**Cherie Noteboom:** Investigating physician perspectives of AI HIT projects for stakeholder management success factors, Project Management Institute's Sponsored Research Program, $50,000, Cherie Noteboom, PI. Successfully passed the first round of evaluation Spring 2022 & notified was not awarded the grant in the final round of assessment, Effort time period: Fall 2021-Summer 2022.

**Austin O’Brien:**

I helped cement the annual AI Sweden / DSU summer research program.

I am currently working on an IUSE grant with Dr. Rich Avery.

I attended the AAAI Conference. I anticipate submitting a paper or talk this upcoming year.

**Kyle Korman:**My primary focus for scholarship has been on my Ph.D. For this, I selected increasingly narrow areas for my dissertation. At the conclusion of the spring semester, I narrowed down to two topics to pursue. These two potential avenues were both to update existing literature; one would validate the impact of certificate revocation in MODBUS/TCP Security, the other is to proxy encrypted traffic in the same protocol for a potentially significant performance gain.

I put time into discussing the project with many faculty and selected a dissertation chair: Dr. Mark Spanier. With him, I began conducting a literature review and discussed how the potential research problems could be addressed by my research. Some dead ends were encountered throughout this time, but research is ongoing.

Concurrently, I was introduced to an existing group of researchers. They were continuing research conducted as part of the AI Sweden partnership. I was welcomed into the group and dug into the problems they are addressing. We started to polish up tooling so that it could reliably be recreated. This pursuit was intended to get the methodology and framework to a point so that a publication was possible.

**Mark Spanier:**

DSU + AI Sweden – Industrial Immersion Exchange Program – Co-Director and Faculty Advisor.

This 10-week summer project consists of teams of graduate students (DSU students + students from Swedish Universities) working on various AI/ML challenges identified by industrial partners. The teams of students begin their project at AI Sweden in Gothenburg, Sweden for 4-5 weeks and then travel to Madison, SD to complete the project for the remaining 4-5 weeks.

2022 Summer Program: Our Summer 2022 program (pilot year) consisted of 5 student researchers working on two projects on federated learning and prevention of backdoor and poisoning attacks related to autonomous cars. Volvo Cars was an Industrial Partner in this project. As a faculty advisor of the project, I traveled with the DSU Students to Gothenburgh, Sweden and assisted in the development of research questions and statements. While back at MadLabs (July) I worked with the students in the lab every day.

News Articles on the 2022 Summer Project:

* <https://dsu.edu/news/2022/08/cutting-edge-learning.html>
* <https://www.argusleader.com/story/news/education/2022/04/27/dakota-state-students-join-international-ai-cyber-consortium-sweden/9554228002/>

Paper from 2022 Summer Project:

**Detection and Prevention Against Poisoning Attacks in Federated Learning**

Viktor Valadi, Madeleine Englund, Mark Spanier, Austin O'Brien

Abstract: This paper proposes and investigates a new approach for detecting and preventing several different types of poisoning attacks from affecting a centralized Federated Learning model via average accuracy deviation detection (AADD). By comparing each client's accuracy to all clients' average accuracy, AADD detect clients with an accuracy deviation. The implementation is further able to blacklist clients that are considered poisoned, securing the global model from being affected by the poisoned nodes. The proposed implementation shows promising results in detecting poisoned clients and preventing the global model's accuracy from deteriorating. Preprint available at <https://arxiv.org/abs/2210.14944>

2023 Summer Project: As this review covers Summer 2022 – Spring 2023 I will only highlight the planning aspects of this project (more about awesome results and outcomes next year).

* During the end of the Fall semester and early Spring semester we held weekly meetings with Mats Nordlund and Mats Hanson from AI Sweden to develop the 2023 summer program.
* In March 2022 we selected the 12 student participants for the 2023 summer program. We had an extremely strong group of student applicants (plans to double Participants in future years).
* Through great efforts of Ashley Podhradsky and the RED office we were able to secure $350,000 ($75000/year) in industrial partnership funding with Case New Holland (CNH).
* In addition to providing funding support, we have work closely with Rami Riashy at CNH to develop one of the 2023 Summer Challenges around intrusion detection in agricultural equipment.
* In addition to CNH, we worked with Volvo Cars, Zenseact, Intel, and HPE to develop additional research problems and challenges for the 2023 Summer Program.

- EAAI: The Symposium on Educational Advances in Artificial Intelligence (DC)

**Varghese Vaidyan:**

V. M. Vaidyan and A. Tyagi, "Hybrid Classical-Quantum Artificial Intelligence Models for Electromagnetic Control System Processor Fault Analysis," 2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET), 2022, pp. 798-803.

V. M. Vaidyan and A. Tyagi, "Towards Quantum Artificial Intelligence Electromagnetic Prediction Models for Ladder Logic Bombs and Faults in Programmable Logic Controllers," 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC), 2022, pp. 1-6.

V. M. Vaidyan and A. Tyagi, " On Fuzzy Inference based Supervisory Control Decision Model with Quantum Artificial Intelligence Electromagnetic Prediction Models”, Int. J. of Cybernetics and Cyber-Physical Systems, Accepted (In press), 2022.

Vaidyan, V.M. and Tyagi, A. Electromagnetic Failure Analysis of Control System Processors. International Journal of Cybernetics and Cyberphysical Systems, 2022, pp. 184-208.

**William Bendix**

I completed two major research goals during the previous academic year. First, and most notably, in March 2023, Paul Quirk and I finished writing a 400-page book manuscript on foreign intelligence collection and subsequently sent it to an editor at Oxford University Press for consideration. The completion of this manuscript represents the culmination of a decade-long effort. Titled *Deliberating Mass Surveillance*, the manuscript tracks the development, implementation, and oversight of national security programs across the last 20 years. My coauthor and I were delighted to learn that the editor agreed to send our manuscript out for peer review because Oxford University Press is among the top academic publishers in political science. We were also delighted because, in having to pay blind reviewers for their referee reports, editors must desk-reject most book queries and manuscript submissions. The reviewers have since returned their reports (both are generally favorable), and we are now waiting for instructions from the editor on how to proceed next.

In the book, we give special attention to the Patriot Act, the USA Freedom Act, and the FISA Amendments Act, because these statutes have given the Federal Bureau of Investigation and the National Security Agency enormous investigative powers. Our main interest is to see whether policymakers, especially members of Congress, can find and maintain a balance between the often-conflicting values of security and privacy or whether they allow needless sacrifices of either one.

Above all, we seek to answer the following questions: Does Congress use information and policy analysis competently to make decisions about surveillance law and practices? What political and institutional conditions affect the quality of deliberation over national security programs? And what legal or organizational reforms would improve the balance between investigative power and privacy protections? To answer these questions, we have conducted case study analyses of the major security laws passed and amended since 2001. We have collected three bodies of evidence to determine whether, and to what extent, legislators made informed policy decisions on intelligence practices and programs. First, we have used the complete transcripts of all relevant committee hearings and floor debates in Congress to identify the public information and arguments that legislators relied upon to support decisions on surveillance. Second, we have examined leaked and declassified security files, and conducted interviews with policy experts, congressional aides, and government officials to determine, at least roughly, what classified information on surveillance programs legislators could access when they deliberated new measures. Third, to provide an independent basis for assessing legislative debates, we have consulted the entire range of substantive policy literature on security- and surveillance-related issues.

Because the manuscript covers debates over privacy, Fourth Amendment law, and surveillance technology, it provides me with important material for teaching CLI 492 (National Security Law). In fact, I could not teach this course without having conducted extensive research for this book project. National security law is a highly specialized area that requires extensive background not only in relevant statutes and court decisions but also in obscure government offices and advanced interception methods. I see the completion of this manuscript as a critical step in my development as a teacher-scholar, and I am confident that over the next year the book will successfully move through the review and revision process.

My second research achievement is coauthoring a paper that has been published in a peer-reviewed journal, *Foreign Policy Analysis*. Accepted in May 2023, the paper explores whether, and under what conditions, hawkish versus dovish members of Congress enjoy greater legislative success on foreign policy issues. Scholars are evenly divided on this matter. Some argue that hawks have disproportionate influence in foreign policymaking because a broad coalition of elites supports US hegemony. Others argue that doves gain legislative advantages when either Democratic presidents are in office or the United States is at relative peace. To settle this scholarly debate, my coauthor and I collected data on some 1,500 legislative measures pertaining to foreign policy that were introduced into Congress between 1971 and 2016. Specifically, we had to identify the sponsor for each measure, its primary foreign policy focus, the vote totals it garnered, and its ultimate legislative outcome. We also had to collect data on the many thousands of House members and senators who served across the five-decade period under investigation. Above all, we had to estimate their ideological locations on the foreign policy dimension to determine whether they were hawkish or dovish. We then conducted a series of statistical analyses—from very basic T-tests to hierarchical regression models—to see whether we would arrive at the same results regardless of our methodological choices. In the paper, we report that hawkish members receive far greater roll call support for their foreign policy measures than dovish legislators do. Additionally, we also show that hawks do not moderate, or water down, their foreign policy measures in order to see their measures pass, indicating that Congress has been a consistent source of hawkish policy for the last five decades.

I am thrilled to see this project in print. For one thing, it took us several years to collect the data, complete the necessary coding, and draft a polished paper. For another, *Foreign Policy Analysis* is an important international relations journal and a top outlet for the foreign policy subfield. I should add that I draw upon this work when I cover foreign policy discussions in POLS 350.