Anh V. Vu

GE-01, Department of Computer Science and Technology, William Gates Building, 15 JJ Thomson Ave, Cambridge, UK, CB3 0FD
(+44) 746 351 1312 | anh.vu@cst.cam.ac.uk | www.cst.cam.ac.uk/people/vv301 | anhvvcs | anhvvcs

My research provides timely empirical measurements to explore cyberspace and its societal impact at scale, with a focus on the underground subcultures that foster online crime and harms. By integrating insights from both academia and industry, my work blends expertise in computer science and criminology to help better understand online threats and inform policy decisions for safety and security.

Education

University of Cambridge — Cambridge, UK
Doctor of Philosophy in Computer Science — 05 Jan 2022 – 05 Jan 2025
- Supervisor: Professor Alice Hutchings · Advisor: Professor Ross Anderson
- Thesis: Online Crime and Harms Following Externalities · Passed with no corrections
- Examiners: Professor Jon Crowcroft, Professor Nicolas Christin

Japan Advanced Institute of Science and Technology — Ishikawa, Japan
Master of Science in Information Science — 01 Oct 2017 – 21 Dec 2018
- Supervisor: Professor Mizuhito Ogawa
- Thesis: Formal Semantics Extraction from Natural Language Specifications for ARM
- Examiners: Professor Mizuhito Ogawa, Professor Kazuhiro Ogata, Professor Keita Yokoyama, Professor Minh Le Nguyen

Vietnam National University — Hanoi, Vietnam
Bachelor of Science in Information Technology — 05 Sep 2012 – 29 Jun 2016
- Supervisor: Professor Xuan Hieu Phan
- Thesis: User Behaviour Analysis and Personalisation in a Vietnamese Medical Information System
- Honours Programme · High Distinction (top 10/473) · GPA: 3.66/4.0

Work Experience

University of Cambridge — Cambridge, UK
Visiting Researcher — 28 Apr 2025 – Present
- **Advisor**: Professor Alice Hutchings / **Topics**: Cybersecurity, Financial Cybercrime
- Regularly visiting the Cambridge Cybercrime Centre and the Security Group to engage in continuous learning and research discussions.

TRM Labs | Blockchain Intelligence — San Francisco, USA
Contract Research Scientist — 28 Apr 2025 – 31 Jul 2025
- **Managers**: Adam Brownell, Aymen Jaffry / **Topics**: Financial Cybercrime, Blockchain Intelligence, Crypto Mixing Services
- Worked within the Traceability Team to develop novel methods for tracing Bitcoin transactions obscured by cryptocurrency mixing services.
- Handled several ad-hoc requests from law enforcement agencies to de-mix blockchain transactions processed by crypto mixers.

University of Cambridge — Cambridge, UK
Research Assistant — 21 Oct 2019 – 27 Apr 2025
- **Advisors**: Professor Richard Clayton, Professor Alice Hutchings, Professor Ross Anderson / **Topics**: Cybersecurity, Online Crime and Harms
- Collected large-scale cybercrime and extremist datasets, then analysed the longitudinal dynamics of their underground subcultures.
- Maintained a data-sharing platform, allowing 400^{+} researchers worldwide to access our cybercrime and extremist datasets.

Delft University of Technology — Delft, Netherlands
Visiting Research Student — 11 Jun 2024 – 11 Jul 2024
- **Advisor**: Associate Professor Rolf van Wegberg / **Topics**: Financial Cybercrime, Crypto Mixing Services
- Collaborated on a research project co-funded by the Dutch Law Enforcement on the facilitators of financial cybercrime.
- Analysed on-chain transactions of crypto mixers to understand the dynamics of their ecosystem following law enforcement interventions.

National University of Singapore — Singapore, Singapore
Research Intern — 06 Jan 2019 – 25 Jul 2019
- **Advisor**: Professor Min Suk Kang / **Topics**: Blockchain Network Security, Bitcoin, Cryptocurrency
- Conducted experiments simulating adversarial scenarios on our newly discovered partitioning attack against the Bitcoin P2P network.

Vietnam National University — Hanoi, Vietnam
Assistant Lecturer — 01 Oct 2016 – 30 Sep 2017
- **Advisor**: Professor Dinh Hieu Vo / **Topics**: Software Engineering, Data Scraping
- Taught several undergraduate modules, including Fundamentals of Informatics (INT1003) and Object-Oriented Programming (INT2204).
- Collected large-scale datasets for a Vietnamese bibliographic database designed to measure and analyse scholarly literature.

FPT Technology Innovation, FPT Corporation Hanoi, Vietnam

Research Intern 01 Dec 2014 - 01 Dec 2015

- **Advisor**: Mr Ngoc Tuan Le / **Topics**: Android, Robotics
- Mentored the FPT S.M.A.C Challenge 2015 competition, which had around 100 participants from over 50 teams.
- Researched and developed a mobile platform enabling developers to interact with smart humanoid robots (NAO).

Teaching & Supervisions

Supervisions at Cambridge

Supervisions at the University of Cambridge are a defining feature of undergraduate education, involving small-group, personalised teaching. One to three students prepare essays, problem sets, or readings in advance, which are then discussed in depth with a subject specialist during the sessions. This interactive format encourages critical thinking and individual analysis while also providing tailored feedback. I have been fortunate to supervise a range of subjects for many Cambridge undergraduate students, who are among the brightest minds in the world.

- Algorithms
  - 2023 Sutton Trust Summer School: 4 groups of 10 students, 4 hours in total.
  - 2022 Sutton Trust Summer School: 4 groups of 12 students, 4 hours in total.
- Software and Security Engineering
  - 2022-2023 Easter: 11 groups of 23 students for Clare (5), Emmanuel (2), Selwyn (3), Kings' (9), and Fitzwilliam (4) College, 33 hours in total.
  - 2021-2022 Easter: 6 groups of 14 students for Kings' (8) and Robinson (6) College, 18 hours in total.
- Databases
  - 2022-2023 Michaelmas: 7 groups of 15 students for Clare (5), Emmanuel (2), Selwyn (3), and Downing (5) College, 21 hours in total.
- Object-Oriented Programming
  - 2022-2023 Michaelmas: 8 groups of 18 students for Gonville & Caius (5), Trinity Hall (4), and Kings' (9) College, 32 hours in total.
  - 2021-2022 Michaelmas: 5 groups of 10 students for Robinson (6) and Fitzwilliam (4) College, 20 hours in total.

Final-year Undergraduate Projects at Cambridge

- 2023-2024: Andrei-Cosmin Moroca → Software Engineer @ Bloomberg.
  - Thesis title: "Interactive Longitudinal Visualisation and Analysis of Contractual Transactions on a Large Hacking Forum."

Teaching at Vietnam National University

- 2016-2017: Fundamental of Informatics (INT1003) for University of Engineering and Technology and University of Economics and Business.
- 2016-2017: Object-Oriented Programming (INT2204) for University of Engineering and Technology.

Publications

Peer-reviewed Conferences

Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services CORE A* PDF

Anh V. Vu, Ben Collier, Daniel R. Thomas, John Kristoff, Richard Clayton, Alice Hutchings 13–15 Aug 2025

- **SEC'25** – USENIX Security Symposium · Acceptance Rate 17.1% Seattle, USA
- Received an Honourable Mention Award for top 25 out of 407 accepted papers, among 2385 submissions.

No Easy Way Out: the Effectiveness of Deplatforming Forums to Suppress Hate and Harassment CORE A* PDF

Anh V. Vu, Alice Hutchings, Ross Anderson 20–23 May 2024

- **S&P'24** – IEEE Symposium on Security and Privacy · Acceptance Rate 17.8% · Briefing · CyCon San Francisco, USA
- Press coverage: The Register · LBT

Getting Bored of Cyberwar: the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict CORE A* PDF

Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton, Ross Anderson 13–17 May 2024

- **WWW'24** – ACM World Wide Web Conference · Acceptance Rate 20.2% · CyCon Sentosa, Singapore
- Press coverage: New Scientist · Associated Press · SC Magazine · The Record · LBT

Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras CORE A PDF

Anh V. Vu, Jack Hughes, Ildiko Pete, Ben Collier, Yi Ting Chua, Ilia Shumailov, Alice Hutchings 27–29 Oct 2020

- **IMC'20** – ACM Internet Measurement Conference · Acceptance Rate 24.5% Pittsburgh, USA
- Press coverage: Hacker News · Cambridge Research · LBT

A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network CORE A* PDF

Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu, Min Suk Kang 18–20 May 2020

- **S&P'20** – IEEE Symposium on Security and Privacy · Acceptance Rate 12.4% San Francisco, USA
- Press coverage: CoinDesk

Formal Semantics Extraction from Natural Language Specifications for ARM CORE A PDF
Anh V. Vu, Mizuhito Ogawa 07–11 Oct 2019
- **FM'19** – International Symposium on Formal Methods · Acceptance Rate 30.0% Porto, Portugal

Peer-reviewed Workshops

Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict PDF
Anh V. Vu, Alice Hutchings, Ross Anderson 30 Jun – 04 Jul 2025
- **EuroS&PW'25** – IEEE European Symposium on Security and Privacy Workshops · Briefing Venice, Italy
- Press coverage: Computer Weekly · Fast Company · Infosecurity · LBT

ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, and Extremism PDF
Anh V. Vu, Lydia Wilson, Yi Ting Chua, Ilia Shumailov, Ross Anderson 09–14 Jul 2023
- **WOAH@ACL'23** – ACL Workshop on Online Abuse and Harms · Website Toronto, Canada

PostCog: A Tool for Interdisciplinary Research into Underground Forums at Scale PDF
Ildiko Pete, Jack Hughes, Andrew Caines, Anh V. Vu, H. Gupta, Alice Hutchings, Ross Anderson, Paula Buttery 06–10 Jun 2022
- **EuroS&PW'22** – IEEE European Symposium on Security and Privacy Workshops · Website Genoa, Italy

Book Chapters

Identifying and Collecting Public Domain Data for Tracking Cybercrime and Online Extremism PDF
Lydia Wilson, Anh V. Vu, Ildiko Pete, Yi Ting Chua 01 Jun 2024
- Chapter in: Open Source Investigations in the Age of Google World Scientific
- Press coverage: Center for Strategic and International Studies (CSIS)

Professional Activities

Programme Committees

- The International Conference on Financial Cryptography and Data Security (FC): 2025
- The International Workshop on Cryptoasset Analytics (CAAW@FC): 2025
- The ACM World Wide Web Conference (WWW): 2024
- The ACM Internet Measurement Conference (IMC): 2022 (shadow)

Journal Reviews

- Journal of Cybersecurity: 2024

External Reviews

- The ACM Conference on Computer and Communications Security (CCS): 2025
- The APWG Symposium on Electronic Crime Research (eCrime): 2024
- The USENIX Security Symposium (SEC): 2024, 2023
- The IEEE European Symposium on Security and Privacy Workshops (EuroS&PW): 2022

Invited Talks & Lectures

- Online Crime and Harms Following Externalities
  [Invited Lecture] · Summer School on Cybersecurity @ Vietnam–Korea University of Information and Communication Technology (VKU), the University of Danang, Vietnam — online · 23 Aug 2025
- From Data to Insights: Evidence-Based Cybercrime Measurement, Prevention, and Investigation
  [Invited Lecture] · Statistics for Social Sciences (ISSS1010) @ Vin University, Vietnam — in person · 04 Jun 2025
- Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services
  [Invited Talk] · Seminar @ Vietnam National University, Vietnam — in person · 27 May 2025
- Beyond Whack-A-Mole: Disrupting Online Crime and Harms through Law Enforcement and Industry Efforts
  [Invited Talk] · Security Seminar @ University of Cambridge, UK — in person · 03 Dec 2024
  [Invited Lecture] · Malicious AI and Dark Side Security (FIT3183) @ Monash University, Malaysia — online · 24 Oct 2024
- Getting Bored of Cyberwar: the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict
  [Invited Talk] · DSO National Laboratories (formerly Defence Science Organisation), Singapore — in person · 17 May 2024
- PostCog: A 'Search Engine' Enabling Interdisciplinary Research into Underground Forums at Scale
  [Invited Talk] · Security Seminar @ University of Cambridge, UK — online · 27 May 2022

Conference Presentations

- Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services
  [Conference] · USENIX Security Symposium (SEC'25) — Seattle, USA · in person · 14 Aug 2025
  [Conference] · Cambridge Cybercrime Conference (CCC'25) — Cambridge, UK · in person · 23 Jun 2025
  [Workshop] · Workshop on Security and Human Behaviour (SHB'25) — Cambridge, UK · in person · 11 Jun 2024
- Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict
  [Workshop] · IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'25) — Venice, Italy · in person · 30 Jun 2025
  [Conference] · Cambridge Cybercrime Conference (CCC'24) — Cambridge, UK · in person · 10 Jun 2024
- Armed Conflicts and the Changing Behaviour of Low-level Cybercrime Actors
  [Conference] · IEEE Symposium on Security and Privacy (S&P'24), short talk — San Francisco, USA · in person · 20 May 2024
- No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment
  [Workshop] · Workshop on Security and Human Behaviour (SHB'24) — Harvard University, USA · in person · 05 Jun 2024
  [Conference] · IEEE Symposium on Security and Privacy (S&P'24) — San Francisco, USA · in person · 20 May 2024
  [Conference] · Cambridge Cybercrime Conference (CCC'23) — Cambridge, UK · in person · 22 Jun 2023
- Getting Bored of Cyberwar: the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict
  [Conference] · ACM World Wide Web Conference (WWW'24) — Sentosa, Singapore · in person · 15 May 2024
  [Conference] · Cambridge Cybercrime Conference (CCC'22) — Cambridge, UK · in person · 05 Sep 2022
- ExtremeBB: A Database for Research into Online Hate, Harassment, the Manosphere and Extremism
  [Workshop] · ACL Workshop on Online Abuse and Harms (WOAH@ACL'23) — Toronto, Canada · online · 13 Jul 2023
- PostCog: A 'Search Engine' Enabling Interdisciplinary Research into Underground Forums at Scale
  [Workshop] · IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'22) — Genoa, Italy · in person · 06 Jun 2022
- Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-Up, Stable, and Covid-19 Eras
  [Conference] · ACM Internet Measurement Conference (IMC'20) — Pittsburgh, USA · online · 29 Oct 2020
- Formal Semantics Extraction from Natural Language Specifications for ARM
  [Conference] · International Symposium on Formal Methods (FM'19) — Porto, Portugal · in person · 11 Oct 2019

Podcasts

- Hackting Out: Defacement and Hate Online amid Global Conflicts, with Michael Joyce and Professor Alice Hutchings.

Honours & Awards

Honorable Mention Award (top 25/407 accepted papers, among 2385 submissions), USENIX Security Symposium 2025 — Seattle, Aug 2025
Selected as a representative of the University of Cambridge at the Global Young Scientists Summit — Singapore, Jan 2023
Awarded the Monbukagakusho Honours Scholarship in financial support for my master's study — Japan, 2017 – 2018
Awarded Outstanding Undergraduate Student at Vietnam National University — Vietnam, Jun 2016
Awarded the Shinnyo-en Japan Scholarship in financial support for my undergraduate study — Vietnam, 2012 – 2016
Awarded 2nd Prize, Nam Dinh Provincial Informatics Merit Competition — Vietnam, Mar 2012

Professional Skills

Cybersecurity · Cybercrime · Threat Intelligence · Blockchain Intelligence · Open-Source Intelligence · Online Harms · Incident Response · Statistics · Data Science · Databases · Data Analytics · Malware Analysis · Reverse Engineering · Formal Methods · Software Engineering · Machine Learning | **Programming**: Python · Java · C/C++ · SQL | **Tools and Frameworks**: IDA Pro · Capstone · Apache Airflow · BigQuery · PostgreSQL · MySQL · Neo4j | **Languages**: English (full professional proficiency) · Vietnamese (mother tongue)

References

Professor Alice Hutchings

PhD Supervisor

- Computer Laboratory, University of Cambridge
- Email: alice.hutchings@cl.cam.ac.uk
- Phone: (+44) 1223 763 660

Professor Richard Clayton

Former Line Manager

- Founding Director, Cambridge Cybercrime Centre
- Email: richard.clayton@cl.cam.ac.uk
- Phone: (+44) 1223 763 570

Professor Nicolas Christin

External PhD Examiner

- School of Computer Science, Carnegie Mellon University
- Email: nicolasc@andrew.cmu.edu
- Phone: (+1) 412 268 4432

Professor Mizuhito Ogawa

MSc Supervisor

- School of Information Science, JAIST
- Email: mizuhito@jaist.ac.jp
- Phone: (+81) 761 511 247

Research Statement

My research provides empirical measurements and analyses to explore cyberspace and its societal impact at scale, with a focus on the underground subcultures that foster online crime and harms. By integrating insights from both academia and industry, my work blends expertise in computer science and criminology to help better understand online threats and inform policy decisions for safety and security. My primary approach is data-driven, with research questions addressed by rigorous quantitative and qualitative measurements of large-scale real-world evidence.

I. Prior Research

External factors, such as the pandemic, may cause significant shifts and enduring changes in human behaviour, both offline and online. My recent work explores the effects of major incidents that *intensify* or *disrupt* online crime and harms. I believe the best way to safeguard systems is to first understand how to attack them, so I am also interested in fundamental research that uncovers novel practical attack vectors as well as research that develops countermeasures.

▸ Intensifying Online Crimes: The Pandemic and Armed Conflicts

Turning Up the Dial @ IMC '20 [1] evidences the significant influence of Covid-19 on illicit trading activity on the largest underground hacking forum. This empirical observation can be attributed to the increasing time spent online by individuals during lockdowns. The paper reveals that various forum users overcame the 'cold-start problem' — where new traders face difficulty settling transactions due to a lack of reputation, yet they cannot gain reputation without trading — by engaging in low-value exchanges to build their trustworthiness before developing larger trading volumes.

Getting Bored of Cyberwar @ WWW '24 [2] explores the involvement of volunteer hacktivists and low-level cybercrime actors in the Russia-Ukraine conflict. Although they promptly participated in targeting digital assets of both countries after the invasion using DDoS and defacement attacks, this intensification was short-lived, with a clear loss of interest after a few weeks. Their activity may cause immediately noticeable effects, but the impact was mainly propaganda dissemination instead of contributing to the 'hard' digital frontline. While popular narratives tend to overhype and conflate these actors with persistent state-sponsored hacktivists, we believe they should be considered separately.

Yet Another Diminishing Spark @ EuroS&PW '25 [3] compares defacements seen in the Russia-Ukraine conflict to those in the Israel-Hamas war, discovering similar patterns peaking shortly after the war started. While attacks were two-sided in the case of Russia-Ukraine, they have been mostly one-sided in the Israel-Hamas war: most targeted Israel while no significant waves have hit Palestine, presumably as Palestine has far fewer sites, many of which are hosted overseas. Overall, the scale of attacks on Israel and Palestine has been much less than those on Russia or Ukraine.

▸ Disrupting Online Harms: Industry and Law Enforcement Interventions

No Easy Way Out @ S&P '24 [4] examines a concerted effort to dismantle Kiwi Farms, the largest forum for online hate and harassment. We show that solely relying on deplatforming, even by swift actions of several competent tech firms, can be insufficient. The forum traffic and activity were quickly disrupted, but gradually recovered after a few months. Many users temporarily decamped to Telegram, but returned when the forum was back and became even more connected. The industry often does better than government actions, but this extraordinary event suggests that shutting down a dispersed community is unlikely to be effective if the censor cannot incapacitate or deter the key operators.

Assessing the Aftermath @ USENIX SEC '25 [5] studies a global takedown of DDoS-for-hire services involving the FBI, NCA, and Dutch Police. In two waves (December 2022 and May 2023), over 60 domains were seized and redirected to police-deployed pages to collect access information. More than half of the first-wave seized domains and all second-wave seized domains quickly resurrected — albeit with significantly reduced traffic. We show that completely eliminating booters and DDoS attacks is hard; the market has demonstrated resilience, with the statistically significant drops in global DDoS attacks lasting only around six weeks. While such recurring efforts may not prevent determined actors from running and selling DDoS attacks in the long term, they contribute to making the market untenable to operate at scale, particularly during periods of heightened attack volumes, such as school holidays and Christmas.

▸ Cyber Attacks and Defenses: Novel Approaches

Erebus @ S&P '20 [6] is a novel attack capable of partitioning the Bitcoin P2P network in a stealthy manner, without the victims realising they are being isolated. It leverages the advantages of big Internet entities such as ASes and ISPs

to intercept and monitor thousands of 'shadow' malicious Bitcoin nodes. These can subsequently establish connections with legitimate nodes, gradually populating a large number of IP addresses into the victims' peering tables, and ultimately isolating them from the rest of the network. This vector also affects many other Bitcoin-based cryptocurrencies, such as Litecoin, Bitcoin Cash, and Dogecoin, necessitating a few protocol tweaks in the Bitcoin codebase.

CORANA @ FM '19 [7] is a dynamic symbolic execution engine designed for multiple ARM Cortex variants. Complicated obfuscations such as packers, indirect jumps, and dead conditional branches (often referred to as opaque predicates) pose challenges to traditional approaches for malware analysis, including both static and dynamic methods. CORANA is capable of effectively tracing IoT malware in the presence of these obfuscations. It was partly generated from natural language specifications of ARM instructions, and our paper demonstrates that this method can be systematically generalised to other variants, opening a potential research direction in applying formal methods to malware analysis.

▸ Open Science: Data Sharing, Reproducibility, and Extensibility

Reproducibility and extensibility are crucial to me. All data used in my work can be shared with researchers, enabling them to immediately pursue ideas to address real-world problems without spending months or years collecting data.

ExtremeBB @ ACL WOAH '23 [8] is a dataset for large-scale research into online hate, harassment, and extremism. It has been licensed to 141 researchers across 52 groups from 34 institutions in 12 countries, including the US, the UK, the Netherlands, Switzerland, Czechia, Poland, Australia, and more. Many publications using this dataset have been published, including five conference/workshop papers, three journal papers, two PhD theses, and a book chapter.

PostCog @ EuroS&PW '22 [9] is an interactive 'search engine' that enables researchers, especial non-technical scientists, to analyse our data visually and straightforwardly. I contributed to a chapter outlining how we ethically collect and share cybercrime and extremist datasets, as part of the book Open Source Investigations in the Age of Google [10].

II. Future Research Directions

Cybercrime proceeds are commonly cashed out via cryptocurrencies due to their decentralised and pseudonymous nature. While most blockchain transactions are transparent, advanced obfuscation techniques, such as crypto mixers, break the trail between deposits and withdrawals, making investigations much harder. My forthcoming work will focus on this specific domain of cybercrime: financial crimes and their facilitators, including three main components.

▸ Behavioural Demixing Methodologies

The inherent transparency of most blockchain transactions enables forensic analysis, which is often carried out by the blockchain intelligence industry (e.g., Chainalysis, TRM Labs, Elliptic, and CipherTrace). These firms and crypto institutions have recently developed advanced mechanisms, such as the Beacon Network, to streamline real-time monitoring, investigation, and response to illicit transactions. Yet uncovering funds that pass through mixers remains a major barrier and is sometimes infeasible: their inherent delays hinder real-time tracking, while their increasing complexity reduces confidence in investigations. If funds are mixed and cashed out within a short timeframe, such as a few hours, the data pipelines may not populate quickly enough to catch them, even by industry standards.

Demixing is the process of linking deposits and withdrawals that have been obfuscated. Obfuscation techniques may include using privacy-enhanced cryptocurrencies such as Monero (which naturally break the trail), non-KYC cross-chain swap services, and crypto mixing services (both centralised and decentralised). Some anti-money laundering regulations have been passed in the European Union and are coming into effect in the next few years. These will ban privacy coins such as Monero, which has already been delisted by many crypto-asset service providers. Law enforcement has intervened in some major mixers in the market, such as Sinbad in 2023 and BestMixer in 2019, collecting some ground-truth data [11]. However, new services have emerged to take their market share, with CryptoMixer now being one of the largest centralised mixers, and Wasabi Wallet the most popular non-custodial Bitcoin mixer.

While mixers use technical means and cryptography to obscure transactions, which may be unbreakable in principle, human behaviour often introduces exploitable patterns. For instance, while handling investigation requests from law enforcement during my work at a leading blockchain intelligence company, I observed recurring patterns of activity on weekends or with predictable delays (e.g., a few hours) when users mixed their funds. My research will further explore how historical behavioural patterns, both at the individual and group levels, can be leveraged to improve demixing, for example, the way they use mixers and their routine habits. This could be carried out in collaboration with law enforcement (who have many ground-truth insights) and leading industry partners (who have extensive resources).

Explainable and Provable Traceability

Law enforcement often relies on the blockchain intelligence industry for state-of-the-art demixing, as part of traceability efforts. While some cases can be handled automatically, many still require manual investigation. These firms, for example Chainalysis, can provide high precision in attribution with low false positives, but this often comes at the cost of coverage (i.e., recall) [12]. Attribution may be reliable for certain entities, yet attributing many mixers remains challenging. Current tracing methods, even those regarded as industry standard, remain largely heuristics-based.

One common heuristic is time-and-value matching, which can produce multiple candidate links, but the results are never certain as mixer fees are often dynamic and, in some cases, the actors have never withdrawn. Another approach relies on analysing user behaviour (as I previously noted), but in many cases, confidence levels remain insufficient. All demixing solutions are inherently probabilistic unless supported by solid evidence, such as shared IP addresses between deposits and withdrawals. As a result, the evidence cannot be used in court for prosecution, posing challenges for meeting the evidentiary standards required in legal proceedings. My research aims to develop more robust, explainable, and provable tracing methods that enhance overall confidence and admissibility in judicial contexts.

Measuring Sanctions and Regulations

The final component of my research agenda examines sanctions and regulations, focusing on how they evolve in response to law enforcement actions and compliance requirements. For example, I will evaluate the effectiveness of sanctions on crypto mixers (e.g., ChipMixer, BestMixer, and Tornado Cash) to assess whether these measures significantly influence the mixer ecosystem and user behaviour, with the ultimate goal of informing future policy decisions.

Another key focus is quantitatively assessing how well crypto institutions comply with regulatory requirements, for example, how regulations are adopted, whether KYC is properly enforced, and how users attempt to circumvent them. An initial observation is that in P2P crypto trading, which accounts for a substantial share of overall transactions, most trades occur outside of exchanges and violate certain KYC provisions. The issue is that, even though these regulations apply to all users, exchanges cannot link crypto assets to fiat transactions once users rotate bank accounts, resulting in a loss of traceability. The situation varies across countries, depending on their respective financial regulations. My research will systematically examine these dynamics and propose evidence-based recommendations.

References

[1] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras," in *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2020.

[2] A. V. Vu, D. R. Thomas, B. Collier, A. Hutchings, R. Clayton, and R. Anderson, "Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict," in *Proceedings of the ACM Web Conference (WWW)*, 2024.

[3] A. V. Vu, A. Hutchings, and R. Anderson, "Yet Another Diminishing Spark: Low-level Cyberattacks in the Israel-Gaza Conflict," in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2025.

[4] A. V. Vu, A. Hutchings, and R. Anderson, "No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Online Hate and Harassment," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2024.

[5] A. V. Vu, B. Collier, D. R. Thomas, J. Kristoff, R. Clayton, and A. Hutchings, "Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services," in *Proceedings of the USENIX Security Symposium (SEC)*, 2025.

[6] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2020.

[7] A. V. Vu and M. Ogawa, "Formal Semantics Extraction from Natural Language Specifications for ARM," in *Proceedings of the International Symposium on Formal Methods (FM)*, 2019.

[8] A. V. Vu, L. Wilson, Y. T. Chua, I. Shumailov, and R. Anderson, "ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, the Manosphere and Extremism," in *ACL Workshop on Online Abuse and Harms (WOAH@ACL)*, 2023.

[9] I. Pete, J. Hughes, A. Caines, A. V. Vu, H. Gupta, A. Hutchings, R. Anderson, and P. Buttery, "PostCog: A Tool for Interdisciplinary Research into Underground Forums at Scale," in *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022.

[10] L. Wilson, A. V. Vu, I. Pete, and Y. T. Chua, "Identifying and Collecting Public Domain Data for Tracking Cybercrime and Online Extremism," in *Open Source Verification in the Age of Google*, 2024.

[11] F. Miedema, K. Lubbertsen, V. Schrama, and R. Van Wegberg, "Mixed Signals: Analyzing Ground-Truth Data on the Users and Economics of a Bitcoin Mixing Service," in *Proceedings of the USENIX Security Symposium (SEC)*, 2023.

[12] K. Lubbertsen, M. van Eeten, and R. van Wegberg, "Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing," in *Proceedings of the USENIX Security Symposium (SEC)*, 2025.

Teaching Statement

I am passionate about teaching and have been involved in education since late 2016, starting as an assistant lecturer at Vietnam National University, where I taught first-year fundamental courses in informatics. Since joining Cambridge in October 2019, I have been actively engaged in university education, enjoying (and learning from) both teaching and advising students. I have supervised over 100 undergraduates through small-group teaching in core courses such as Object-Oriented Programming, Databases, Algorithms, and Software and Security Engineering. I have also supervised the final-year project of a Cambridge undergraduate student, who later landed a great software engineering position.

I. Teaching Philosophy

Cambridge is famous for its undergraduate supervisions (small-group teaching), where students are divided into groups of one to three for each subject. They prepare essays or problem sets in advance, which are then discussed in depth with a supervisor weekly. This format fosters critical thinking, independent analysis, and personalised feedback. Supervisors then report to the Director of Studies, ensuring that students receive proper guidance and support.

I have supervised students across several Cambridge colleges, and my teaching style is strongly shaped by this tradition. I aim to make my teaching interactive, engaging, hands-on, and personalised. I approach every session with preparation, supportiveness, and a focus on student engagement. I view teaching as a two-way process: not only imparting knowledge but also learning from students' perspectives. Some of my most rewarding experiences at Cambridge have come from exploring challenging questions and ideas sparked by my undergraduate students.

▸ Students Are the Centre

My teaching is student-centred, with the ultimate goal of helping students reach their full potential. I encourage them to think critically, actively identifying and comparing the pros and cons of multiple solutions before I explain my own. Once students have grasped the core material, I encourage them to ask questions that go beyond the lectures and introduce adjacent topics to foster curiosity and deeper engagement. I believe that students learn best from their peers, so I encourage them to complete homework independently and then discuss their solutions collectively with others to share perspectives and challenge ideas. In addition to live discussions, I prioritise asynchronous communication with students, aiming to respond promptly to their emails within one day, especially when exams are approaching.

> "*Your explanations are very clear and help a lot in my understanding of the course. You are also very careful to include everyone in the discussions and allow all of us time to contribute and come up with our own solutions before giving us the answer.*" — said a student at Gonville & Caius College, Cambridge.

> "*Good supervisions, which helped me improve conceptual understanding through clear communication. I was set a lot of supervision work, but I suppose I wouldn't know as much otherwise!*" — said a student at King's College, Cambridge.

> "*Great supervisor! Really enjoyed having supervisions with you, I felt you explained everything very well and the work was relevant to the course. :)*" — said a student at King's College, Cambridge.

▸ Personalisation is Key

I believe that every student is unique, so I evaluate each assignment individually, providing personalised feedback that highlights both immediate areas for correction and longer-term strategies for growth. I adapt question sheets when necessary — for example, by varying the level of challenge or by framing problems to align with students' backgrounds and circumstances — ensuring that the homework is challenging but not overwhelming. After every supervision, I provide detailed written feedback, which not only helps students recognise their strengths and identify areas for improvement but also offers alternative approaches, additional resources, and, sometimes, code corrections.

> "*Thorough discussion of questions, marked responses very helpful.*" — said a student at Selwyn College, Cambridge.

> "*The comments left on the supervision work were often very insightful, helping me consider better ways at tackling the problems. Additionally we had interesting discussions about topics adjacent to the module that helped challenge and expand my knowledge.*" — said a student at Fitzwilliam College, Cambridge.

> "*Hardworking and dedicated supervisor, very friendly and explains stuff well.*" — said a student at Downing College, Cambridge.

> "*I really enjoyed my supervisions with Anh and, although there was a lot of work to do at times, I feel that he was able to help me understand the all content covered in the course.*" — said a student at Robinson College, Cambridge.

Interactive and Hands-On Experience

I believe that hands-on experience with real-world examples is the best way to teach. Learning becomes far more engaging and meaningful when students can connect theory to practice, rather than relying solely on textbook concepts. I believe that if we want to educate future engineers, we should teach them how to build things, not just how to read things. Whenever possible, I always try to bring in concrete case studies for demonstration and, in some instances, live examples. For example, in the Security course at Cambridge, we explore aspects of physical security by teaching students how to pick a lock (and how to secure it), which not only illustrates key design principles of the world's most popular security system but also fosters problem-solving skills and curiosity. During open days, I demonstrate hands-on lock-picking to provide prospective students with a direct and memorable introduction to the subject.

"*I've learnt a lot about exploits that weren't covered in the lectures.*" — said a student at King's College, Cambridge.

"*A really great supervisor, who obviously puts a lot of effort into his supervisions. He manages to bring up interesting case studies and discussion topics while not losing sight of what is relevant to course material and exam question.*" — said a student at Fitzwilliam College, Cambridge.

"*Our supervisions were always filled with interesting discussion and enjoyable to be a part of. :)*" — said a student at King's College, Cambridge.

"*It was an eye-opener; a student immediately emailed me saying it was really enlightening.*" — said a professor who invited me to give a guest lecture to their students at Monash University.

II. Mentoring Philosophy

I have advised only one undergraduate student on their final-year project, so my mentoring experience is admittedly limited. I strive to be as supportive as possible of my students' goals, providing them with as much freedom as possible while ensuring they stay on track. I aim to foster their genuine passion, encouraging them to pursue projects that truly excite them rather than merely follow my instructions. I suggest potential ideas, but students are free to choose what aligns best with their interests or even propose entirely new projects. I encourage students to take full ownership and accountability for their work, understanding that failure is part of the process — much like my own PhD experience.

I view advising students as a two-way process: they have opinions and perspectives that I can learn from, and I have guidance and experience that they can learn from. To me, mentoring is more of a collaboration than a one-way process. I respect their opinions and in return, I expect mutual respect. I provide regular feedback but I am also equally open to receiving it, creating a constructive environment where both mentor and student can grow together.

III. Teaching Interests

Scaling my small-group experience to larger classes (e.g., hundreds of students) can be challenging. However, I believe my teaching philosophy remains applicable with the right strategies. I plan to extend my style with the support of PhD students, TAs, and peer students, while effectively layering it through core lectures, mid-sized tutorials, and optional deep dives. I will also attend all necessary training sessions to meet any university's teaching qualifications and audit courses taught by existing professors to learn effectively from their teaching methods. I am also open to collaborating with education researchers to incorporate new teaching methods into my classes whenever possible.

To preserve active interaction at scale, I will employ methods such as think-pair-share, live polling, and structured debates. To accommodate personalisation, I will design tiered assignments with optional challenge problems and combine automated grading for fundamentals with detailed feedback on more complex tasks. I will incorporate structured peer review of students' work using guided rubrics to approximate one-on-one feedback, and train TAs with sample solution guidelines to provide consistent, constructive comments. For hands-on experiments, I will introduce in-class mini-labs, live demonstrations, and optional TA-led breakout sessions. I will encourage peer learning and out-of-class Q&A through forums and dedicate a few minutes in each lecture to address the top-voted questions collected online.

I am excited to teach courses related to security at both the undergraduate and graduate levels, such as Computer Security and Software and Security Engineering. I am also eager to teach foundational courses in which I have prior experience, including Object-Oriented Programming and Databases. I would also be happy to teach courses on Cybercrime, covering major issues from an interdisciplinary perspective and providing advanced, up-to-date insights into the technical, legal, and societal dimensions of cyber threats — e.g., how cybercrime is committed, detected, regulated, policed, and prevented. I will adopt an interactive teaching style that fosters live in-class discussions with an evidence-based approach, drawing on real-world cases. I am also happy to supervise bachelor's and master's theses.