Report on

Roundtable Discussion

Cyber London and CyNam

AI and Cybersecurity

TABLE OF CONTENTS

Date: 21/10/2024

Time: 14h00 – 17h00

Venue: Room AG01, City St George's, University of London

Number of Participants: 21

1. Introduction and Welcome

The roundtable event began with opening remarks from Mark Child, Co-founder and Director of Cyber London, who chaired the session. Mark outlined the session's focus: exploring the intersection of AI and cybersecurity and how Cyber London can influence UK policy in these domains. He underscored the need for collaboration across sectors; government, industry and academia to keep pace with rapid technological advancements, especially in the context of AI threats to cybersecurity.

Raj Rajarajan, Professor at City University and Co-founder of Cyber London emphasized the growing risk of AI-generated threats, such as deepfakes and other forms of AI manipulation, which challenge the detection and management of fake media. Raj highlighted Cyber London's role in leading the dialogue around decentralized security, online harm and cybersecurity education.

Both speakers emphasized the importance of proactive engagement with policy makers to address the critical gaps in AI regulation and cybersecurity resilience.

Introductions:

Each participant introduced themselves, providing insights into their professional background and perspectives on AI and cybersecurity.

Mark Child (Chair): Co-founder of Cyber London, Chief Executive at Quantum Evolve Business Enablement, where he focuses on driving innovation and strategic growth through advanced cybersecurity solutions. With a strong background in cybersecurity and business transformation, Mark leverages his expertise to help organizations navigate complex security challenges and enable business resilience. He focused on supporting SMEs in strengthening their cybersecurity practices.

Raj Rajarajan: Professor of Security Engineering and Director of the Centre for Cyber Security for Society at City St George's, University of London with a strong background in cybersecurity research and education. He is one of the Co-Founder of Cyber London. With over 20 years of experience in cybersecurity, he is recognized for his contributions to securing digital infrastructures and developing cybersecurity talent through academic leadership. Raj spoke about the challenges of deepfakes and the difficulty of detecting AI-generated images and voices. He has worked on numerous innovation projects and stressed the urgent need for decentralized AI security solutions.

Izak Oosthuizen: CEO of Zhero Cybersecurity & IT Support, focusing on bespoke cybersecurity solutions for SMEs. He is also the Co-Founder of Cyber London, recognized as the official Cyber Cluster for London, and the Founder of Winelands PASS. As a member of the Entrepreneurs' Organization, Izak actively contributes to the cybersecurity community with over 20 years of experience, bringing strategic insights and innovative solutions to the industry. He emphasized the need for pragmatic security measures for SMEs, many of which face financial and technical barriers to adopting comprehensive AI cybersecurity solutions.

Paresh Deshmukh: Co-founder of Cyber London and Founder of Baseel Group, which focuses on cybersecurity and data protection across 100+ countries. Paresh is a seasoned entrepreneur with significant experience in building high-growth businesses and fostering innovation. He is also the Founder and Director of the Global CISO Society, bringing together cybersecurity professionals. He discussed his work in AI practice in Saudi Arabia, stressing the lack of AI understanding among organizations and the growing complexity of security attacks. He highlighted the dual nature of AI, both its positive and negative impacts on businesses.

Simon Newman: Co-founder of Cyber London, currently the CEO of the Online Dating and Discovery Association (ODDA), Simon has a distinguished career in cybersecurity and public service. He previously served as CEO of the Cyber Resilience Centre for London, helping businesses and charities mitigate cyber threats. Simon has held senior management roles in the UK and internationally, including as Programme Director for the National Police Air Service at the Home Office and Strategic Advisor to Abu Dhabi Police.

Alistair Sharp: Senior Manager at Capgemini Invent, Alistair has extensive experience in consulting and strategy, working with organizations to drive innovation and digital transformation. His focus includes helping businesses navigate complex technological changes, particularly in the areas of AI and cybersecurity.

Clarie: Senior Project Manager at NCC Group, discussed her experience in managing AI-related projects and the exploration of new cybersecurity solutions for AI model security.

Amber Jayne: Head of Operations at RevEng.AI, Amber specializes in managing operations within the AI sector, with a focus on driving efficiency and overseeing strategic initiatives. Her leadership plays a key role in ensuring smooth operational workflows and innovation in AI solutions. She highlighted her focus on malware analysis, noting the ethical challenges in ensuring AI tools are used responsibly while maintaining stability in security systems.

Michael Charles Borrelli: Director at AI & Partners, Michael leverages over a decade of experience in financial services, compliance, and technology. He specializes in helping firms navigate the EU AI Act and ensuring responsible AI use with a focus on social impact.

Michael is also an AI 2030 Chapter Advisor and a prolific speaker and writer on AI, FinTech, and compliance. He emphasized the need for trustworthy AI solutions that safeguard patient data and healthcare systems from cyber threats.

Edward Starkie: Specialist in Cybersecurity Risk and Cyber M&A at Thomas Murray, Edward brings deep expertise in helping organizations navigate cyber risks, particularly in the context of mergers and acquisitions. His experience in managing cybersecurity during corporate transitions ensures that organizations can mitigate threats while maintaining operational security.

Yunus Ali: Founder of Offline AI Systems, highlighted the challenges of deploying AI-based machines in real-world environments, particularly the security implications of offline AI systems.

Jinal Shah: Co-Founder and CEO of Regulativ.ai, Jinal leads the development of AI-powered compliance automation solutions, helping clients streamline regulatory processes and save costs. His expertise lies in leveraging AI to provide comprehensive global compliance coverage across various industries. He focused on the regulatory challenges of AI and cybersecurity, and the trust issues that arise when deploying AI in critical sectors. He also emphasized the ongoing skills shortage in cybersecurity and the urgent need to train and upskill professionals.

Dmitry Blyumin: Co-founder and CEO at Atomatik, and Co-founder and Managing Director at RightClick Solutions, Dmitriy specializes in technology-driven solutions and leadership in automation and software development. His expertise spans managing teams and delivering innovative digital solutions across industries. He stressed that his background wasn't originally in cybersecurity but noted how AI introduces new threats, particularly in automating workflows and looked forward to innovative solutions for these problems.

James Henry: Consulting Director at Crossword Cybersecurity, James is an expert in cybersecurity consulting with certifications such as CISSP, CISA, and CISM. He is also a member and contributor to the OWASP AI Exchange, focusing on integrating AI into cybersecurity frameworks and ensuring compliance with international security standards like ISO 27001.

David Beer: Account Executive at Tendo Consulting, David specializes in managing client relationships and providing strategic consulting services. His role focuses on helping clients navigate complex business challenges through tailored solutions and innovative approaches.

Daniel Lang: Senior Account Director at Tendo Consulting Limited, Daniel specializes in building strategic partnerships and managing client relationships. His experience spans across various sectors, where he helps organizations achieve their goals through effective consultation and tailored solutions. Daniel spoke about the slow pace of regulatory changes and the challenges this poses in an evolving AI landscape.

Jed Kafetz (CREST): Cyber Practice Lead and a UK CREST Council Member, Jed specializes in cybersecurity leadership and shaping best practices within the cybersecurity industry. His role focuses on developing innovative strategies to address emerging cyber threats and ensure robust security frameworks. He discussed the need to securely deploy AI models, highlighting challenges such as the integration of AI into legacy systems and the security risks associated with large-scale AI deployment.

Agwu Nwoke: Partner in Cybersecurity and a Senior Cybersecurity and Risk Executive, Agwu brings extensive expertise as a Chief Information Security Officer and Head of Cybersecurity Consulting. With credentials like CISSP and CISM, he is a trusted advisor, mentor, and keynote speaker, helping organizations navigate complex cybersecurity challenges.

Bofin Babu: AI and Cybersecurity Leader and Co-Founder at CloudSEK (XVigil), Bofin has been driving AI innovations in cybersecurity since 2016. His expertise lies in developing cutting-edge AI solutions to detect and mitigate cyber threats, making significant contributions to the field of cybersecurity. He focused on deep learning in AI, noting its potential but also its susceptibility to being exploited if not secured properly.

James Leeke: International senior leader with expertise in strategy development, sales growth, and team leadership, James excels in identifying new revenue streams and driving customer success. With a proven track record in leading multinational teams and managing large-scale transformations, he focuses on building high-performing teams and delivering impactful business outcomes.

William Gurney: Technology Lead at Plexal, William is responsible for driving technology initiatives and innovation within the organization. His expertise includes leading teams in developing and implementing cutting-edge technology solutions across various sectors. He discussed the evolving cybersecurity challenges startups face, particularly around the adoption of AI models and the lack of available resources to secure these models.

2. Biggest Challenges in AI and Cybersecurity

During the introductions, participants also shared their views on the biggest challenges in AI and cybersecurity. The key challenges identified are:

- **Deepfakes and AI-Generated Manipulation**
  Several participants emphasized the growing threat of deepfakes and AI-generated content that can be used for misinformation. These AI-driven technologies are becoming increasingly difficult to detect and regulate, especially when they involve voice and image manipulation. This challenge is amplified by the difficulty in

identifying fake media at scale, especially in sensitive areas like marketing, public communication, and politics.

- **Lack of AI Regulation and Ethical Concerns**
  A recurring theme was the lack of AI-specific regulations, especially in critical sectors such as financial services and healthcare. Participants voiced concerns that regulations are not keeping pace with the rapid development of AI technologies, leaving organizations exposed to risks and compliance gaps. There was also significant concern about the ethical use of AI, with some participants highlighting the potential misuse of AI models for malicious purposes.

- **Data Security and Centralization**
  Many participants raised concerns about the centralization of data on platforms like YouTube, Facebook, AWS, and Google, which become major targets for cyber-attacks. State-sponsored actors and other malicious entities can exploit vulnerabilities in these centralized platforms, leading to large-scale data breaches. This risk is particularly high in cases where AI tools are used to process or store sensitive information.

- **Skills Shortage and Training Gaps**
  The skills shortage in AI and cybersecurity was identified as a significant barrier to progress. Participants pointed out that there is a lack of trained professionals who can manage the complex challenges posed by AI and cybersecurity, particularly in SMEs and startups. It was suggested that collaboration between academia and industry is crucial to close this gap and upskill the current workforce.

- **Misuse of AI Tools**
  A key concern expressed by several participants was the misuse of off-the-shelf AI tools by organizations without a deep understanding of cybersecurity. This issue is especially prevalent among SMEs, which may deploy expensive AI solutions without fully understanding the security risks involved, such as improper configurations or neglecting basic security protocols.

3. AI Priority Areas for the UK

The group then explored which AI-related areas should be prioritized for the UK's cybersecurity strategy:

- **Data Protection and Privacy:** Data protection frameworks were identified as a priority, particularly how AI is reshaping privacy concerns. The need to secure AI-driven data processing and storage systems was highlighted.

- **AI-Specific Regulations:** There was strong consensus on the need for AI-specific regulations that balance innovation with the protection of consumer rights. Regulations must encourage ethical AI development without stifling creativity or overburdening smaller firms.

- **Addressing the Skills Gap:** The cybersecurity skills shortage was another key focus, with participants stressing the importance of aligning academic training with industry needs. Collaborative efforts between universities and businesses were suggested as a way to close this gap.

- **Support for SMEs:** The discussion also touched on the need to create affordable, scalable solutions for SMEs, helping them navigate the complex regulatory landscape without being overwhelmed by costs or requirements.

4. Global AI Acts and UK Alignment

Participants discussed how the UK should position itself in relation to global AI regulations, especially those from the EU and US:

- **Global AI Acts:** The conversation touched on the development of AI acts in the EU and US, with participants debating how the UK should align its cybersecurity and AI regulatory policies to stay competitive while ensuring robust data protection.

- **Corporate Responsibility and Ethical AI:** There was broad agreement on the importance of corporate responsibility, especially for large tech firms, to ensure that their AI models are secure and ethically sound. Ethical considerations were seen as crucial to building public trust in AI technologies.

5. Defining Cyber London's Role in Influencing AI Policy

The group discussed how Cyber London could influence AI policy in the UK, identifying several strategic initiatives:

- **Unified Lobbying Message:** The importance of presenting a consistent and unified message when lobbying for regulatory changes was emphasized. Participants urged

Cyber London to collaborate with other cyber clusters to develop a common set of recommendations.

- **Creation of a White Paper:** The session proposed the development of a White Paper to consolidate the key points from the roundtable. This document would serve as a strategic roadmap to inform policy makers about the necessary regulatory updates and security initiatives needed to safeguard AI advancements.

6. Key Takeaways and Next Steps

The session concluded with a set of clear takeaways:

- **Commercially Viable Regulations:** Participants stressed that regulations must be commercially viable, enabling innovation while ensuring compliance. This would be particularly important for SMEs and startups, which often struggle with regulatory complexity.

- **Collaboration and Advocacy:** There was a strong consensus on the need for continuous collaboration between the industry, government, and academia. This collaboration would ensure that policies evolve alongside technological advancements.

- **Skills Development and Training:** Addressing the cybersecurity skills gap was a recurring theme, with participants calling for more partnerships between universities and businesses to provide practical, real-world training in AI and cybersecurity.

- **Focus on SMEs:** The need for affordable cybersecurity solutions for SMEs was seen as a priority, given the unique challenges they face in adopting AI while maintaining security compliance.

- **Drafting a White Paper:** A proposal to develop a White Paper was well-received, with the goal of influencing UK policy by summarizing the session's key insights and recommendations for future action.

7. End Note

The session concluded with Mark Child and Raj Rajarajan offering their closing remarks. They expressed gratitude for the engaging discussions and emphasized the importance of turning these insights into actionable steps. Mark reaffirmed Cyber London's commitment to supporting AI and cybersecurity innovations, particularly in the areas of policy influence, skills development, and cross-sector collaboration. The proposed White Paper will be an essential tool in advancing these goals, ensuring that the UK stays at the forefront of AI and cybersecurity.