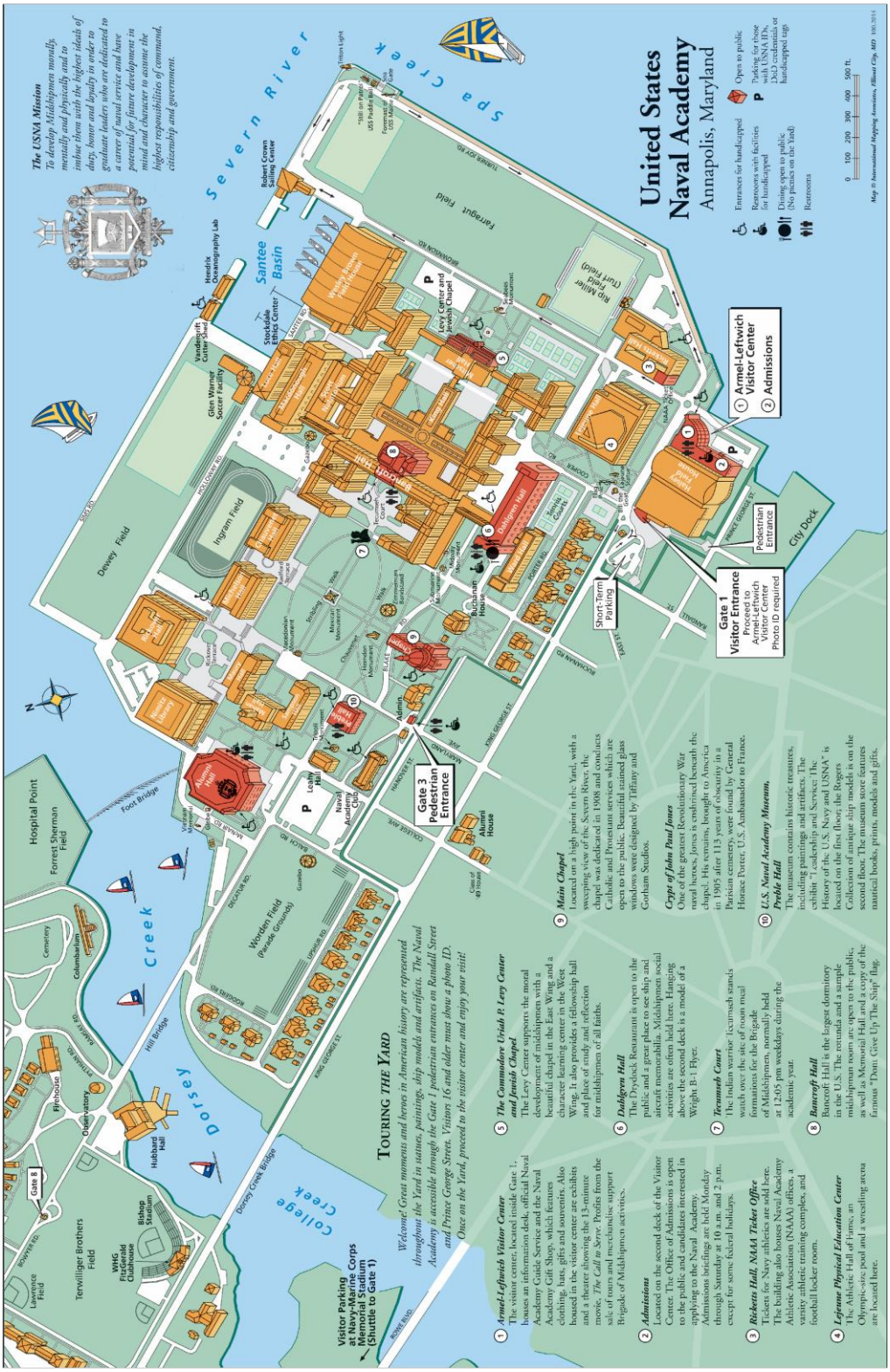
Reagan National Airport. Super Shuttle is approximately $56 for a shared ride. Annapolis Taxi Service is approximately $75. Uber prices vary from as low as $40 to as high as $180 depending on time of day and service choice.

Dulles International Airport. Super Shuttle is approximately $139 for a shared ride. Annapolis Taxi Service is approximately $125. Uber prices vary from as low as $60 to as high as $300 depending on time of day and service choice.

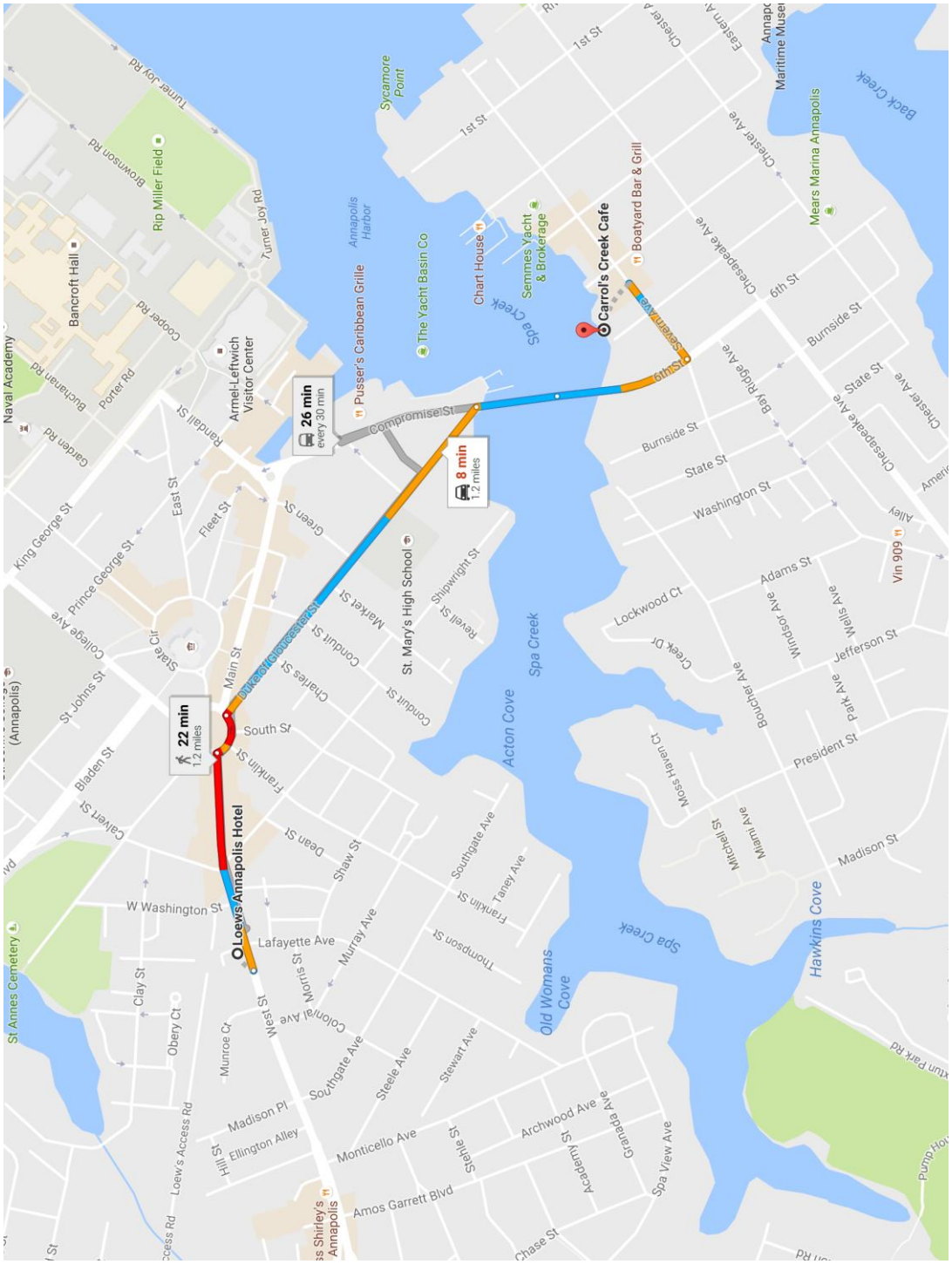
In addition to the choices listed above, the City of Annapolis offers information on local and regional travel. A map of Annapolis may also be useful.

Venue:

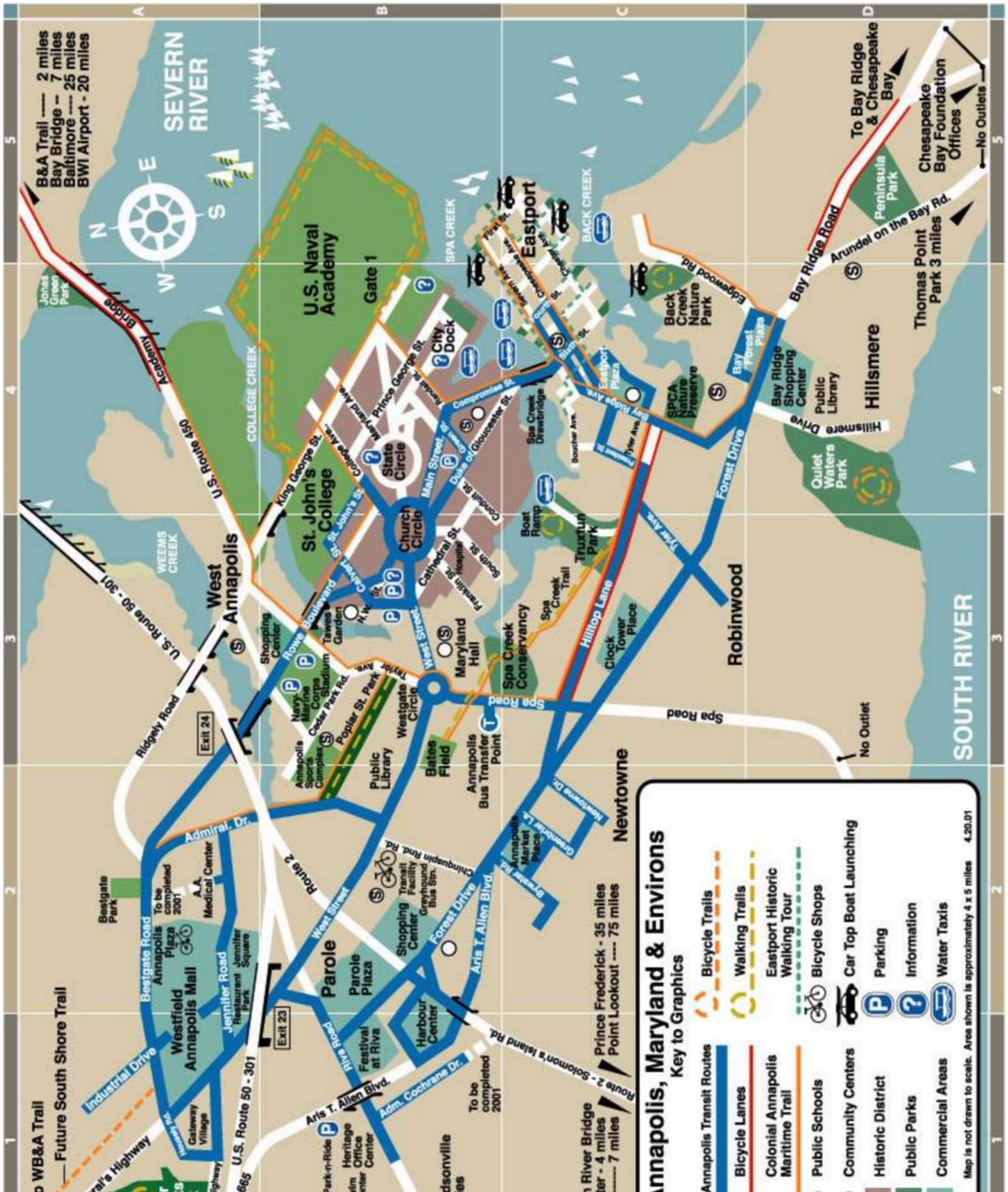
Enter at Gate 3, Workshop in Naval Academy Club one block northwest



Hotel and Banquet:



City of Annapolis:



Contacts:

Mr. Jonathan Milgrim, graduate assistant
jonathan.t.milgrim@wmich.edu
(870) 869-1087 (mobile)

Dr. Fritz Allhoff, conference organizer
fallhoff@law.stanford.edu
(269) 599-8595 (mobile)

Dr. Edward Barrett, local host
ebarrett@usna.edu
(312) 622-0261 (mobile)

Notes:

Notes:

Notes: