The importance of cybersecurity has been all the more emerging with the continuing development of information age. However, news on severe computer security vulnerabilities could be seen nearly every day. 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. Solving cybersecurity issues needs joint efforts, and I 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, making me feel the new generation of cybersecurity to be more promising. For example, in the paper *Computational Sensor Fingerprints*, Professor Paweł Korus and Professor Nasir Memon from NYU CCS proposed a neural network-based approach to improve the performance and security of sensor fingerprints. As a matter of fact, I have finished several projects on AI + security, which enable me to realize that the combination of AI and security will become a trend in the future development of cybersecurity.

I was exposed in AI + security for first time when I joined Dr. Peng Zhang’s cybersecurity research group as an intern and researched Phishing Website Detection based on URL Sequences. He is an associate professor in Institute of Information Engineering, CAS. I thoroughly reviewed 50+ highly cited related papers published after 2021, distilling relevant methods and seeking suitable ones to support my research. And I found that although all the SOTA models can achieve impressive performance on detection, low efficiency caused by huge resource requirement 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 field and reduce the time for training and detection. Then, the output of the convolutional layers was put into GRU models, an efficient RNN model which 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 an significantly speed up by 34.93% , while the accuracy is 98.3%, which was close to that of the SOTA models. The results of this research have been documented in a published paper and the model has also been encapsulated into a browser plugin for users to utilize in their daily activities.

Inspired by the forementioned research, I joined professor Wang Weiping’s team for summer research. At there I was assigned to create a model to generate a knowledge graph from a galaxy of unstructured Cyber Threat Intelligence(CTI) reports, whose vertexes are Structured Threat Information eXpression(STIX) entities extracted from each reports and edges are the relationships of different STIX entities(STIX Relationship Objects, SRO). The main barrier is that it is difficult for model to accurately grasp 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 turn to AI to tackle it. I found Sentence Bert, a powerful deep learning model designed to capture the contextual information and semantic meaning of sentences, is perfectly suited for solving this problem, and tailored the original model to suit the specific situation. Consequently my model succeeded in this task with Precision of 82.8%, while the non-AI model based on rule-based algorithm can only reach Precision of 72.1%.

Despite my research experiences, I also built a solid fundamental for my advanced study in Cybersecurity during college. Comprehensive courses in computer science and software engineering such as data structures, computer architecture, computer networks, and software engineering were completed 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 within systems, and proactively preventing systems from security attacks. For example, I came up with a secure communication software based on the RSA/AES algorithm as computer networks class project, 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 further my study in the master degree in Cybersecurity and eventually attain a Ph.D. degree. Your program can expose me to extensive research opportunities, preparing me for further academic trials. Moreover, your Security Core courses can provide me with systematic training in Cybersecurity. I am especially interested in Applied Cryptography, which is a novel domain I expect to explore. Meanwhile, the Depth Electives can help me learn Cybersecurity from different perspectives. I also want to learn Biometrics to explore security from the perspective of biometric technology, thus generating more diverse perspectives in my future research. I believe that learning from the prestigious faculties in your program will help me get closer to my goals.