Testimony of Dr. Mai Abdelhakim
Assistant Professor at University of Pittsburgh

Pennsylvania State Senate
Local Government and Communications & Technology Committee Hearing
Cybersecurity Issues for Local Governments and Municipal Authorities
Wednesday, January 31, 2024

Chairwoman Pennycuick, senators, members of the Communications & Technology Committee, it is an honor to be here today and testify on critical cybersecurity issues in light of the recent cyberattack on the water authority of Aliquippa.

My name is Mai Abdelhakim. I am an assistant professor of electrical and computer engineering at the University of Pittsburgh. Prior to joining the University of Pittsburgh, I worked as a research scientist in the industry (2015-2016), and before that I was a postdoctoral researcher at Michigan State University (2014-2015). I received my PhD degree in Electrical Engineering from Michigan State University in 2014, where I focused on designing secure and efficient networks. For over thirteen years, I have been working on different cybersecurity problems including identifying vulnerabilities, detecting anomalies, locating compromised devices, authentication for reliable communications, and decision making in the presence of malicious attacks. I have led multiple funded research projects, as principal investigator or co-principal investigator, on cybersecurity, artificial intelligence, information networking, and internet of things, with funding from the Department of Defense, Department of Energy, National Science Foundation's Industry-University Collaborative Reseach Center (IUCRC), and partnerships with industry. I advise doctoral and master's students on the research topics mentioned above. I have active research collaborations with MIT Lincoln Laboratory, Naval Nuclear Laboratory, U.S. Army, Duquesne Light company, among others. In addition, this summer I will co-lead a program in collaboration with Idaho National Laboratory, which will focus on the resiliency of energy systems. I co-authored more than thirty-five publications in journals and refereed conferences, hold three patents/applications, and have been a speaker and chair at multiple technical conferences and other venues. Since 2016, I have been teaching graduate and undergraduate courses on information security, computer networks, and machine learning at the University of Pittsburgh. I also led multiple education initiatives including the development of a new school-wide certificate program, entitled, "Cybersecurity in Emerging Engineering Systems"[1], which was featured in the Pittsburgh Post-Gazette[2]. I designed it to enhance the cybersecurity skillset of engineering students in all engineering majors (electrical, computer, industrial, chemical, mechanical engineering, etc.). Based on my technical background and relevant experience, I

[1] https://news.engineering.pitt.edu/joining-the-frontlines-of-cybersecurity/
[2] https://www.post-gazette.com/business/tech-news/2023/12/02/aliquippa-water-authority-hack-technology-

recognize the importance and complexity of cybersecurity, and I am delighted to be here today to testify in this hearing about such a critical issue.

Today's engineering systems in our critical infrastructures that deliver vital resources to people, like water and energy, are facing major cybersecurity challenges. In those systems, we are witnessing increased integration between Operational Technology (which includes the control of various physical processes) and Information Technology (which includes cyber assets, digital data processing and networking). Such integration brings enormous benefits of increased productivity, flexibility and connectivity allowing remote monitoring and control of the physical processes. Yet, those features also introduce a wide range of vulnerabilities, which open the door for various threat agents to attack. For example, systems of Operational Technology traditionally used to operate in isolated networks that are disconnected from the global internet, but now they are increasingly utilizing internet connections often without having adequate cybersecurity measures. Accordingly, adversarial attacks could come from local or geographically near locations or from anywhere in the world. Hence, integrating cyber-and-physical assets introduces unprecedent cybersecurity concerns. Specifically, the impacts of cybercrimes are no longer confined to computers or cyber elements, which could result in revealing sensitive information, but could also cause devastating damage to physical assets, such as potential damage to equipment, contamination of water, blackouts in cities, or even more disturbing events. Therefore, cybersecurity has a direct impact on public safety, health, and local as well as national security, and there is an urgent need to secure our critical infrastructure from cyberattacks.

On November 25, 2023, attackers were able to disable the pressure monitoring system at Aliquippa's water authority. Adversaries targeted an electronic device, which is used to monitor and regulate water pressure, and were able to take control and shut down the device's operation. Based on publicly available information, the Cybersecurity and Infrastructure Security Agency (CISA) identified that the adversaries likely gained access to the system by exploiting weak or default passwords and internet connection[3]. Specifically, there has been human-machine interface (HMI) in the system that has security vulnerabilities as it did not enforce strong authentication. This unfortunate episode vividly highlights the importance of cybersecurity and the existence of hidden risks in both our public and private facilities. Moreover, the cyberattack on Aliquippa's water authority is one of many instances of cyberattacks on critical infrastructure in recent years. For example, there was a cyberattack on a water treatment plant in Florida in 2021, where the attacker was able to increase the sodium hydroxide level in the water supply hundred times more than it should be[4], which could have caused severe harm to the public. Fortunately, an operator was able to revert the setting to its safe state. These are just alarming examples that show how vulnerable many of today's systems are. Threat agents exploit known and unknown vulnerabilities to conduct their attacks. It is crucial to first recognize and analyze the breath of vulnerabilities in our systems involving modern cyberphysical technologies.

[3] https://www.securityweek.com/cisa-warns-of-unitronics-plc-exploitation-following-water-utility-hack/
[4] https://stateline.org/2021/03/10/florida-hack-exposes-danger-to-water-systems/

In general, the vulnerabilities in any system stem from three main sources: First, the **network**, including vulnerabilities in both local and global networking protocols. Example of local networks includes WiFi or ethernet, while global networks include internet connections; each of these two types of networks pose different security risks based on their associated protocols that could be exploited. Second, the **software**, including vulnerabilities in software applications, operating systems, and other programs that exist in the system, even if such software is not the frequently used or does not primarily contribute to operating the system (any malicious code attached to an app or interface, such as a cloud interface). Third, the **user**, including vulnerabilities introduced by people, not necessarily those who may have malicious intent, but more likely by benign users who are not aware of the risks, do not follow best practices to ensure the security of the system, or could fall victims to social engineering attacks (such as responding to phishing emails).

A major challenge with cybersecurity is when systems are heterogeneous, where different technologies, legacy and more modern ones, are used within the same system. This means that there could be variations in networking, software, and security protocols used in different parts of the same system, which drastically increases the vulnerabilities that could be exploited by threat agents. The exploit typically starts from the weakest link (aka most vulnerable part) and propagates to other parts of the system. Hence, installing one advanced and secured software cannot be expected to fully secure a system if used in conjunction with other highly vulnerable elements belonging to any of the three sources of vulnerabilities mentioned above: network, software, or user. As an analogy, consider a house with three doors, and we secure only one or two of them very well while leaving the third wide open. How secure will the house be? Now, imagine another hypothetical house with a thousand doors. That is the type of risk our new cyberphysical systems are facing today.

While difficult and critical, there are many ways we can secure our systems, or at the very least improve their resilience and security. To help address cybersecurity risks, multiple federal agencies have studied these issues and provided valuable resources in that regard. For example, the National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, has developed a cybersecurity framework[5] composed of five key elements, which emphasizes the need to identify assets, protect them, detect attacks, respond to attacks, and recover from any damage caused by cyberattacks. The framework serves as a guideline to formulating various aspects of ***security policies***, which elaborates on how security and resiliency are achieved. Implementing these policies will be through applying security mechanisms. ***Security mechanisms*** include methods to ensure the confidentiality, integrity, availability, and safety of systems.

Below, I am including some specific examples and best practices for security mechanisms that are becoming universally essential for enhancing cybersecurity. One key example is that for all applications allowing remote access, it is essential to apply ***strong authentication***, such as dual authentication methods, which will prevent intruders from accessing systems' resources

[5]. https://www.nist.gov/cyberframework

remotely. In addition, ***authorization*** based on access control policies should be applied while ensuring that security principles are achieved, such as least privilege (where access to resources is granted based on the absolute need to function). Other security mechanisms include ***Intrusion detection*** systems and ***firewalls***, which should be applied in multiple locations within a system and should be tailored to the system's operations to detect and filter suspicious network traffic. Another crucial security mechanism is to ensure that ***security patches*** of software are up to date, which helps guarantee that the applications are secure against newly discovered vulnerabilities. The update mechanisms of software should have integrity validation to ensure that it is from a trusted source. This hinges on requesting that companies providing software utilized in critical infrastructure responsibly disclose vulnerabilities and update their software when vulnerabilities are found or reported. It is worth noting that the U.S. government and other non-governmental organizations keep record of known vulnerabilities in commercial software and make this information publicly available, for example through the National Vulnerability Database maintained by NIST[6]. Finally, it is essential to address the vulnerabilities introduced by people, because responding to a simple phishing email can result in malicious software that can spread to all machines on the same network. To mitigate these user-introduced vulnerabilities, ***cybersecurity education and training*** for all those using systems in critical infrastructure could be provided.

Moving forward, it is of paramount importance to recognize the dynamic nature and fast pace of advancement in the technologies exploited by malicious actors. As technology advances, it gives both legitimate users as well as threat agents more capabilities. Hence, another key challenge with security is that attack strategies are continuously developing, where attackers can find new ways to circumvent security protocols in place. For example, attackers may use tools of artificial intelligence to craft attacks that are hard to detect. Accordingly, not only do we need to secure systems now, but we also need to continuously ensure that our systems are still secure as technology evolves. Hence, it is essential to regularly ***audit*** systems to examine their security strength, keeping in mind that attack strategies become smarter and more sophisticated with time. In sum, defense methods should improve accordingly and be ahead of attack development. That would necessitate ***supporting research and development*** on cybersecurity issues, which ideally involves close collaboration between universities, government agencies (local, state, and federal), and industry. Finally, it is becoming increasingly important to support ***developing and enhancing academic programs and workforce development efforts*** tailored toward boosting awareness and cybersecurity skills of graduates in the Commonwealth of Pennsylvania, especially that, as stated in the National Cybersecurity Strategy released by the White House, "there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide, and this gap is growing"[7].

[6]. https://nvd.nist.gov/

[7]. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf