With the rise of the information age, cybersecurity has become increasingly crucial. According to Cybercrime Magazine, there will be a global talent shortfall of 3.5 million professionals in the field of Cybersecurity by the year 2025, making me expect to be one of the contributors. Moreover, the combination of artificial intelligence and information security in recent years has proven to hold significant research potential. This has made me even more excited about the future of cybersecurity. As someone who has completed several projects on AI + security, I am convinced that the combination of AI and security will be a trend in the future development of cybersecurity.

I was exposed to AI + security for the first time when I joined Dr. Peng Zhang's cybersecurity research group as an intern and researched Phishing Website Detection based on URL Sequences, during which I published a paper at the 2nd International Conference on Software Engineering and Machine Learning (CONF-SEML 2024). Dr. Zhang is an associate professor at the Institute of Information Engineering, CAS. I thoroughly reviewed over 50 highly cited related papers published after 2021, distilling relevant methods and seeking suitable ones to support my research. I found that although all the SOTA models can achieve impressive performance on detection, low efficiency caused by huge resource requirements and long training and inference time may become the bottleneck for published use. So I created an efficient model with the advantages of CNN, RNN, and attention mechanisms. Using parallel CNN layers with different-sized convolutional kernels, I could extract local features from different receptive fields and reduce the time for training and detection. Then, the output of the convolutional layers was put into GRU models, an efficient RNN model that could shorten the time with an efficient extraction of contextual information. Finally, a multi-head attention layer was applied for weighted enhancement, followed by a fully connected layer for result output. As a result, I achieved a significant speed-up by 34.93%, while the accuracy was 98.3%, which was close to that of the SOTA models. The proposed model has also been encapsulated into a browser plugin for users to utilize in their daily activities.

Inspired by the aforementioned research, I joined Professor Wang Weiping's team for summer research. My task was to create a model to generate a knowledge graph from a galaxy of unstructured Cyber Threat Intelligence(CTI) reports. Essentially, this means extracting Structured Threat Information eXpression (STIX) entities from each report and identifying the relationships between different STIX entities (STIX Relationship Objects, SRO). The main challenge was accurately grasping SRO between distant entities like one is in the beginning while another is in the end of the text. Since those traditional rule-based methods for CTI report analysis can do little for this problem, I turned to AI, and more specifically, Sentence Bert, a deep learning model designed to capture the contextual information and semantic meaning of sentences to solve this problem. I tailored the original model to suit the specific situation, and consequently, my model succeeded in this task with a Precision of 82.8%, while the non-AI model based on rule-based algorithms can only reach a Precision of 72.1%.

Despite my research experiences, I also built a solid fundamental for my advanced study in Cybersecurity during my Bachelor’s at Xi’an Jiaotong University. Moreover, diverse system development projects ingrained in me the importance of crafting secure system architectures, safeguarding sensitive data and resources, and proactively preventing systems from attacks. For example, I came up with a secure communication software based on the RSA/AES algorithm as a capstone project in Computer Networks, which can withstand man-in-the-middle attacks, replay attacks, and denial of service attacks targeting WebSocket communication, ensuring the security of the communication. These courses and training equipped me to grasp the essence of a system effectively, assisting in identifying potential security vulnerabilities.

In the future, I hope to be a security architect or security engineer in the industry. Your program can expose me to extensive practice opportunities and the most systematic training in Cybersecurity, preparing me for further career trials. I am especially interested in the Capstone Project, which will be helpful in my career search in Cybersecurity by exposing me to the real working environment. I will seize the chance to learn more advanced and practical techniques during the Capstone Project and broaden my networks in the industry. I believe that learning from your prestigious faculties in your program will be an eye-opening journey for me, helping me get closer to my goals.