CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Spring 2021

CDT update

Director's report

There are pros and cons of being a PhD student on a scholarship during a national lockdown. The pros are temporary job security (no furloughing!), and a job that is relatively self-contained and can be done remotely.

The cons are almost the same of course! The job is temporary, so those coming to an end have to job-seek remotely. The autonomous aspects of a PhD can also make it a lonely and isolating experience. Indeed the whole idea behind the CDT model is to inject a supporting infrastructure and social cohesion into the process, everything that lockdown withdrew. For some students with more practical fieldwork to conduct, lockdown has been highly disruptive and plans have been forced to change.

The eight students who started in September 2020 have had a surreal start. They were able to meet one another physically at the very start of term, but soon all training was online and they became increasingly used to knowing one another as animated digital rectangles on a screen. Fortunately they are all complete stars and, perhaps because of the adversity of the situation, they have pulled together as an outstanding cohort, delivering a fascinating group project on contact tracing apps and storming through all their virtual training events. Through virtual support from our external partners, we have been able to run a full training programme.

I think students in the middle of their PhDs have had the hardest time. This can involve dark hours of ebbing confidence, when having others around to help cajole projects onwards is so important. I am very impressed with all PhD projects that have progressed during the last few months, especially those where students had less-than-ideal working conditions and were suffering from personal anxiety. Every student deserves a pat on the back. Both the EPSRC and Royal Holloway have also been very supportive and most students who felt the need have had scholarships and deadlines extended as partial mitigation for time lost. This has come as welcome relief for those concerned.

And – yes – despite it all, PhD theses kept dropping out the end of the production line during the last few months. It seems a shame to hold a virtual PhD viva but, in the end, I think everyone agrees that they work perfectly well. The one big deficiency is the inability to go to the pub at the end (although a special thanks to Nick Robinson for making the pub come to us after his – nice one Nick...)

There have been many other successes, with CDT students continuing to publish top-quality research, write articles, record podcasts and conduct virtual internships. Please visit our blog and see the social media feeds for more details about some of those highlights. However, I do have to single out the CDT team who won the UK Cyber 9/12 Strategy Challenge earlier in the year. This is the CDT's second triumph in this competition, on each occasion with an all-female team. I shouldn't have to single the latter fact out, but cyber security remains a primarily male-dominated discipline and it is so important to promote female role models. Well done Team Minerva!

Let's hope for a slightly less virtual future and that there will soon be opportunities to get the CDT community back together in anything other than a Teams or Zoom meeting. We have closed recruitment to the CDT earlier than in any previous year, such has been the demand from high quality applicants, so the CDT's future looks bright despite the chaos that has surrounded us.

Inside the cohort

Giuseppe Raffa: A Definitely Unusual Start

We made it! The COVID-19 crisis has undoubtedly created a rather challenging environment for my cohort, as we did not have the opportunity to start our PhD journey in a traditional way. I must say that initially I was rather perplexed, as I thought that the lack of face-to-face interaction with lecturers and fellow students would have a negative impact on our learning experience. What happened over the last six months proves that I was certainly too pessimistic, and the spirit of co-operation of the 2020 cohort was the real winner.

The taught element of the CDT was a pleasant surprise for me. We all knew that our training would be interdisciplinary, but I suspect that very few of us, including me, had imagined that it would be so engaging, despite the circumstances created by the global pandemic. If I were asked to choose the highlights of the first term, I would mention the geopolitics course, where interaction is to my mind the key to success. I have always read about politics and international relations, which I see as an important background to many things that happen in the information security world, but the geopolitics lectures brought this to a different level. The second personal highlight was the group project, which explored contact tracing apps from a socio-technical and legal point of view. While I value what I learned about this important subject, co-operating with my cohort in a way that I had never experienced before was for me the most important outcome.

The presentation skills training and the white paper, which we completed at the beginning of March, were at the centre of our attention during the second term. After the first very intense workshop in January, I realized that delivering bad presentations is incredibly easy! The discussed examples made me think a lot about my style and I think that I am now much more aware of the possible pitfalls. In my experience, when working in a typical corporate environment, where people are frequently under pressure, delivering high-quality presentations is indeed a challenge. I am confident that this activity will guide us in the future and reshape the way we communicate in public.

My cohort has already been briefed on the summer project, which will now be our main focus as we transition from the taught element of the CDT programme to the beginning of our research. We are all aware that this is an important opportunity to start learning about either the topics we would like to explore during our PhD or a completely different area. At the moment, I have a very general, high-level idea of what I intend to work on. Having the experience of the Information Security MSc thesis though, I have no doubt that I will get all the support that I need to develop my ideas, however vague they might be now!

Dray Agha: Information Security has been a Wonderful Distraction

This may be an understatement, and oft repeated, but it has been a strange year. I can't claim that the last year has been any more strenuous for academia than other sectors, but over the last twelve months I've found myself in uniquely strange situations through being a PhD student. Whilst life has turned upside down for many, mine has only been mildly affected. I've felt like a cloistered monk; privileged to devote myself to philosophical tasks whilst other struggled. That doesn't mean, however, that the last year has not been both strange and frustrating at times.

For some PhD students, the research train has been running on schedule, just as planned. For others, it was derailed and alternative transportation had to be arranged!. Given the state of the world, it feels somewhat 'petty' to be frustrated at my own derailed research train. In the second century AD, the physician and philosopher Galen argued that the emotional reactions to the plague exacerbated many of the existing challenges against society's health. For some of us, anxiety and anger have consumed much of 2020, to the detriment of our mental health. It has been hard to concentrate this year, to be perfectly honest.

My personal priority this past year has been to better govern how I feel, so I do not find my research further disrupted by despair. Fortunately for us, the information security world is rife with knotty, messy distractions that offer refuge.

For example, I have thoroughly enjoyed getting stuck into the consequences of the Microsoft Exchange vulnerabilities that were woven together to create a devastating exploit.

ProxyLogon enables an attacker to bypass authentication controls and obtain administrative rights on a system. ProxyLogon has received much attention for how it has destabilised actors in the defence industry and governments across the world. Often forgotten, however, are the small businesses who do not have the technical or financial capacity to overcome the challenges that ProxyLogon has presented. I have enjoyed being involved in problem-solving projects concerning how best to support these smaller actors recover from resulting damage to their systems.

I've also been thinking a lot about wider problems. One issue involves the culture of open-source tools. Incredibly successful pen-testing companies generate enormous profits from using tools they obtain for free from Github. They're not required to contribute a penny to the creation or maintenance of these tools, and this is beginning to have real-world effects. A number of interesting discussions have come up around open source and the lack of financial remuneration authors receive. In March 2021, one of the maintainers for Responder - a tool that can catch the NTLM password hash relayed across a Windows environment - announced on Twitter that without financial support they would no longer be able to maintain the tool. This is just one example of the problems open-source culture is facing, and there's no simple solution to this very human problem. I'm working on it...

I haven't changed the world in lockdown and I haven't progressed my PhD as far as I would like. But I am very grateful to have had some wonderful and important distractions to wrestle with. No more distractions, however – the show goes on!

Inside the Cohort

Neil Ashdown: It's bigger than that, it's large

In his book Flag Fen, the archaeologist Francis Pryor writes about going through university at a time when the new technique of carbon dating was fundamentally challenging the accepted wisdom about human prehistory. "The new tide of radiocarbon dates produced some extraordinary results. At first, some of the dates were much earlier than archaeologists had expected. But, being human, they were loath to throw out their old ways of doing things just because some scientists told them their dates were wrong. So they pressed on regardless."

However, "[b]y the time I was doing the revision and research for my final degree exams, it was becoming increasingly apparent that the radiocarbon revolution was not about dates alone. Prehistory was being reassembled in a new order that would have profound effects not just on what we researched … but on our thought-processes themselves." Looking back with the benefit of hindsight, Pryor emphasises the positives – the opening up of the subject for new research, new methods, new vistas to explore. I wonder whether, at the time, he would have been more frustrated at having memorised a bunch of inaccurate dates.

The Day Today, Chris Morris' satire of television news, makes the same point. After it is reported that Prime Minister John Major has punched the Queen, crisis correspondent Spartacus Mills is asked, "this is huge history happening, isn't it?" He replies, "It's bigger than that Chris, it's large. I mean, if you've got a history book at home take it out, throw it in the bin, it's worthless, the history books now will have to be rewritten."

That feeling of seeing something being rewritten in front of your eyes seems very pertinent today. But it is also familiar. I graduated in the summer of 2007. Living in London at the end of that year, with friends working in finance, you heard that something bad was coming. "There's no liquidity anywhere," someone confided to me

at a party. I thought they meant we were running out of beer! Then came the financial crisis in 2008. I remember seeing someone I vaguely knew at university on the front page of the Times, carrying a cardboard box out of Goldman Sachs, their career changed overnight. I'm sure they landed on their feet. Lots of people didn't.

The traumatic experience of responding to systemic shocks can change how people and organisations act in the future. In the UK, the 'three Fs' – flooding and fuel protests in 2000 and the foot-and-mouth epidemic in 2001 – prompted a change in the government's approach to civil contingencies. The terrorist attacks in the US in 2001, and in London in2005, had a similar effect on government approaches to counterterrorism. Will something similar happen as the government moves out of the response phase of the pandemic, and what will that mean for the relationship between the state and society? Over the last twenty years, through all those crises, the UK government has advocated a new focus on national security as the protection of the population, their wellbeing and confidence in the future. The pandemic has shown the true scale of that endeavour. All the dates we memorised were wrong. What do we do now?

These are the questions I ponder as I sit in my flat watching the sun climb up the wall again. As I listen to the distant rustle of Slack notifications, the strained politeness of another overrunning Zoom conference. As I try to find positives in a year of colossal human suffering and waste.

At the end of the report about John Major punching the Queen, Spartacus Mills is asked to sum the situation up in a word. He says he can't. "How about a sound?" Mills replies: "Wuuurrhrhh".

Inside the Cohort

Tash Hales: A parent's view of the Oxford Spring School

I consider myself incredibly privileged to be able to do what I do: study at Royal Holloway, work towards my PhD and, after a successful application, attend the Oxford Spring School. Offered by the Politics and International Relations department at Oxford, I virtually attended 'Quantitative Methods for Social Scientists', a week-long course on methodologies and tools for quantitative text analysis, to help me better understand the large corpora I will be analysing in my research. The course was led by Dr Tom O'Grady from UCL's Department of Political Science, an excellent lecturer who left me feeling confident that I had been introduced to the most relevant areas of text analysis and that I was well equipped moving forward. All examples and case studies were modern, relevant, and the literature and reading lists given were current and accessible.

The online conference experience is a very different one to my pre-pandemic memories. I'm sure I wasn't the only attendee to be disappointed not to be dining in the 'Harry Potter' hall, socialising post-session with a cold beer in the sun, talking to my peers, meeting new people, and connecting. Despite that, I was determined to make the most of the content and the opportunity. The course ran every afternoon, with additional sessions in the early evening. I have three young children. As anyone who has young children will know, these are amongst the most awkward times of day for a parent , since they coincide with joys such as the afternoon school run, the witching hour of misery, dinner time, bath time and bedtime. The idea of leaving the children and staying for a week in Oxford seemed like a much preferable option to online screen gazing but, with a few small adjustments, online conferencing with children turned out to be a surprising success!

The lessons I learnt from a week-long conference included:

1. Instead of being a lively, engaged participant, the sound and video options must be turned off at all times to avoid embarrassing toilet requests or admissions.
2. Questions must be timed with precision, to ensure that you can be heard, and the answer understood, but also for the previously mentioned reasons.
3. During what would usually be the coffee break, where you mill around drinking terrible coffee that makes you feel jittery, talking awkwardly to people you've never met before, you instead have to mount a military operation in which aid packages are provided to every other child in order to negotiate a further 50 minutes of peace and quiet. This could include fruit, snacks, a drink, tissues for possible runny noses, and lots of nodding and smiling.
4. Data analysis programming tasks are best done with a glass of wine late in the evening when everyone else is asleep.
5. A miraculous solution must be found for the school run, in the absence of a scientific solution to the problem of how to be in two places at once.

After five days of fascinating topics such as document classification, scaling documents, unsupervised versus supervised methodologies, topic modelling, word embedding and automated data collection and web scraping, for the first time in a reasonable time during the pandemic, I felt really positive. There are many things that have changed for the worse in the last 18 months, but this week I was allowed to have my cake and eat it (the children ate quite a bit of it as well). If nothing else, the pandemic has made the Oxford Spring School accessible for people with caring responsibilities, which is also is a really positive outcome.

Inside the Cohort

Laura Shipp: The intimate geopolitics of charitable knitting: how crafting makes bodies

Published in *Social and Cultural Geography* on 22nd March 2021.

This research is based on fieldwork I did as part of my MSc in Geopolitics and Security dissertation. It focuses on the geopolitical (the spatial ways that power relations unfold) power of knitting for charitable causes. It is interested in why people participate in this activity and what they feel they achieve by doing it. The paper brings together two geographical areas of study in order to investigate this phenomenon, but also calls for more research to occur within this disciplinary intersection. These are intimate geopolitics, which studies entities that have otherwise been deemed apolitical, and the geographies of making which is interested in sites, practices and the materials of making.

Knitting in particular has a long history of being used for political causes and statements which rely on knitting's association as a cosy, comforting and domestic. I was particularly interested in the work of a charity that collects and donates knitted objects to send to refugees across the world, as those involved in its processes obviously felt that their work was achieving some good and chose this method of doing good over others. I set out to investigate what these motives were, how knitters imagined their work, and to more intimately understand what the charity does.

My fieldwork was conducted at the charity in the summer 2017 and a big part of this was becoming one of their volunteers. This meant participating in its everyday activities from unpacking and sorting the knitting that came in, sending it out to causes that needed it, and replying to knitters to let them know their knitting had safely arrived. I also conducted a set of 15 interviews with knitters, volunteers and the charity's founder. My final method was to learn to knit myself as a way of understanding the charity and the materials that flow through its networks in an embodied way, and to give my presence a kind of legitimacy with those I was working with day to day. This was a decision I made following pilot research in which the question, 'are you a knitter?' came up constantly and realising it was an important source of connection.

Within geographical scholarship, we often talk about 'the body' which we see as both a site in which different power relations come to take place on, but also as an actor that has its own geopolitical power. From my fieldwork, it became clear that the charity's work, and charitable knitting more generally, was all about bodies; both those of the knitters who were sending in their objects, and the imagined ones that they may imagine receiving the objects. Knitting is a practice that provides many benefits to those taking part in it, from improving mental health to a reason to socialise with others and prevent loneliness. It was also a way of being altruistic and the knitters felt exceedingly better to think of their handmade creations being gratefully received. The charity provided a means for those knitting to feel like they have the power to change something in the world whether or not their making fulfils the imagined future they have for it. This is done whilst encouraging them to use their skill and continue a hobby they enjoy.

Yet, the objects they produce, their size, shape and colour, confines the work the charity can do. The charity was overwhelmed with objects for small bodies, that of the imagined lost and lonely refugee child, but this imagined need did not reflect the actual needs request. Recipients of the charity's objects were far more often adolescent or adult men, bodies that greatly differed from the knitters' imagined beneficiaries. Each object became a representation of the geopolitical imaginations of their makers and who they felt needed caring for. This is particularly as the materiality of that object makes it inherently impractical, delicate and difficult to care for. The reality is that the charity was far less about connecting knitters with recipients, and more about connecting knitters with one another. This was vastly different from my own imagination of charitable knitting as a practice, but I found that the charity had a positive impact elsewhere. The charity convenes a community of knitters around this cause of making for others, which might otherwise never have formed. Giving knitters a motive to knit that warms their soul, caring for their donations, writing to them to say they have safely arrived, accepting their means of giving where few other places would, is all work the charity does to look after people and bring them together.

Inside the Cohort

Lenka Marekova: Breaking Bridgefy

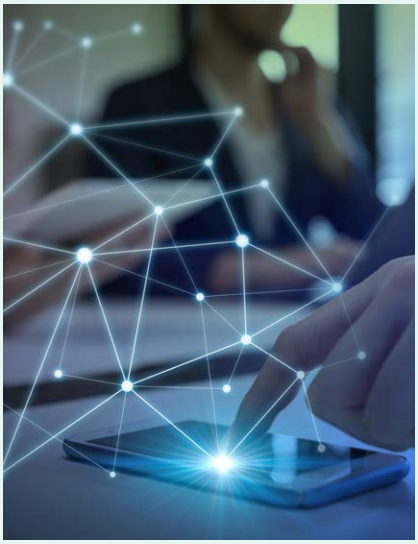
Mesh messaging applications allow users in relative proximity to communicate without the internet by way of wireless technologies such as Bluetooth Low Energy. Among such applications, there currently exists only one viable offering. Bridgefy has risen to public awareness with reports of internet shutdowns among protests across the world, starting in Hong Kong with the anti-extradition law bill amendment protests (though an internet shutdown did not take place there) and later spreading to protests in India, Iran, US, Zimbabwe, Belarus, and other countries.

However, the application was not initially intended for such a use case. Bridgefy began as an application for "music festivals, sports stadiums, rural communities, natural disasters, traveling abroad", and though its developers claimed it was secured by end-to-end encryption, none of its original use cases could be compared with the adversarial environment that result from situations of unrest, where attempts to subvert the application's security are not merely possible, but to be expected, and where such attacks can have harsh consequences for its users. Despite this, the developers also began promoting it for the protest use case.

Researchers from the ISG performed a security analysis of the application as well as its underlying software development kit, which other developers can use to build their own mesh messaging applications. First, we reverse-engineered the Android application to determine the specification of their cryptographic protocol. We examined this protocol and found several vulnerabilities, affecting both common security goals such as privacy and authenticity, as well as properties especially relevant in a protest such as reliability.

In Bridgefy as analysed, messages sent on the Bluetooth mesh network were first compressed with Gzip and then encrypted block-by-block using RSA with the deprecated PKCS#1 v1.5 padding standard. Without internet, all devices that came into Bluetooth range of each other automatically performed a handshake during which they exchanged their public keys. This handshake was not cryptographically authenticated and instead relied on user IDs and Bluetooth addresses to establish identity. As a result, two attacks were possible: an attacker could impersonate any user, as well as perform a full attacker-in-the-middle between any two users in range, without the users noticing that their messages are no longer private and may have been modified by the attacker. The use of PKCS#1 v1.5 was also problematic – thanks to composition with Gzip compression, we were able to instantiate a new variant of Bleichenbacher's attack that could decrypt a message using 130,000 chosen ciphertexts on average, a more resource-intensive attack but well within reach of an adversary with the ability to confiscate the target user's phone and hold it overnight (without unlocking the phone). Further, an attacker with a physical presence could easily track Bridgefy users and reveal their social graphs just by passively observing the network. Finally, it was possible to effectively shut down the entire network with a single specifically-crafted message, a blow to the claims of resilience when faced with internet shutdowns.

We verified the attacks in practice on Android devices using an attacker's device running a Bridgefy application modified with Frida, a dynamic instrumentation toolkit that allows injecting scripts into a running application. We disclosed the vulnerabilities to the Bridgefy developers at the end of April 2020, agreeing on a public disclosure date in August, as would be standard. However, the Bridgefy team began informing their users that they should not expect confidentiality guarantees from the current version of the application much earlier, though it did not stop them from continuing to promote the application for use in protests. At the end of October, the Bridgefy application was updated to use the Signal protocol. If implemented correctly, this would rule out many of



the attacks we found, but we have not reviewed these changes and we have recommended an independent security audit to the Bridgefy team.

Since this research was concluded, it has become clear that media reports may have exaggerated the real use of Bridgefy on the streets, especially in Hong Kong. However, there is some evidence to suggest that media stories may have taken on a life of their own, serving as inspiration for protesters who have decided to adopt the "Hong Kong protesters' playbook". The application recently continued to be promoted in Myanmar, where the military regime imposed internet shutdowns in an attempt to prevent dissent. While Bridgefy was not envisioned as a "protest app", its users have effectively made it into one, and so our work emphasises the need for analysing applications under the conditions they are used, and in the presence of the types of adversary they are likely to face. We would also like to draw attention to the problem space of designing secure mesh messaging protocols and tools, since it is clear that users only turned to Bridgefy because there were no alternatives. This is a pressing topic for future work. This will require clear understanding of the relevant security and privacy needs, in order to avoid another disconnect between what technologists design and what technology users require.

Away From the Cohort

Minerva task force wins cyber 9/12 strategy challenge

This year we participated in the Cyber 9/12 Strategy Challenge. The yearly event, which is normally hosted in the BT tower but was virtual this year, presents competitors with a fictional scenario that requires them to propose policy options to judges playing the role of the Prime Minister's office. The competition aims to provide participants with a better understanding of the technical, societal and strategic implications of cyber security and conflict. We represented the CDT under the team name of "Minerva Task Force". Given our multidisciplinary shared knowledge and that we were going to be taking part in a strategic challenge, we thought the name of the Roman goddess of wisdom and strategic warfare worked well. We are also an all-female team, and so the name of a Roman goddess seemed fitting.

Stephanie and Sofia had come across the competition in the past, and were keen to take part this year having heard great reviews from past participants. They asked the rest of the 2020 cohort to see who would be interested in joining, and were soon joined by Kyra and Emma. Between the four of us, we had a diverse range of knowledge. Initially we divided ourselves between non-technical and technical subjects, but by the end of the competition we were all contributing ideas to areas beyond our comfort zone. The final member of our team was our coach Nick. Having participated a few years ago in the competition himself, he provided us with great advice, insights and support throughout the challenge.

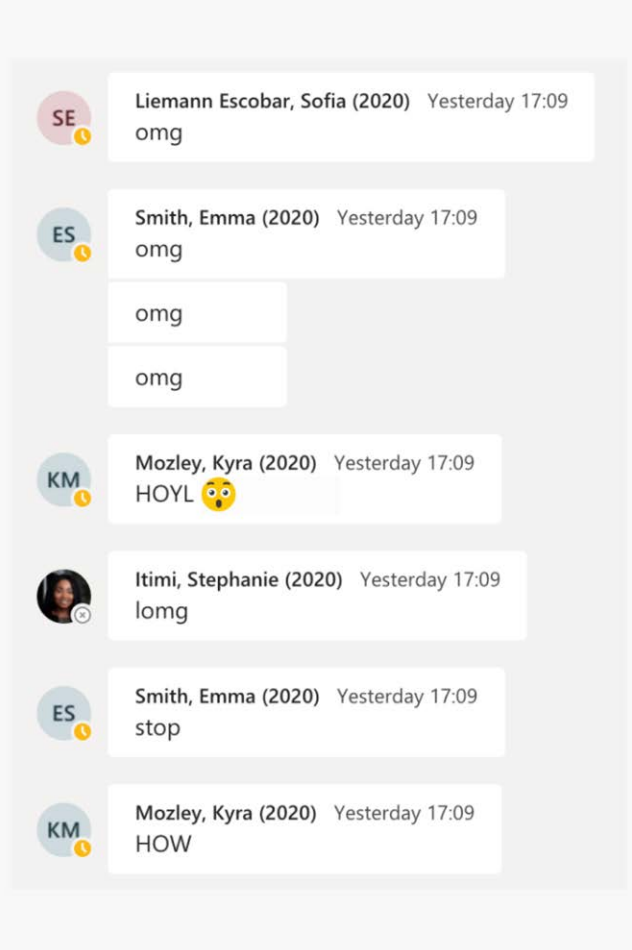
Keeping in theme with the pandemic, this year's fictional scenario centred around threats to intensive care unit oxygen systems, the vaccine supply chain, and disinformation on social media. The diversity of threats required us to conduct widespread research to identify who and what would be affected should the threats materialise. As there was not enough intelligence to assess which of the threats we would need to prioritise, in the first round we opted to create policy options aimed at preparing the country to try to mitigate the impact of some of the more harmful threats. Ultimately our aim was to ensure the pandemic recovery was not affected by the developing situation.

We were delighted to find out at the end of the first day of the competition that we had not only made it through to the semi-finals, but that we had also been awarded a prize for most creative policy response. We were therefore eager to receive the second intelligence pack and start working on the next briefing. After we all ate pancakes (it happened to be Shrove Tuesday), we set out to assess the developments in the scenario and start preparing policy options. It was a very long night (particularly for Kyra who decided not to go to sleep), but by 8a.m. the next morning we had a brief ready and were looking forward to presenting our policy options to the judges.

Although lacking sleep, the second round of presentations went well and we received some great feedback from the judges with one judge saying our team was a "powerhouse"! A couple of hours later the finalists were announced and we were excited to be chosen as one of the top three teams who would be proceeding to the final round.

The last round was very challenging as we had to process new intelligence and prepare a policy response, alongside a 10-minute oral brief, all in 20 minutes! We drew from our second policy brief to address the new developments we encountered. The preparation time went very quickly and we were straight into presenting for the judges. We were all nervous to be presenting in front of the other competitors and the questions we received were challenging. With such limited time to prepare, it was only natural that we were quite critical of our own performance. However, looking back, we now realise it was a great learning experience to have to think so quickly on our feet and be prepared to answer difficult questions.

Being announced winners of the competition was a genuine surprise! We frantically messaged each other in disbelief and excitement (see below). We were confident after our first two rounds and happy with our performance. But we felt much less confident after the last round (although Stephanie was convinced we would win all along). Perhaps it was Stephanie's optimism that saw us through that final briefing...



Away From the Cohort

Reaction to results announcement

Of course, we would have liked to have been able to meet all the other competitors and judges in person. But the virtual competition was still a great experience and we learnt a lot from taking part. Throughout the competition, professionals from around the world gave talks that really gave us an insight into different roles within cyber security. Each round required pooling our combined expertise from our wide range of backgrounds, which helped us understand both the complexity that policymakers face when solving cyber security issues and the need for multidisciplinarity. Presenting our policy responses to a team of experienced judges helped us build our briefing skills. Finally, the competition was a great way for us to get to know each other better as a team. We all had a lot of fun whilst preparing and having conversations both about cyber security and much more.

One of the biggest lessons we have learned is how to use our individual strengths in the cyber security sector. Our CDT training already instils the importance of multidisciplinarity in cybersecurity but participating in the competition made it even more visible. We also broadened our understanding of policy responses to cyber-attacks. The challenges set by the Cyber 9/12 competition reinforced the need for cooperation between private, public, and civil society when addressing everyday security threats.

We are now looking forward to attending the Black Hat Conference in November, and receiving our collection of cyber security books (both part of our prize). And since we didn't get to travel this time, you might see us competing next year in Geneva.

If anyone wants to take part in the competition next year, we would definitely encourage participation. A degree in computer science is not a prerequisite to enter the competition - as you can see from our backgrounds, some of us are non-technical. Take the step to enter, and we are sure that you'll learn a lot from the process, as we have done.

Sofia Liemann Escobar (War Studies & International Security), Stephanie Itimi (Economics), Kyra Mozley (Computer Science), & Emma Smith (Mathematics)

Nick Robinson – Coach, Team Minerva

Back in February this year, Royal Holloway and the CDT were once again well represented at the annual UK Cyber 9/12 Strategy Challenge, with our team *Minerva Task Force* (Emma Smith, Kyra Mozley, Sofia Liemann Escobar and Stephanie Itimi) producing a stunning performance to win the competition over two grueling, yet enjoyable, days.

Due to the ongoing Covid-19 pandemic, the competition was held remotely for the first time, and the team did a brilliant job of understanding and interpreting their tricky scenario (see above), whilst also communicating their astute policy proposals to esteemed cyber professionals, all from behind their own computer screens. As a team of first-year CDT students, remote working came naturally, but their collaborative efforts and stellar performance throughout the competition should be commended – particularly after many late nights spent together on Microsoft Teams!

During the competition itself, the team received some fantastic feedback from judges (including some very senior policymakers and security practitioners) and were frequently praised for their teamwork, presentation delivery and creativeness. One judge remarked that the team were "powerhouses", whilst another tweeted "Again, so good I fell into character and thought I was back in the Cabinet Room in No. 10!" - high praise indeed!

This, of course, is now the second time that Royal Holloway has won the competition after Team CDT (Amy Ertan, Angela Heeler, Georgia Crossland and Lydia Garms) won the inaugural UK Cyber 9/12 back in 2018. This is also now the second time an all-female RHUL CDT team has brought home the trophy – some feat, and long may that tradition continue in the future!

As coach (not that much 'coaching' was necessary), I just want to say a huge congratulations to the team on their success. You were a pleasure to work with, albeit from afar, and now preparations begin for the international edition, hopefully held on location in Geneva in 2022. Stay tuned!

CDT journeys

Blake Loring

For my PhD I focused on improving automated program analysis tools for JavaScript programs. JavaScript is the language of the web but has often been overlooked by program analysis researchers due to its dynamic program structure and confusing specification. To remedy this, we developed and open-sourced a new dynamic symbolic execution engine called ExpoSE (github.com/ExpoSEJS/ExpoSE), which is widely compatible with modern JavaScript and has state of the art support for strings and regular expressions.

While I was finishing up my thesis I was given the opportunity to move to Hong Kong, first working for a start-up that focused on machine learning for process automation and then moving on to work for ExpressVPN, one of the worlds largest VPN providers. While both of these roles are distant from the research I did during my PhD, I frequently use the knowledge and skills developed during my studies. This is particularly true in my role at ExpressVPN, where I work to improve the protocol design and performance of the VPN without compromising security or enabling censorship.

During my PhD I was able to do two internships, the first at Cloudflare, a major CDN provider, and the second at Brave, the developer of a privacy-focused browser by the same name. These internships were a great experience, furthering my practical skills and providing invaluable experience working with others that helped the transition from an academic lifestyle to industry.

Since finishing, I have even been able to do a small amount of research, contributing to the paper "Oblique: Accelerating Page Loads Using Symbolic Execution", which was presented at NSDI in April this year. I began working on this project with my co-authors in 2019, so I am thrilled that I could see it over the finish line.

My time in the CDT at Royal Holloway was enriching and set me up for a painless transition to industrial life afterwards. I cannot recommend the experience enough.

Andreas Haggman

I submitted my thesis in September 2018 and took up a role with a large firm in the insurance sector. On paper it was a great role: heading up a new function to identify areas where academic cyber security and geopolitics research could help the business. In practice, however, it was a largely frustrating experience as I did not have a budget (can't commission much research without a budget...) and I spent much of my time unsuccessfully trying to drum up interest (and money) within the company. Moreover, the culture of working in the City was not a great fit for me, so I left after a year.

During my time in the CDT I had been keenly interested in cyber policy and strategy, so a government role made a lot of sense. I joined the Department for Digital, Culture, Media and Sport (DCMS) in 2019, initially working on cyber skills policy. In addition to meaningful and rewarding work, it has certainly proved a fascinating time to be in government, with EU Exit, elections and COVID-19 providing their own challenges and opportunities. I have also pivoted my role to take better advantage of my background, and I now serve as an internal cyber security subject matter expert providing advice across our range of policies and programmes.

I can confidently say I would not be where I am today without the CDT. The PhD credentials have served me exceptionally well, but there is so much value to all the other components of the programme. Industry collaboration, teamwork projects, and conference participation all contribute to immersion into the cyber security community. The professional skills I developed in the CDT underpin any career success I can lay claim to, and I hope other students benefit in the same way.

Graduation

We would like to pass on our huge congratulations to the following CDT students who have submitted their theses and passed their vivas. Some of these students completed a while ago, but are yet to celebrate with a graduation ceremony since, for the second year in a row, these were cancelled at Royal Holloway. Others used their lockdowns wisely and managed to submit and complete their vivas during the pandemic over the last year.

We wish these students all the best in the next stage of their careers and look forward to celebrating alongside each of them at the next available opportunity.

Dr Ben Curtis, *Cryptanalysis and Applications of Lattice-based Encryption Schemes,* now a Research Assistant at the Alan Turing Institute.

Dr Alex Davidson, *Computing Functions Securely: Theory, Implementation and Cryptanalysis or, Topics in Insecurity,* now a Cryptography Engineer at Cloudflare.

Dr Amit Deo, *Variants of LWE: Attacks, Reductions, and a Construction.* Now a Postdoctoral Researcher at ENS Lyon.

Dr Lydia Garms, *Variants of Group Signatures and Their Applications,* now a Postdoctoral Researcher at IMDEA Software Institute.

Dr Torben Hansen, *Cryptographic Security of SSH Encryption Schemes,* now an Applied Scientist at Amazon Web Services.

Dr Elizabeth Lee, *Advancements in Proxy Re-Encryption: Defining Security for wider Applications,*now a Research Scientist at Cambridge Quantum Computing.

Dr Blake Loring, *Practical Dynamic Symbolic Execution for JavaScript,* now a Senior Systems Engineer at Network Guard.

Dr Jake Massimo, *An Analysis of Primality Resting and its Use in Cryptographic Applications,* now an Applied Scientist at Amazon Web Services.

Dr Dusan Repel, *Techniques for the Automation of the Heap Exploit Synthesis Pipeline.*

Dr Joanne Woodage, *Provable Security in the Real World: New Attacks and Analysis,* now a Researcher at Microsoft Research Cambridge.

CDT Research newsbites

- **Mesh Messaging in Large-scale Protests:** Breaking Bridgefy - Martin R. Albrecht; Jorge Blasco; Rikke Bjerg Jensen; Lenka Mareková Paper accepted at CT-RSA and presented at RWC.
- **Improved privacy-preserving training using fixed-Hessian minimisation.** Tabitha Ogilvie, Rachel Player and Joe Rowell. Paper accepted at WAHC 2020.
- **Estimating Quantum Speedups for Lattice Sieves** Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, John M. Schanck Paper accepted and presented at ASIACRYPT 2020.
- **Remote Working and Cyber Security.** Literature review white paper by Georgia Crossland, (co-authored by Amy Ertan and Nadine Michaelides) published on RISCS, www.riscs.org.uk/wp-content/uploads/2021/02/LitReviewV2.pdf.
- **Policy Paper on UK Offensive Cyber now out.** Amy Ertan is a co-author on a recent King's Policy Institute Report titled: *The National Cyber Force that Britain Needs?* Written with Tim Stevens (KCL), Joe Devanny (KCL) and Andrew Dwyer (Durham University), the report reflects on the UK's approach to offensive cyber activity. www.kcl.ac.uk/policy-institute/research-analysis/national-cyber-force.
- **Amy Ertan** presented at the NATO Side Event Cyber Pledge Conference 2021 alongside Dr Max Smeets and Dr Brandon Valeriano on the topic of NATO and offensive cyber. Write-up ccdcoe.org/news/2021/highlights-from-the-public-side-event-of-the-nato-cyber-pledge-conference-2021/ and recording www.youtube.com/watch?v=gocp2QYCJ3c.

8408 05/21

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