Cyberwarfare and Artificial Intelligence

August 1-3, 2017

University of Iceland
Reykjavik, Iceland

Háskólatorg HT-300
University Center
4 Sæmundargata
101 Reykjavík

Purpose:

Welcome to our workshop on the social, ethical, and legal implications on cyberwarfare and artificial intelligence. 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), and Dr. Patrick Lin (California Polytechnic State University). It is supported by funding from the U.S. National Science Foundation (NSF), under awards #1318126, #1317798, #1318270.

We owe special thanks to Mr. Jonathan Milgrim (University of Washington) and Dr. Ryan Jenkins (California Polytechnic State University) for administrative support. We also thank Dr. Helgi Thorbergsson for local support and venue procurement. Finally, we thank you, our workshop participants, for participating in this event!

Tuesday, August 1

6:00-7:00 Welcoming Drinks
Mikkeller & Friends Hverfisgata 12, Reykjavík

7:00-9:00 Self-Organizing Dinner

Wednesday, August 2

10:00-10:30 Opening Remarks

10:30-11:30 "Iceland and the Cyber Threat"
Dr. Helgi Thorbergsson, University of Iceland

11:30-12:30 "Cyberwarfare and AI: Diplomacy, Intelligence, and the Military"
Dr. Shannon Ford, University of New South Wales

12:30-2:00 Lunch at Háma
University Center (same building)

2:00-3:00 "Cybersecurity, Artificial Intelligence, and Nuclear Modernization"
Dr. Heather Roff, University of Oxford

3:00-4:00 "Making Democracy Harder to Hack"
Dr. Scott Shackelford, Indiana University

6:00-8:00 Dinner at Ostabúðin
Skólavörðustíg 8, 101 Reykjavík

Thursday, August 3

10:00-11:00 "Grey Areas in the International Law of Cyber Operations"
Ms. Liis Vihul, Cyber Law International

11:00-12:00 "Liability to What?: Responding to Non-Lethal Cyber Attacks"
Dr. Edward Barrett, United States Naval Academy

12:00-1:30 Lunch at Háma
University Center (same building)

1:30-2:30 "The UN, Cyberspace, and International Peace and Security"
Ms. Kerstin Vignard, UN Institute for Disarmament Research

2:30-3:30 "Interactions between Cybersecurity and Artificial Intelligence"
Dr. Peter Eckersley, Electronic Frontier Foundation

3:30-4:30 "Drone Killings in Principle and in Practice"
Dr. Morten Dige, Aarhus University

4:30-4:45 Closing Remarks

6:00-8:00 Dinner at Slippbarinn
Mýrargata 2, 101 Reykjavík

Presentation Abstracts

"Iceland and the Cyber Threat"
Dr. Helgi Thorbergsson, University of Iceland
In this presentation, the cyber threat situation in Iceland will be discussed. In particular, the role of the CERT-IS (Computer Security Incident Response Team) will be examined. CERT-IS's role is the analysis of cyber security threats and to give assistance to its primary constituency members using both proactive and reactive measures to prevent cyber security incidents and to minimize their impacts. In the event of cyber crisis CERT-IS's role is to coordinate responses.

"Cyberwarfare and AI: Diplomacy, Intelligence, and the Military"
Dr. Shannon Ford, University of New South Wales
Recent literature suggests that modern warfare involves new and unique features that render conventional ways of thinking about the norms of international political conflict as inadequate or redundant. One fundamentally important change has been the internet's emergence and global expansion and what actions in cyberspace might escalate a conflict. Another key change is the emergence of artificial intelligence and what it might mean for notions of meaningful human control. This session provides the opportunity to explore the key ethical considerations of the convergence of cyberwar and AI technologies for diplomacy, intelligence and the military. Traditionally, these are state institutions with significant responsibilities for national security. In particular, they have leading roles in managing international political conflict on the state's behalf. But how is the convergence of cyberwar and AI likely to impact the ability of these government institutions to play their respective roles in this area? And what are the key ethical considerations involved?

"Cybersecurity, Artificial Intelligence, and Nuclear Modernization"
Dr. Heather Roff, University of Oxford
Artificial intelligence (AI) is now at the essence of cybersecurity. We require AI to sift through vast amounts of network traffic and data flows to look for malicious activity. However, there is one area that we ought to start considering now that may prove a necessary evil and ostensibly a terrible idea at first glance: the need for AI nuclear surety. With increased calls in the US to modernize its strategic nuclear arsenal, there is a concomitant realization that the entire nuclear command and control structure envisioned in the early 1960s to ensure that nuclear missiles were never fired without appropriate authorization is threatened by the need to introduce modern information communications technologies. Presently there is no cybersecurity risk. Modernizing creates one. This talk works through how artificial intelligence may help or hinder cybersecurity risks to nuclear safety and surety.

"Making Democracy Harder to Hack"
Dr. Scott Shackelford, Indiana University
With the Russian government hack of the Democratic National Convention email servers and related leaks, the drama of the 2016 U.S. presidential race highlights an important point: nefarious hackers do not just pose a risk to vulnerable companies; cyber attacks can potentially impact the trajectory of democracies. Yet a consensus has been slow to emerge as to the desirability and feasibility of reclassifying elections—in particular, voting machines—as critical infrastructure, due in part to the long history of local and state control of voting procedures. This Article takes on the debate—focusing on policy options beyond former Department of Homeland Security Secretary Jeh Johnson's decision to classify elections as critical infrastructure in January 2017—in the U.S., using the 2016 elections as a case study, but putting the issue in a global context, with in-depth case studies from South Africa, Estonia, Brazil, Germany, and India. Governance best practices are analyzed by reviewing these differing approaches to securing elections, including the extent to which trend lines are converging or diverging. This investigation will, in turn, help inform ongoing minilateral efforts at cybersecurity norm building in the critical infrastructure context, which are considered here for the first time in the literature through the lens of polycentric governance.

"Grey Areas in the International Law of Cyber Operations"
Ms. Liis Vihul, Cyber Law International
This presentation will outline some of the key grey areas of international law that will emerge as the law is applied to cyber operations. Since very limited cyber-specific international law exists, most of the legal principles and norms that apply to state conduct in cyberspace are of a general nature, such as the principle of sovereignty and international humanitarian law. States can often interpret those pre-cyber international law norms differently when they apply them in the cyber context, resulting in states abiding by dissimilar rules when they engage in cyber activities. In order to achieve predictability and stability in cyberspace, states should publicly indicate how they understand those broad international law principles and norms to apply in the cyber context. This presentation will demonstrate how the interpretation of many key international law principles and norms can yield vastly different results.

"Liability to What?: Responding to Non-Lethal Cyber Attacks"
Edward Barrett, United States Naval Academy
Increasingly, states are maximizing their relative power through sub-lethal means that weaken adversaries economically, militarily, ideologically culturally and politically, but avoid crossing the threshold of "cause for war"—a line legally associated with the UN Charter Article 15 notion of "armed attack." This paper will examine justified responses to sub-lethal harms, with a focus on low-level cyber attacks. The first part will argue that anticipatory lethal defensive harm is justified in rare cases. The second part will argue that because even non-lethal responses are harmful, they should be governed by the criteria used to evaluate the use of lethal force. For example, before their use, authorities should determine that such measures are (narrowly) proportionate and necessary, and have a reasonable chance of succeeding in a proportionate manner. When used, the guilty should be targeted only as necessary, and collateral harm should be minimized and proportionate. However, I will also argue that because non-lethality relaxes constraints associated with lethality, responses to such attacks can include the consequentialist purposes of deterrence and reform, and can target "indirect participants" such as financial supporters who are not liable to be killed.

"The UN, Cyberspace, and International Peace and Security"
Kerstin Vignard, UN Institute for Disarmament Research
Since 2004, the UN General Assembly has convened five Groups of Governmental Experts (GGEs) on ICTs and International Security. The Groups have mainly focused on identifying norms of responsible State behavior, considering how international law applies to the use of cyberspace, as well as promoting confidence- and capacity-building measures. The latest GGE will conclude its work at the end of June 2017 but at the time of writing it isn't known whether the Group will agree on a consensus report. What is next for GGE process? Should the limited membership of the GGE be further expanded or should the process become more transparent and open to all Member States? If the current GGE is unable to reach agreement, will there be further steps at the multilateral level to build an open, secure, stable, accessible and peaceful ICT environment?

"Interactions between Cybersecurity and Artificial Intelligence"
Dr. Peter Eckersley, Electronic Frontier Foundation
This talk explores some of the likely implications of existing "narrow" AI techniques for cybersecurity; some of the unsolved security problems in current deep learning and reinforcement learning algorithms; some more speculative questions on how computer (in)security may affect the development of "general" AI technologies and contribute to geopolitical stability or instability in the process; and some of the policy options that are available for promoting stability during the development of these technologies.

“Drone Killings in Principle and in Practice”

Morten Dige, Aarhus University

It is a widely accepted claim that whether a given technology is being justly used in the real world is a separate question from moral issues intrinsic to technology. We should not blame the technology itself for immoral ways it happens to be used. There is obviously some truth to that. But I want to argue that what we see in the real world cases of drone killings is not merely an accidental or contingent use of drone technology. The real life use reflects to a large extent features that are inherent of the dominant drone systems that has been developed to date. What is being imagined "in principle" is thus to a large extent drone killings in dreamland. I use an historic example as a point of reference and departure: the debate over the lawfulness of nuclear weapons.

Participant Biosketches

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).

Edward Barrett, Col., Ph.D. is the Director of Research at the United States Naval Academy's Stockdale Center for Ethical Leadership. An Air Force ROTC-scholarship graduate of the University of Notre Dame, he completed a Ph.D. in political theory at the University of Chicago, and is the author of *Persons and Liberal Democracy: The Ethical and Political Thought of Karol Wojtyla/John Paul II* and numerous journal articles on ethics and political theory. While in graduate school, he worked for two years as speechwriter to the Catholic Archbishop of Chicago. After serving nine years as an active duty C-130 instructor pilot, he joined the Air Force Reserve, was recalled to active duty in 2003-2005 for Operation Iraqi Freedom, and recently retired as a Colonel from the Air Staff's Directorate of Strategic Planning.

Morten Dige, Ph.D. is Associate Professor in applied ethics at Aarhus University. He has given lectures, taught courses and provided expert advice in normative and practical ethics to a very broad audience of professionals in continuing education and professional development projects, committee members, politicians, business leaders, clinical ethicists etc., as well as university students at all levels. He has published articles and books about euthanasia, genetic enhancement, professional ethics, torture, drone warfare, and the ethics of war.

Peter Eckersley, Ph.D. is Chief Computer Scientist for the Electronic Frontier Foundation, and leads EFF's technology projects team. His work has included privacy and security projects, such as Let's Encrypt and Certbot, Panopticlick, HTTPS Everywhere, and the SSL Observatory; Helping launch a movement for open wireless networks; fighting to keep modern computing platforms open; helping to start the campaign against the SOPA/PIPA blacklist legislation; and running the first controlled tests to confirm that Comcastwas using forged reset packets to interfere with P2P protocols. He is currently leading a new EEF initiative on the policy, strategy, and governance questions raised by artificial intelligence and machine learning technologies.

Shannon Brandt Ford, Ph.D. is a Visiting Fellow at the University of New South Wales, Canberra where he is working on a research project supported by the Australian Army Research Scheme titled "Emerging Weapon Technologies: Political, Ethical and Legal Dilemmas." Before embarking on an academic career, Dr. Ford was an Intelligence Analyst and then Defence Strategist with the Australian Department of Defence. His recent publications include: "Cybersecurity, Trustworthiness, and Resilient Systems: Guiding Values for Policy," (2016 with Adam Henschke); "I, Spy Robot: The Ethics of Robots in National Intelligence Activities," (2015 with Patrick Lin); and "Jus Ad Vim and the Just Use of Lethal Force Short-of-War," (2013) in *The Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*.

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.

Silja Bára Ómarsdóttir, M.S. is adjunct lecturer at the Faculty of Political Science at the University of Iceland. Her research mainly focuses on Icelandic society and politics, Iceland's foreign and security policy and feminist international relations. She holds degrees in international relations from Lewis & Clark College in Portland, Oregon and the University of Southern California, as well as post-graduate certificates in methodology and university teaching from the University of Iceland. She is currently completing her PhD at University College Cork in Ireland and is engaged in numerous ongoing research projects on resilience and societal security. Ms. Omarsdottir is a women's rights activist and has served on the boards of the Icelandic Feminist Association, The Icelandic Women's Rights Association, the UNIFEM National Committee in Iceland, and the Icelandic Gender Equality Council. In the summer of 2011 she served on Iceland's Constitutional Council and chaired the committee addressing human rights and natural resources. Currently, she serves on the board of the Institute of International Affairs at the University of Iceland and the board of advisors of Höfði – Reykjavik Peace Centre.

Heather Roff, Ph.D. is currently a Senior Research Fellow in the Department of Politics and International Relations at the University of Oxford, a Research Scientist in the Global Security Initiative at Arizona State University, and Associate Research Fellow at the Leverhulme Center for the Future of Intelligence at the University of Cambridge. She is also a research fellow at New America in the Cybersecurity Initiative and the Future of War Project. Her research interests include the law, policy and ethics of emerging military technologies, such as autonomous weapons, artificial intelligence, robotics and cyber, as well as international security and human rights protection. She is author of Global Justice, Kant and the Responsibility to Protect (Routledge 2013), as well as numerous scholarly articles. She is currently working on a new project with Google Deepmind on ethics and AI.

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.

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.

Helgi Thorbergsson, Ph.D. is the Chairman of the Board of the Computing Services at the University of Iceland. He received his Ph.D. in computer science from Rensselaer Polytechnic Institute. He was the Technical Director of the Computing Services at the National University Hospital in Reykjavik, worked as a software engineer for several companies in Reykjavik and has been an Associate Professor of Computer Science and later Electrical and Computer Engineering at the University of Iceland since 1998.

Liis Vihul, M.L., M.S. is the Chief Executive Officer of Cyber Law International. She also serves as a member of the Estonian delegation at the United Nations Group of Governmental Experts on Information and Telecommunications in the Context of International Security, the Deputy Chair of the newly founded Global Commission on the Stability of Cyberspace's Research Advisory Group, the co-editor of the International Humanitarian Law Group in the Manual on International Law Applicable to Military Uses of Outer Space project, and is an Ambassador of the NATO Cooperative Cyber Defence Centre of Excellence. Previously, she spent 9 years as a senior analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence and was the managing editor of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Ms. Vihul holds master's degrees in law from the University of Tartu and in information security from the University of London. In 2016, she was awarded the Golden Badge of the Estonian Ministry of Defence for her work in international cyber law.


Center Hotel
Aðalstræti 4,101
University Square
Háskólatorg

Contacts

Dr. Fritz Allhoff
fallhoff@wmich.edu
+1 (269) 599-8595 (mobile)

Dr. Patrick Lin
palin@calpoly.edu
+1 (805)570-5651 (mobile)