**Marymount University**
**School of Technology and Innovation**
**Capabilities Statement**

1. *Introduction*

Marymount University is a nationally recognized academic institution headquartered in Arlington, VA. One of ten schools at the university, the School of Technology and Innovation focuses on education and research at the intersection of emerging technology, cyber defense, artificial intelligence, and human factors. Marymount is designated as a center for Academic Excellence in Cyber Defense (CAE-CD) by the NSA and DHS and holds a number of prestigious grants from NSA and NSF. Marymount has played a major role in developing cybersecurity education programs since 2008, with objectives to improve the number and the diversity (women and minorities) in the cybersecurity workplace, bearing in mind the significant workplace gap.

2. *Related Activities*

Marymount's programs involve up-to-date curriculum with hands-on learning and research at the undergraduate, graduate and doctoral level, also focusing on soft skills such as critical thinking and communication. Research is an important part of our culture and is encouraged at the undergraduate, masters, doctoral and post-doctoral research fellows.

Marymount faculty recognizes that technology alone will not solve the increasing cybersecurity defense dilemma. We recognize the need to understand the reasons why attackers attack and why users still click on phishing emails – the *cyberpsychology*.
We are currently playing a major role in developing higher-order thinking and research skills in practicing cyber professionals, in part through the doctoral program which is designed to stimulate some 150 working cybersecurity professional (working in military, civilian, academia, and private sector roles) to think deeper about solutions to the cybersecurity issues throughout the real world.

This doctoral research includes:

- Human factor considerations in cybersecurity
- Linguistic indicators of security failures
- Social media addition and its impacts
- Vehicle cybersecurity
- Mitigating risks with IoMT, cybersecurity in healthcare
- Cyberthreat Intelligence
- Supply chain cyber risks
- Election security
- Cyber diplomacy
- Cyber physical attacks
- Cyber audit readiness
- Small business cybersecurity readiness
- Cyber warfare
- The Dark Web
- Cybersecurity workforce
- Privacy, data and security in US.
- And many more

*3. Related Contract Experience*

Marymount continues to develop its grant and contract work including:

3.1. Red Team Research

Under an award from Millenium Corporation, Marymount Faculty and students are researching AI tools that can be used to improve the red team activities at the US Army, Thread System Management Office (TSMO), Test and Evaluation Cyber Center of Excellence (TECCE). Students are researching the role of social media in dissemination and how artificial intelligence models can be used to quickly identify disinformation campaigns.

3.2. Data Security Research

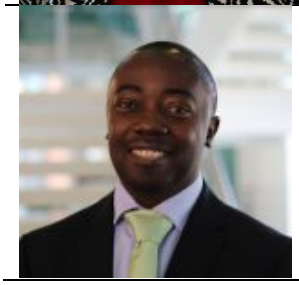
Data security and privacy are increasingly important with the increased volumes of data in most organizations (public and private) and the increasing distribution of this data including data lakes and data fabric. This research is funded by NTT Data and is in collaboration with the Cloud Security Alliance. The result of this research will be discussed at an RSA panel discussion in April 2023.

*4. Key Personnel*

Our research covers a broad range of cybersecurity topics, both technical and behavioral, as demonstrated by the key personnel shown below.

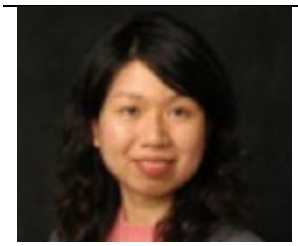
Dr. Diane Murphy is the Director of the School of Technology and Innovation and a Distinguished Professor. Her research areas include data security, trustworthy AI and innovation in the cybersecurity workforce. She is an experienced contract and subcontractor administrator having previously started and operated a software development company.

Dr. Alex Mbaziira is a professor with extensive experience in machine learning, primarily to detect deception and cybercrime using computational linguistic processes and psycholinguistic features to detect cyber-crime in the form of scams, fake review, fraud and disinformation. He is an experienced researcher and manages one of the school's research-focused contracts.



Dr. Andy Hall is a professor with expertise in the multidisciplinary fields of operations research, data science, and cybersecurity, specializing in applying advanced analytic techniques in solving complex decision programs. He is a veteran and joined Marymount after nearly 30 years in the US Army, finishing his military experience as the head of the cybersecurity program at West Point.

Dr. Michelle Liu research mainly concerns dynamic and complex relations between emerging technologies and human decision-making. She focuses on the governance, ethics and accountability of AI- based systems. Another area of her research is the resiliency and security of the healthcare industry, particularly medical devices and distributed data collection.



Dr. Alvaro Cintas-Canto's research interests are in hardware security, post-quantum cryptography engineering, and high-performance embedded systems design. His research consists of identifying vulnerabilities in different cryptosystems, including post-quantum cryptography, and implementing different security measures on hardware platforms such as field-programmable gate arrays (FPGA).

Dr. Nathan Green's research is primarily in Natural Language Processing (NLP), machine learning (ML) and human computer interaction (HCI). Dr. Green is also currently conducting research in new interfaces for human robot interfaces and interfaces and uses for extended reality (XR).

5. *Next Steps*

The Marymount University diverse team possesses interdisciplinary talents applicable to the ReSCIND program, including expertise in cyber defense, behavioral science and artificial intelligence. Our faculty is augmented with students at the undergraduate, masters and doctoral levels. Marymount is interested in finding collaborators (companies and academic institutions), as a subcontractor.

Contact: Dr. Diane Murphy dmurphy@marymount.edu.

## References

Mbaziira A.V, Sabir M., Al Harrack M. (2021), Book Chapter: Lying Trolls: Detecting Deceptions and Text-based Disinformation Using Machine Learning, Cybersecurity, Psychology, and Cognitive Science. Elsevier

Liu, X. & Murphy, D., (2020). A Multi-Faceted Approach for Trustworthy AI in Cybersecurity. Journal of Strategic Innovation and Sustainability, 15(6), pp 68-78.

Cintas-Canto, A., Mozaffari Kermani, M. and Azarderakhsh, R. (2021) "Reliable CRC-based error detection constructions for finite field multipliers with applications in cryptography," IEEE Trans. on Very Large Scale Integrated (VLSI) Systems, vol. 29, no. 1, pp. 232-236, Jan. 2021.

Beshaj, J. and Hall, A. (2020) Recent Developments in Cryptography, 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020, pp. 351-368.

Mbaziira, AV and Murphy, DR (2018). An Empirical Study on Detecting Deception and Cybercrime Using Artificial Neural Networks. In Proceedings of the 2nd International Conference on Compute and Data Analysis (pp. 42-46). ACM. - (Best paper presentation award)

Alhayani, S. and Murphy, D.R. (2022): A Machine Learning-Based DDoS Detection Approach for Early Warning on Internet Exchange Points, Security and Communications Networks (Submitted)

Sabir MF, Jones JH, Liu H. and Mbaziira AV (2019), Predicting Stealthy Watermarks in Files Using Deep Learning, 7th International Symposium on Digital Forensics and Security (ISDFS), 1-6

Green, N., Larasati, S., Duro, D., Murphy, D., and Laskey, K. (2022). Fact Rep: A Machine Learning Resource for Identifying and analyzing Misinformation During the COVID-19 Pandemic, Proceedings of the 51st Annual Meeting of the Southeast Decision Sciences Institute (SEDSI)

Liu, X. and Murphy, D. (2022): Applying a Trustworthy AI Framework to Mitigate Bias and Increase Workforce Gender Diversity, IEEE International Symposium on Technology and Society (ISTAS) 2022

Conrad, S., Liu, X., & Murphy, D. (2017, June 12-14). Do You Have a Cyber Delinquent at your House? A Strategic Framework to Prevent and Intervene Teen Cybercrimes. Paper presented at the 21st CISSE (Colloquium for Information Systems Security Education), Las Vegas, NE.

Nesvit, KV (209) The computational approach for recommendation system based on tagging data. Journal of Advances in Mathematics, Council for Innovative Research, Vol.16, 2019, pp. 8359-8367