CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Autumn 2019

CDT update

Director Report
Professor Keith Martin

A new chapter has begun with the launch of the EPSRC Centre for Doctoral Training in Cyber Security *for the Everyday* at Royal Holloway. This is our first year operating under the modified name, but our seventh year as a CDT in Cyber Security.

The latest cohort

Our main aim for the new CDT was to diversify the research work conducted within the CDT. This requires not just diversification of projects, but also of recruitment, particularly with respect to disciplinary background. We are delighted that the cohort of ten students joining us in September 2019 admirably reflects these aims.

This cohort have backgrounds in Computer Science, Physics, Psychology, Politics & Economics, Mathematics and Natural Science. Four have previously worked in aspects of education, two have worked in journalism, and one has over a decade of consultancy experience. In a sector where women are significantly under-represented, it is also worth noting that six of the ten are women. This is going to be year of fascinating cross-disciplinary conversations!

New space

In May 2019 the Information Security Group and the CDT were moved to the refurbished Bedford Building, Royal Holloway's former library. There was some concern about the possible impact of this move, particularly since most of the new PhD desk space is within a large open plan area. I think, now the dust has settled, that the majority of students are happy about the move. The open plan area has been well-designed and is adjacent to a very nice communal kitchen area. The new dedicated CDT Hub on the lower ground floor is also a larger, brighter, and more pleasant space than the room we previously used for training, group working and other events. Overall, from the CDT perspective, I believe the move has been a good one.

Advisory Panel

An important aspect of the CDT governance is our external advisory panel, who are tasked with informally auditing the programme and keeping us in touch with ideas and perspectives from around the wider cyber security sector. We greatly appreciate the time that members of the advisory panel give to us, and the interest that they show in our progress. We are very grateful to the following new advisory panel members, who have all joined to help us with the slight realignment in focus of the CDT: Prof. Emma Barrett (University of Manchester), Conn Crawford (5G North East), Budgie Dhanda (Qufaro), Dr Johannes Kinder (University of Federal Armed Forces, Munich), Emma Leith (Santander), Prof. Kenny Paterson (ETH Zurich) and Dr Thyla van der Merwe (Mozilla).

Internal CDT management

Lastly, the new CDT comes with an enhanced support role. Claire Hudson will be continuing to support the CDT, but now as a full-time CDT Manager (previously her role was part-time). The enhanced role is primarily to improve our communications and publicity. Carlos Cid will also be taking up a new internal role in charge of our external partnerships – please get in touch with Carlos if you wish to get involved with the CDT through the likes of supporting training events, summer projects or hosting internships.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Inside the cohort

Blake Loring – 2015 cohort

As my PhD project is focused around program analysis for JavaScript, I rarely consider use cases for the approaches I develop outside of bug testing and program verification. As such, it came as some surprise when I was approached by Ronny Ko, a PhD student at Harvard University, who was considering using ExpoSE to improve the security and speed of content delivery optimization proxies. A content delivery optimization proxy is a tool that aims to reduce the time it takes to load a webpage. In particular, his idea was to use dynamic program analysis to reduce the cost and improve the performance of resource dependency resolution proxies. In resource dependency resolution proxies the proxy will load the target webpage in a real browser instance to detect the dependencies of a webpage and begin sending them before they are requested by a client. Here, we would use ExpoSE, a Royal Holloway developed symbolic execution engine for JavaScript, to automatically detect all of the resource dependencies for a webpage ahead of time, removing the need for the expensive and error-prone browser instance inside the proxy. To achieve this we had to redesign ExpoSE to enable symbolic execution of web pages and design a new style of symbolic test that would allow us to explore web page resource dependencies.

Our collaboration has been a brilliant experience and has led to a strong friendship. We have even had the chance to meet twice since beginning working together. Once when my plane fell flaming from the sky near Boston [https://edition.cnn.com/2019/07/05/us/virgin-atlantic-flight-fire-diverted/index.html], and a second time more recently in Hong Kong. Collaborations such as this are a big strength of academic life, and we have each expanded the other's knowledge beyond what could have been achieved if we had each stuck to our niche.

Robert Choudhury – 2018 cohort

I am just starting my second year of the CDT programme having finished a busy first year which included eight taught modules. Prior to entering the CDT I had completed an MSc in Information Security at Royal Holloway and therefore took advantage of the opportunity to explore subjects outside my previous experience. By attending classes and participating in labs, I learned about topics such as Machine Learning and Game Theory and was able to make contacts and friends in other departments. I was also permitted to attend courses at institutions outside Royal Holloway – namely a Malicious Software module at Oxford University.

The first CDT year has involved a lot more than just courses; it has included several elements designed to ready us for a career in research. Along with the other members of the cohort, I have participated in classic paper readings and presentations, training events in research skills and industry visits to explore prospective career paths. I have also had the opportunity to attend relevant conferences in Belfast and Croatia, enabling me to network with other researchers and get a sense of the current state of the art.

Overall I have found the cohort experience to be rewarding and helpful because the different scenarios we are exposed to highlight our diverse strengths and backgrounds, allowing us to learn from each other. We are currently brainstorming ideas for conveying security concepts for an upcoming HP event.

Thankfully, the first CDT year has not been 'all work and no play'. Social events have included wine tasting, pizza making, hiking and foraging! There is still a lot more work to do, but I feel in a much better position to progress thanks to this first year.

Natasha Rhoden – 2019 cohort

I have just completed the first month of my first year of the new CDT, which has been both exhilarating and challenging. I first met my cohort during an excellent hike which was organised by previous CDT cohorts and took place prior to the commencement of my classes. Given my psychological background, the technical knowledge and skills that I have developed as a result of my lectures have helped me to reflect on the relationship between my research interests and information security concepts.

The emphasis within the CDT on collaborative and multi-disciplinary perspectives is reflected in my cohort, whose research backgrounds include natural sciences, mathematics, cognitive psychology and computer science. The teaching methods are varied and include seminars led by accomplished researchers, reading groups and group presentations. In addition, we are provided with the opportunity to attend training sessions and national cybersecurity competitions. I have been fortunate to participate in a variety of social events with my incredibly friendly and supportive cohort. During my time here, I already feel truly welcomed and supported by everyone in the CDT and I look forward to the years that I will spend here completing my PhD.

Navigating Maritime Cybersecurity Training

Rory Hopcraft, 2016 cohort

Over the past few years, across all sectors, there has been an increased drive to improve cybersecurity training within companies. By providing training, companies aim to raise employee's awareness of the cyber risks they face, and provide the skills needed to help mitigate some of that risk.

Cybersecurity training and awareness programs are not new, but they pose challenges for industry to overcome. For the maritime industry these challenges include determining what cyber skills seafarers need to ensure the continued security and safety of vessels and crew, how to deliver training to employees who have limited connectivity and spend relatively short periods of time in one place, and how cyber skills provision can be verified and enforced.

For the maritime industry some of the answers to these questions can be found within the work of the International Maritime Organisation (IMO). While the IMO is the UN specialised agency charged with oversight of the maritime industry, they have engaged in very little discussion regarding maritime cybersecurity training.

The skillset and qualifications required by seafarers are outlined in the International Convention on Standards of Training, Certification and Watchkeeping (STCW). This Convention, created by the IMO, sets out detailed mandatory competencies that seafarers require before operating on board ships. These competencies include navigations skills, fire safety skills, and some security skills. However, there is currently no mention of cyber security skills.

The STCW Convention does assert the importance of seafarers being qualified and fit for their duties. The convention also states that all crew should be able to make a knowledgeable and informed contribution to the safe operation of a ship. This therefore means that the STCW obligates companies to provide training of crew that allows them to operate ships' systems safely. This provision is only going to gain importance with the continued digitalisation and automation of maritime operations.

However, the solution is not simply to provide generic training. The integration of maritime technology has been uneven and differences in ship type or operational environment can dramatically change the type of systems found on board. Therefore, the training and skills required by a particular crew will vary enormously.

STCW argues that seafarers who are newly on board a ship should be given a reasonable opportunity to become familiar with the shipboard equipment and necessary operating procedures for the performance of their duties. However, due to the complexity of system integration and the time-pressured nature of the maritime industry, crews are often required to learn on the fly.

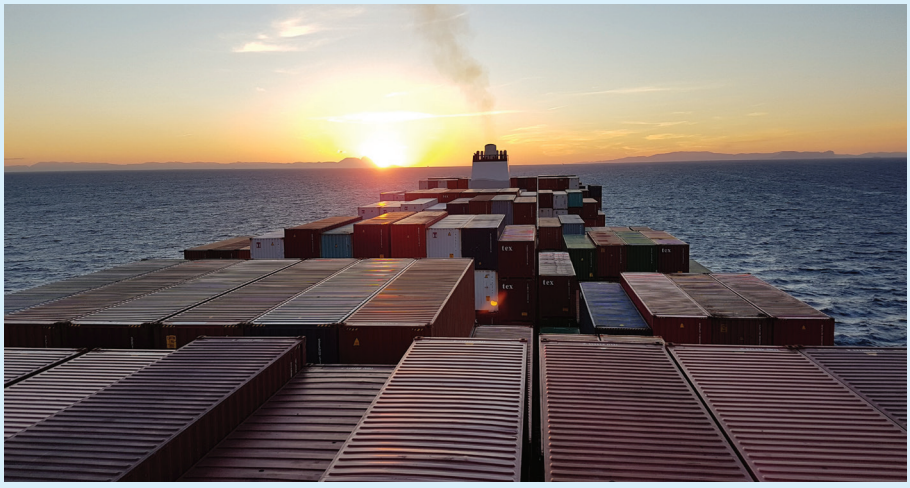
There are other IMO conventions that argue the importance of providing cyber skills to crew. Mandated under the Safety of Life at Sea Convention, the requirements of the International Safety Management Code (ISM) are designed to ensure that ships are operated safely. The ISM Code outlines that a company should identify equipment and technical systems for which sudden operational failure may result in hazardous situations. This implies that for a company to fully manage the safety risks presented by on-board systems, crew must be provided with the appropriate skills to reduce the likelihood that a ship will enter a hazardous situation and, if it does, be equipped to mitigate the situation.

The Code stipulates that these safety procedures should be documented within a ship's Safety Management System (SMS). In 2017 the IMO published Resolution MSC.429(98), which outlines that cyber risk management should be considered in a ship's SMS. As part of this process a company should establish procedures, plans and instructions for critical shipboard operations concerning safety that relate to cyber risks. The responsibility for implementing these processes should then be assigned to qualified personnel. However, these plans are often bespoke, as are the skills required to implement them. Further, the number of different systems (e.g. bridge systems, satellite communication systems or engine room management system) makes it almost impossible to foresee all the possible scenarios that a crew could find themselves in.

Determining the necessary competencies of seafarers is one thing, but ensuring companies are developing them is quite another. However, the solution to this problem is somewhat simpler. Through the current ship certification process, when a ship enters a port it undergoes Port State Control. At this point in its voyage the Port State Control Officer's (PSCO's) inspection ensures that the ship has the correct documentation and certification. For a ship to be issued with a Document of Compliance it must be able to prove that the crew have been provided with the appropriate skills to operate systems safely and securely.

Whilst this control process can be used to facilitate the enforcement and verification that appropriate training is being developed, it does raise its own challenges. What skills would a PSCO require to be able to determine whether a ship's systems are secure? What knowledge would a PSCO need to decide whether the crew is adequately trained in ensuring the cyber safety of a ship's systems? These are questions that have not been discussed openly by the international community.

The provision of cyber security skills to seafarers is challenging. This will only become harder as the industry moves towards fully autonomous ships. The international maritime community is starting to discuss these issues, but we are a long way from solutions.



International Data Protection

Amy Ertan – 2016 Cohort

This summer, Amy was a UK-Brazil Data Protection Fellow at the Institute for Technology and Society (ITS). As part of this appointment, Amy travelled to Rio de Janeiro for six weeks to join the institute's Law and Technology team.

As a PhD researcher straddling the intersection of information security and multidisciplinary security studies (looking at issues such as technology's impact on society, the role of the state, and human relationships with emerging technology), I am always interested in trying to understand the 'big picture'. There is always more to every story: how privacy means different things to different groups, and how data protection is treated as part of a wider security goal by the state, organisations, or members of a given society. The chance to undertake a Data Protection Fellowship at ITS represented a great opportunity for me to work with prominent researchers at an internationally recognised research institute both in (and beyond!) law and public policy forums. Thanks to support from the British Embassy and the UK Foreign and Commonwealth Office, I was able to join ITS in their main office in Rio de Janeiro, Brazil for a whirlwind six-week research fellowship.

What is ITS?

The Institute for Technology and Society has an incredibly broad mandate in contributing to international debates on the internet, digital rights and regulation of emerging technologies. The ITS are world-leading contributors to the international public policy landscape and provided expert advisors during the development of the Marco Civil Bill of Digital Rights in Brazil, continuing to advocate on issues including end-to-end encryption, privacy and data protection in the age of big data. In just one week of appearances in Brazil, ITS researchers spoke on the impact of cryptocurrencies, misinformation, election security, surveillance and artificial intelligence. The Law and Technology team focuses on the impact of legislation on regulation and the economy, and I became involved in analysing Brazil's Data Protection legislation which is due to be implemented in March 2020.

Being a Fellow

I arrived in Rio in late June (winter in Brazil, but still a very pleasant 32 Celsius). The first week was spent meeting the team and undergoing a crash course on the Brazilian technology and policy landscape, from serious issues around disinformation to government attitudes towards encryption and citizens' privacy. The ITS is well respected in Brazil and has close relationships with major civil advocacy groups and universities throughout (and beyond) Brazil. I was able to contribute information on UK implementation of European data protection legislation, and gave presentations on our data protection architecture, as well as how this regulation may need updating to incorporate advances in artificial intelligence. As part of the Fellowship, I attended and presented at two Law and Technology Conferences in Rio de Janeiro and Sao Paulo, speaking on 'Scrutinising AI', where I explored the current gaps in the regulatory regime and the active debate on whether AI regulation stifles innovation. I represented ITS and Royal Holloway at a Facebook 'Encryption and Privacy' workshop in Sao Paulo, covering the UK's encryption debate (and more recently GCHQ's 'Ghost Proposal' on WhatsApp group surveillance which was widely condemned by privacy campaigners). Knowledge exchange was a key part of the Fellowship and ITS arranged meetings with Google, Facebook, NuBank (a Brazilian digital bank similar in concept to Monzo), and various digital start-ups and civic advocacy groups. I also benefited from a fantastic day in Brasilia, meeting data protection experts from the executive, legislature, judiciary and the civil service. Being able to engage with a range of actors who will be key to shaping the future of Brazilian data protection standards provided an amazing opportunity to ask questions relating to ongoing developments and share information on the British approach to GDPR implementation.

Research

Similar in principle to Europe's GDPR, the Brazilian legislation has some differences when it comes to their data protection authority (which is not currently independent from the government). My research at ITS included an analysis of Presidential vetoes on the legislation that happened in my first week (culminating in my first 'FaceBook Live' interview), and answering queries about the British Data Protection landscape from Brazilian stakeholders. Discussing the challenges of operating a trusted, data protection authority with the senior civil service tasked with the creation of that very body remains one of the highlights of the Fellowship (topped by his compliments on my Facebook Live analysis!). As the Brazilian legislation represents a key opportunity for Brazil to strengthen data transfer agreements globally, I spent time looking at comparisons between Brazil and other Latin American countries such as Uruguay and Argentina, both of whom have met GDPR's adequacy standards for data transfer partnerships. Particularly in the context of wider trade deals (EU-MERCOSUR, in progress), data protection becomes a key condition on which trade might take place, highlighting the intersections between security concepts and information management, politics, economics and society.

Reflections

The fellowship was a fantastic experience not only to benefit from thinking about new issues, but also to gain perspectives and insight into public policy development around key technological challenges. Learning about the vibrant Brazilian civic advocacy and technology research environment, alongside the challenging and urgent priorities for Brazil, highlighted how privacy is a relative

concept depending on who, and where, you are. The attitudes of the right-wing Bolsonaro government when it comes to human rights (and the right to privacy) marks a sharp divergence from the UK approach. The legislative success of Brazil in terms of their Digital Bill of Human Rights, WhatsApp freedom and thorough data protection legislation is a testament to the expertise of public policy professionals in the country, and it was fascinating to have a window into this environment.

I will fondly remember many of the wonderful colleagues I met through the trip. The researchers at ITS – from the lively executives to the equally enthusiastic legal research interns – demonstrated a welcome willingness to share information and best practices. Additionally, a major part of my time on the fellowship was liaising with academics visiting from the University of Montreal and learning about how law and public policy departments tackle many of the same end goals as information security: the integrity and confidentiality of data, and the right to privacy. It was also excellent to have the opportunity to work alongside Fellows from Canada, the US, Switzerland, Argentina and Brazil, sharing our stories and the challenges of researching our related fields.

Living in Brazil was (of course!) an adventure in itself, and one that I recommend to others. Brazil is a beautiful place to visit: from morning runs along Copacabana beach, to samba in the streets, the trip to the Maracanã football stadium for Argentina-Venezuela and the gastronomical delights of Sao Paulo. Following the fellowship, I was able to fulfil a childhood dream of visiting the Amazon rainforest, being bitten by fire ants, catching my first piranha, and learning about indigenous rights in the current context of Brazilian political developments. I would recommend a fellowship of this type to any researchers who want to understand and contribute to policy debates elsewhere in the world.

For more details about ITS please see: **https://itsrio.org/en/en-home/**

CDT journeys

Andreas Haggman

I came to the CDT almost as the token non-technical person in my cohort. With an academic background in War Studies I thought I was going to occupy a small niche in cyber security separate from computer science and mathematics. I was partially right, but also very wrong.

Sure, my previous knowledge was different from most other students, but instead of working in isolation from more technical colleagues, I found that their skills and experiences enriched my own work and in turn I was able to enrich theirs – I hope! Cyber security truly is an interdisciplinary subject and for me the CDT offered an ideal environment to both appreciate and embrace this.

My research journey was unlike anything I could have envisaged – indeed, I am still not entirely convinced I did a PhD. My thesis emerged from my summer project investigating cyber wargaming, which had just been intended as an exploratory foray into something different and fun, but quickly grew into something much more substantial. For my thesis I ended up producing a tabletop wargame based on the UK National Cyber Security Strategy intended to provide players with an introduction to key concepts and terminology in cyber security. Through serendipity and perseverance, the game got traction with key stakeholders and I then travelled the world deploying the game to different groups of people to ascertain its pedagogic efficacy. Does three years of playing board games constitute legitimate research fieldwork? Apparently so!

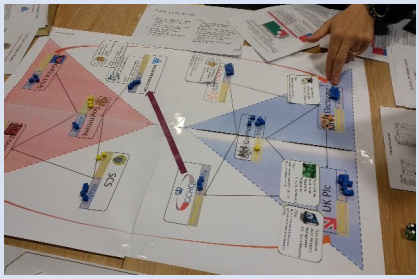
Aside from being an immensely engaging thesis that I never tired of, the work also yielded some insightful results. Most importantly, the game was successful in enabling players to create learning moments where they could share knowledge and come away from the game with a greater understanding of cyber security than they started. Statistically, the groups who performed best in the game consisted of players from mixed backgrounds (technical, non-technical, military, civilian) which reinforces the idea that cyber security is best tackled through interdisciplinary approaches.

In addition to my thesis work I used the opportunities afforded by the CDT to put my fingers in as many pies as possible. I published articles and book chapters on diverse topics including Stuxnet, offensive cyber, cyber deterrence, communications and technology, and cyber defence exercises. Also counting various magazine articles and blogs my total publications amounted to some 23 pieces. I attended 53 conferences and spoke at 27 of these. I led the organisation of the first two inter-CDT workshops with the Oxford CDT, which is a legacy that continues today. I spent three months in Canberra on work placement with Thales Autralia. I also participated in a CDT team in the 2017 Cyber 9/12 student policymaking competition in Geneva, on the back of which I was invited to help organise a UK version of the event, which I continue to be affiliated with today as Scenario Development Lead. In sum, I got busy, and the CDT was a wonderfully supportive environment in which to

CDT journeys

explore all the wonders that cyber security has to offer.

Amongst all these things some highlights certainly stand out as memorable. Being invited to guest lecture at the German Command and Staff College, with my game, was a an achievement dear to me because it meant both walking in the footsteps of Carl von Clausewitz – who is the doyen of War Studies – and taking my game to its spiritual home – the German military pioneered modern wargaming in the 19th century. I was also invited to write an article about my research for New Statesman which I still roll out whenever anyone asks what I did for my PhD (it is available online for anyone interested).



After all the excitement and adventure of the PhD, gainful employment had a lot to live up to. After submitting my thesis, I spent a short stint in the insurance sector trying to bring academic research to bear on cyber and geopolitical risks. Growing frustrated with this, however, I left for what is probably my ideal role as a Cyber Security Skills Policy Lead in the Department for Digital, Culture, Media and Sport (DCMS). In essence this has taken me full circle from being a product of the National Cyber Security Strategy to helping write the next iteration of the Strategy, alongside working on related policy initiatives. Working in the skills area is particularly gratifying as it is related to my thesis, and it lets me stay close to the academic community that has given me so much. If I can affect policies that enable the cyber security academic community to flourish it will be my way of giving something back, a small measure of thanks for four fabulous years in the CDT.

Jonathan Hoyland

As I neared the end of an undergraduate masters degree in 2013 I knew that I wanted to do a PhD. Casting around for programmes to which I could apply, one of my lecturers mentioned the CDT programme due to start at Royal Holloway the next academic year. My undergraduate and master's theses were both on using formal methods to analyse security protocols, so I knew that I was passionate about the subject. Analysing security protocols in this way involves building mathematical models of the protocol and proving the models have the properties we expect. I wanted to continue studying formal protocol analysis, and so I wasn't sure that a broadening training year was what I wanted, but I decided to try my luck and apply. As it turned out, this was an excellent decision.

The training year gave me a chance to consolidate my Computer Security knowledge, and take the time to study in depth all the topics I had read about during my undergrad, but this was not the most important part. The most important thing it allowed me to do was to read around my subject in a way I never had before, and learn about topics that I had never even heard of, let alone thought about studying for my PhD. I didn't realise until I was writing up my thesis years later that even the course that I had felt was furthest from my area of interest, Principles in Geopolitics and Security, had provided me with the language and tools I needed to argue the last chapter of my thesis.

At the end of my first year I decided make higher-order recursion schemes (HORS) the focus of my summer project. Higher-order recursion schemes are a powerful tool for describing complex tree structures in a form that can be reasoned about rigorously. Studying HORS played to my theoretical computer science background, and led me to spending a few months with a professor at the University of Tokyo towards the end of my second year.

At the start of my third year however, a chat over coffee about protocol analysis tools led me to helping out on a formal analysis of TLS 1.3 with Sam Scott and Thyla van der Merwe, in collaboration with partners at Oxford and the Max Planck Institute for Software Systems . TLS 1.3 is the latest version of TLS, the de facto standard for securing traffic on the internet. Because of its fundamental role in securing the internet the Internet Engineering Task Force (IETF) sought input from academia, including formal analyses to help with the design process of the new version.

Working on IETF standards became the heart of my thesis, which ended up not including any of my work on HORS. Turning on the head of a pin, I spent the remaining years of my PhD working on authentication in the context of TLS. It was through the IETF that I was introduced to Nick Sullivan, Head of Research at Cloudflare, who had drafted an extension to TLS 1.3 called Exported Authenticators. Exported Authenticators extend the security guarantees of a TLS connection to include multiple certificates from both the client and the server. I worked on a formal analysis of the draft and developed some new tools to capture its complex security properties. This analysis was a factor in the draft being advanced towards standardisation.

Whilst TLS 1.3 was being standardised, a topic that was raised repeatedly in the TLS working group was the removal of all non-forward secrecy modes. Forward secrecy means that an attacker who steals a server's long term key cannot decrypt sessions that completed before the theft. This is equivalent to saying that a passive attacker who knows the server's long term key cannot decrypt sessions. This makes it difficult for middle-boxes installed in corporate environments to monitor traffic in the way they could with TLS 1.2 and earlier. Those who were in favour of supporting this use case and those who were against it both published long documents as to what the requirements of a decryptable protocol would be. For the final chapter of my thesis I designed a proof-of-concept protocol that met all the requirements of both sides. This is where Foucault's writing on Panopticism came in useful, as it gave me the language to describe exactly under what circumstances it was unjustified to be able to decrypt a TLS session, particularly with regards to user consent.

The CDT provided me with so many opportunities, from working with academics from across the globe to exposure to topics from numerous different fields of study. I journeyed from America's Deep South to Tokyo's

urban jungle, and from the abstract reaches of theoretical computer science to the pragmatic concerns of wide-scale protocol deployment. The CDT broadened my horizons both literally and figuratively. My supervisor supported me in studying those topics that interested me, and I am immensely grateful for the opportunity to have studied at Royal Holloway.

After I finished my PhD I decided that I wanted to continue working in protocol design and analysis, and applied for a job with Cloudflare's Crypto team, which is where I now work. If you also would like to work on interesting and impactful crypto projects, Cloudflare is hiring both full time staff and interns. If you're interested you can email me at jhoyland@cloudflare.com

Steve Hersee

I joined the first Royal Holloway CDT cohort in September 2013 following careers in the RAF, police and private sector. Having spent 10 years working in security and intelligence I was attracted to a move into academia by the increasing relevance of cyberspace to the field of security, a desire to expose myself to a different perspective and a growing thirst to learn. Traditional PhDs were available but the Cyber Security PhD at Royal Holloway offered something different: a truly multidisciplinary approach, a close connection between Geopolitics and Information Security, the chance to take classes as well as conduct research, a close connection to the real world through industrial placements, and a cohort environment where we had others around to learn from.

I began with no clear idea of my research area but soon realised that there was one topic which both interested me and animated the cyber security community. In June 2013 Edward Snowden caused uproar by leaking top secret information from the NSA and GCHQ. Within my previous world of security and intelligence Snowden had committed a cardinal sin, compromising our capabilities and assets and handing a massive advantage to our enemies. But to much of academia Snowden had exposed the reckless activities of the security agencies, who had run roughshod over individual privacy and left the Internet more insecure. Whilst the cyber security community was working to improve network security, the security agencies were apparently undermining it.

Early within the CDT we held a debate amongst CDT students, geopolitics students and staff members about whether Snowden was a hero or a traitor. I led the argument against Snowden but was surprised by the passion and anger expressed by the other side and I sensed some hostility at my deviation from the academic status quo. The debate was great fun and was followed by further discussion in common rooms and pubs over the coming weeks, but this only succeeded in entrenching our pre-existing views. Mirroring the crypto wars, we were stuck in the same seemingly intractable problems of privacy versus security and state versus individual.

During this time, I attended Geopolitics classes with MSc students from the Department of Geography and I was exposed to a whole new way of thinking about security. Instead of focusing on how to create security we concentrated on security practices and queried whose security we were trying to defend. One concept which caught my interest was that of securitisation: a constructivist approach which describes the process by which an issue becomes a matter of security due to the existence of an existential threat. Once an issue has become securitised in this way, extraordinary activity (usually by a government) can be justified to counter this threat.

Within this framework I saw an interesting opportunity to study the crypto wars from a different perspective. To avoid becoming entangled in the debate I could use the securitisation framework to study how each side constructed their own versions of security. In doing so I hoped to bypass questions of who was right and expose ways by which better outcomes could be delivered for everyone.

Some limited literature covered the securitisation of cyberspace but focussed almost entirely on how the UK and US governments justified mass surveillance through the securitisation of terrorism, cyber attacks and hostile states. The literature was interesting but often seemed highly partisan and designed to fuel the debate rather than help address it.

I began to realise that whilst these acts of securitisation formed the building blocks of the crypto wars, they were also fuelling each other. Fearing threats to national security, the state tried to control use of encryption, but fearing a totalitarian state, digital rights activists tried to subvert controls on cryptography. Similarly, the state tried to enforce key escrow, while activists resisted it. More recently, the state siphoned data from technology companies, but those companies then implemented end-to end encryption. As actions by one side lead to reactions by the other, we descend into a spiral of increasing fear and insecurity.

Whilst looking for a way to describe this descent into insecurity I discovered the international relations concept of the spiral model, more commonly known as the security dilemma. This describes the process by which two parties end up at war despite their peaceful nature. Initial distrust leads one side to take security measures which spook the other, causing them to respond in kind. To the first party this action looks hostile so they increase their own security, leading to a spiral of insecurity and fear which can end in open conflict.

I realised that I could use this model, and the vast volume of research surrounding it, to study the crypto wars. My focus became not the actions of each side, but the feelings of fear and insecurity which drove these actions. This required me to focus on personal experiences, which I was able to collect through interviews with staff at GCHQ and directors of the Open Rights Group. I was also able to use my participation in the television show 'Hunted', which investigated different experiences of the surveillance state.

Through the unique opportunities presented by the CDT and the support of my supervisors I hope I have produced a unique thesis which adds a different perspective to the literature. I'm proud of what I achieved at Royal Holloway and left not only more qualified, but more capable of embracing new ideas and viewing the world from different perspectives. I also left Royal Holloway with a wife and three children but that's a different story - a PhD really is a life-changing process!

Summer Graduation

Professor Pete Adey

It didn't just rain, it poured! Fortunately, the bad weather didn't dampen the celebrations of the CDT graduands at this summer's ceremony who included Steve Hersee, Rob Lee, Pip Thornton, Naomi Farley, Carlton Shepherd, Andreas Haggman and Giovanni Cherubin. For me this was particularly meaningful as I had co-supervised both Steve Hersee and Pip Thornton through their PhD projects - in rain and sun - with Prof. Keith Martin. Both Steve, Pip and Andreas were also the first cross Information Security and Political Geography students who had gone through the CDT and helped set some of the groundwork for our new CDT in Cyber Security for the Everyday.

I always have mixed feelings on graduation day. It's a wonderful time to celebrate the success of the students, and there is plenty here – both in the way these students carried out their projects, winning paper prizes, presenting at eminent conferences, undertaking internships and paid working positions at numerous organisations and businesses - but also what they have gone on to do. For instance, Naomi Farley is a Senior Research Scientist at Thales, Carlton Shephard is a Research Scientist at Onespan, Andreas Haggmann is Cyber Security Skills Policy Lead at the Department for Digital, Culture, Media and Sport, Rob Lee is Senior Cryptography Engineer at Crypto Quantique. On the other hand, graduation is tinged with the sense that these brilliant people have gone on to other roles. Researchers like these are essential to the life of the academic community and working with them is a privilege and a mixture of fun, sometimes frustration (with each other!), and mostly hugely interesting ideas and hard work.

CDT Research newsbites

Blake Loring presented a paper on accurate automated testing of JavaScript code at the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI 2019) in Phoenix, Arizona.

Alpesh Bhudia, Lenka Marekova, Liam Medley and **Simon-Philipp Merz** each delivered presentations at a cyber-security research session, which preceded the 30th Information Security Forum's Annual World Congress in Dublin.

Feargus Pendlebury with Fabio Pierazzi, Roberto Jordaney, Johannes Kinder, and Lorenzo Cavallaro presented the paper, "TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time" at USENIX Security, Santa Clara, CA as well as three posters at CyberSec and AI, Prague. Their work focuses on the challenges of machine learning in a hostile, evolving environment, a theme that Feargus has continued to work on while spending three months at Facebook with the Abusive Accounts team.

Nick Robinson recently organised the 1st International Workshop on the Extraterritoriality of Data in Tallinn, Estonia (19/09), with colleagues from TalTech University and the University of Tartu. Next steps are being discussed regarding a special issue in an e-government journal.

Simon Butler has recently had a paper accepted by Chatham House, the Royal Institute of International Affairs, for the Journal of Cyber Policy. The paper explores the use of cryptocurrencies for illicit purposes and considers the threats that they could potentially pose. Comparisons are made to cash, which remains a far more useful and overlooked tool for criminal enterprise.

2020 entry: We are now open to receive applications for students to start their PhD studies in September 2020. If you are interested in applying, please contact us directly to discuss your suitability for the programme. Selected applicants are awarded fully-funded PhD studentships for four years. To be awarded one of the studentships, candidates will need to have an undergraduate and/or masters qualification in a relevant discipline. Suitable backgrounds are (but not limited to) computer science, criminology, economics, electronic engineering, geography, geopolitics, information security, law, mathematics, philosophy, politics, psychology, software engineering and war studies. We will also consider applicants with a professional background, so long as they are able to provide evidence of demonstrable academic skills as well as practical experience.

8194 11/19

EPSRC
Engineering and Physical Sciences Research Council

www.royalholloway.ac.uk/CDT
CyberSecurityCDT@rhul.ac.uk
@RHULCyberCDT

Royal Holloway, University of London
Egham, Surrey, TW20 0EX
+44 (0)1784 434455
www.royalholloway.ac.uk