@RHULCyberCDT rhulcybercdt.blogspot.com YouTube

CDT Newsletter

ROYAL HOLLOWAY UNIVERSITY OF LONDON

EPSRC Centre for Doctoral Training in Cyber Security

March 2022

CDT update

Director Report

It's pertinent that our CDT is named Cyber Security for the Everyday since it's that very notion of `everyday' that has changed so much over the period since this iteration of the CDT commenced in September 2019. Just like everyone else, researchers are getting used to a hybrid world of home working, occasional office visits and meetings where some people are in a room and others are on a screen. I suspect elements of that are not going to go away anytime soon.

One aspect of research that has dramatically changed is travel. Our CDT has a generous travel allowance and prior to the pandemic our PhD researchers were considerably on the move, attending workshops, conferences and visits all around the world. This can be an invigorating experience for those on a PhD research apprenticeship, with such events providing opportunities to build personal networks and reputation. So, too, for many fully-fledged academics. Some of my colleagues seemed to be living in airports, less often home than away – always on the move, exchanging ideas, dining on different cuisines...

I have to confess that for a while prior to the pandemic I had been getting increasingly concerned about this wandering lifestyle. It struck me that so much academic travel was unnecessary. It had become a habit rather than a need. In an age where information is so digitally accessible, was it really necessary for an international research roadshow to be in place? Don't get me wrong - I do think it is good to travel and to meet people. But I think far too much of it was going on.

Well – that's certainly changed! The pandemic has shaken research travel culture to the core. It's never been easier and cheaper to attend an international conference in the new world of online delivery. In this sense, our PhD researchers have never had it so good. However, I also believe that they are missing out, particularly on international network building – it's hard to do that online. What I fervently hope is that a saner academic research culture will emerge, with more selective and valuable opportunities to travel, rather than the mass movements of the past.

With this in mind, I was particularly pleased to learn that three CDT researchers were among the winning entries in Royal Holloway's internal COP26 competition inviting students to submit a creative response to climate change and related issues of sustainability. Students were asked to consider climate change and the impact that it is having, and will have, both in terms of the global context and at a more local level. Oliver, Cherry and Rebecca all submitted extremely thoughtful responses. It pleased me to see a new generation of researchers in training who may help to develop a more responsible research culture. But it also delighted me to see how the CDT, which is not focused on an area directly targeting climate change, supports researchers who are so creatively able to voice their opinions on issues beyond their core area of study. This is exactly the breadth and maturity that we hope for from our CDT researchers.

Another event which didn't happen in the manner of the past was what was previously termed our annual CDT Showcase. Before the pandemic, we held an outward-facing event where the CDT research was presented to external stakeholders. In November, partly due to pandemic restrictions and partly due to a need to reconnect with ourselves, we held an internal residential event just for members of the CDT. It was a wonderful two days and a reminder of everything good that is happening – without the need for anyone to get on a plane!

Of course, we do still want to share what we are doing with everyone. I thoroughly recommend checking our CDT Blog, which contains a range of short articles about what's been going on, internship reports, links to publications, as well as a chance to see Oliver, Cherry and Rebecca's winning entries in the COP26 Competition.

Professor Keith Martin

Inside the cohort

Charlotte Hargreaves

Just a few months ago I was at the beginning of my doctoral research journey. Four years can seem like a daunting task but within my first week as part of the CDT at Royal Holloway, I felt reassured that I was best placed to achieve my goals. I feel so lucky to have had the opportunities to meet some of the best academics in the cybersecurity field. I have also thoroughly enjoyed meeting my fellow CDT cohort and I have learnt a lot already from some of the older CDT students.

It has been exciting to learn of, and experience, the inter-disciplinary nature of the course. I originate from the field of Psychology but I am thrilled to have the opportunity to take on new areas of study and new perspectives surrounding security. Within the short time I have been here, I have had many interesting perspectives provided to me from my peers, lecturers, and independent study.

The first year of the CDT involves taught modules from the Information Security MSc at Royal Holloway. It has been great to engage with the modules and the challenges that come from learning a new field. I believe everyone has enjoyed the breadth and depth of the different topics. My cohort have been busy lately with comprising a report and presentation on the prospective features to be implemented by Apple on reducing CSAM. As a group we have coordinated the mixture of backgrounds well and delivered a successful combination of technical and social elements for discussion.

Moving forward, I am really looking forward to engaging more with the course and discovering new areas of research within cybersecurity, particularly through my summer project. Furthermore, the prospect of developing a thesis based on a culmination of these new ideas feels like a unique and privileged chance to work within such a rapidly growing, important field.

Purple Visits... Could do better

Natasha Rhoden

"This article was first published in the August 2021 issue of Inside Time, the UK's National Newspaper for Prisoners and Detainees"

Since the start of the pandemic, purple visits has operated the video calling service at prisons in England and Wales - but in the summer it was announced that a different provider, Phonehub will take over. Here, Natasha Rhoden describes some of the problems users had with the purple visits service.

This past year of Covid-19 lockdowns has spawned new ways to stay in touch with loved ones across the country. It is possible that video calls for prisoners and families introduced in response to the lockdowns may be here to stay. However, to ensure that video calling meets the needs of prisoners and their families, their views on the service will be crucial.

I wanted to understand more about how prisoners and their families experienced this change from face-to-face visits to video calls, and how this experience might be improved. My end goal was to start conversations around how technology for prisoners in England and Wales might help them to build, or maintain, social ties with the people they care about.

Here are the key points I found about video calls:

- Prisoners' family members noted that the security within the video calls often interrupted and disconnected their video calls to prisoners.
- Family members felt that slight movements at their end of the video call usually led to the call being disconnected, and believed this was a security measure.
- People from organisations and charities which support prisoners suggested that prisoners will want any kind of technology which helps them to have private conversations with their family.

Some families who had used video calls to stay in touch with loved ones in prison were using social media like Twitter to ask questions of the prison service and share their own thoughts about video calls.

I searched the comments sent by people in prisons to *Inside Time* newspaper, and found further comments online including on Twitter and YouTube. I read reports on the Internet which outlined the views

Purple Visits... Could do better

of politicians, prison governors, prison-focussed charities and research studies on technology for prisoners. I used this information to find out what people were saying about their experience of using mobile phones and tablets to facilitate video calls from prisons, and the most effective ways for prisoners to keep in touch with their families. I also spoke with people in leadership roles at charities which support prisoners and prisoners' families, journalists reporting in the interests of prisoners and organisations supplying the software and online services for prisons, to gain as many different perspectives from those involved in technology for prisoners as possible.

The research narrowed in on a few key questions about technology for prisoners:

- How did the Covid-19 lockdowns change the ways that prisoners and their families experienced technology?
- What was the feedback on the internet and in prisoner's letters to *Inside Time* about having the use of technology to communicate with family?
- What had prisoners and their families discovered about the best ways to use technology to stay in contact with each other?

The comments and criticisms included in this research referred specifically to video calls to prisons in England and Wales and the Purple Visits service between April and July 2020.

Overall, family members who discussed this issue online seemed to feel that the security used as part of prison video calls could be disruptive at times. For example, comments suggested that the security technology within the video calls frequently disrupted their video calls with prisoners by disconnecting the call. Feedback from families implied that the security of video calls worked by repeatedly comparing the live picture of the prison 'visitor' (which was being generated by the camera on their phone or tablet during the video call), against the photo ID the 'visitor' would have registered to get permission to use the video call service. Feedback from family members online suggested that the security technology used within the video calls appeared to automatically disconnect video calls whenever family members shifted or moved during the video calls. It was felt that this movement might have prevented the security technology within video calls from repeatedly checking that the 'visitor's' live face image was the same as their photo ID image.

Calls dropped because of people moving around meant that it was often not possible to complete meaningful conversations within the prearranged time slots. The video calls were described as "unusable" and "bungled" by some users, because the security of the video call service was so sensitive that even the slightest movements on camera could trigger their call to a prisoner being dropped.

Dropped calls may have been especially distressing for prisoners' children, because family members would have to repeatedly try to re-connect calls within the time limit for their arranged call session. One parent left feedback on the Google Play review website about the video call service being "overbearing" and preventing a prisoner's three-year old daughter from seeing her father on camera: "The face recognition is so sensitive the slightest movement... re-authorities (sic) your picture so spend best part of the 14 mins... doing this [...] Considering this is recorded and monitored by the prison [why] does it need to be so over bearing (sic)... If it wasn't for the fact I had a 3 yr-old wanting to see her dad I wouldn't bother..."

In addition, families suggested that the repeated disconnections of video calls also prevented them from having private conversations with their loved ones.

Another review on the Google Play store said: "...too invasive and couldn't get verified but also now will not remove my information for 6 years... I'd rather not try an[d] see my friend in prison than be made to feel like a prisoner myself."

A key concern noted in government reports and from the perspective of companies supplying technology for prisons in England and Wales was that non-authorised individuals may attempt to use the video calls system to contact prisoners. Those who were interviewed as part of this research felt that this might be the motivation behind the stringent security used as part of the video calls. However, most of the charity executives and academics who were interviewed felt that communication with families was the main benefit which was driving the demand for technology within prisons. It was suggested that any form of technology which gave prisoners a chance to speak freely about their experiences with family members, or have meaningful catch-up time with children, would be sought after and welcomed by prisoners and their family.

I will be continuing this research by discussing these problems with families and the charities that support prisoners and families. I would like to ask readers with thoughts on this topic to please write to *Inside Time* and share your stories and thoughts on technology for prisoners, and how technology might be adapted to improve the experience of video calls between prisoners and families.

Inside the cohort

PhD research and write-up during COVID-19

Georgia Crossland

In this short piece I will discuss my PhD journey during COVID-19, highlighting some of the issues I faced, how I overcame these and providing recommendations to help others in the same position. Of course, first and foremost, the COVID-19 crisis is a global health crisis, and people have been put in much worse situations than their PhD research being delayed. I was fortunate that the EPSRC granted me an extension for my research, a great benefit that was not extended to many other PhD students from different disciplines. However, social distancing has been essential to minimise the spread of COVID and for many researchers this represented, and still does, a change in fieldwork methods, write-up strategy, as well as changing the way we interact with our cohort and supervisors.

1. Field work

When we went into the first lockdown in March 2020, I had just found an organisation (a global law firm) willing to let me conduct my research with their employees. The plan was to spend a few days a week for a few months at their different office sites around the UK.

This plan was swiftly thwarted. After a lot of **panic**, and with help from my supervisor, I came up with a new plan to get the research done. The solution was to do online interviews and focus groups. I was initially worried about this , especially with how online methods might impact my ability to build rapport with participants. So, I started Google Scholaring (a new term for PhD students that replaces googling) the efficaciousness of such techniques.

I discovered online interviewing to be a widely used method, backed up by breadth of research evidence demonstrating its effectiveness, and I found such research evidence helpful to read through to both gain technique and confidence in the method. Moreover, there were a few research papers suggesting a number of ways researchers can build rapport with participants online. One of the main factors that fostered rapport in one study was good quality video. There are also some potential benefits of online interviews. One paper has suggested that participants can feel an increased sense of ease online, as the physical absence of the researcher reduces the risk of exposure or embarrassment. Others highlight the opportunity presented for a geographical spread of participants in a timely and affordable way.

For further advice and resources on interviews and focus groups, and other social research methods, there is an extremely useful crowd sourced document, initiated by Prof. Deborah Lupton, available online. This document provides many papers and resources for social researchers and I have found it extremely useful, link here.

However, the research was still heavily delayed, and I did not start the field work until July 2020, finishing in October 2020.

2. Supervision

Throughout the past few years, I have also felt increasingly isolated, especially from my supervisor and cohort. I found it difficult to manage my workload, understand what was expected of me, and to take ownership of my project. Especially when my interviews and focus groups were constantly being rescheduled due to issues relating to remote working, returning to the office, and other pandemic related matters.

To work through these issues, I made sure to schedule regular calls with my PhD supervisor and began to set myself manageable deadlines and goals. It is often hard to manage your own progress expectations within a PhD, especially during the confusion of a pandemic and when you compare yourself to other PhD students not doing field work. However, when I spoke to my supervisor, I was reassured that the small steps I was making still counted as progress and that certain tasks do often just take time. My supervisor also made sure I felt I was able to reach out to them with any issue, big or small, which greatly helped me feel able to ask for help when I needed it.

When my own research was slowed by issues outside of my control, I also got involved in other projects, such as research outside of the PhD, internships, writing papers with my supervisor and helping others with aspects of their work. The 3-month internship I completed at Meta was extremely helpful for me, giving me a break from, and perspective on, my thesis. One of the projects I am most proud of during this time, is a piece of research I did with colleague Amy Ertan for the Research Institute for Sociotechnical Cyber Security, entitled Remote Working and (In)Security. This helped me remember that a PhD is not all about your thesis, but everything that you are able to experience during these years.

I was also able to apply for an extension during this time and was awarded one by the EPSRC. This was very much a saving grace for me, without this, I would not be completing my PhD within my funded deadline. I am very grateful to my supervisor and the CDT who supported me throughout this application process.

PhD research and write-up during COVID-19

3. Write-up

From November 2020 to present, I conducted the analysis of my findings, and am now in the final stages of my thesis write-up. Despite the fact we are now coming out of the pandemic, or now the UK is reducing restriction pertaining to the pandemic, I have found this time to be the most challenging. Writing up and editing your thesis is very gruelling, and probably the loneliest time of the PhD journey (or at least, this has been my experience). It is hard to know where to start, and what tasks to complete when, and I often found myself jumping between writing sections, feeling as though I had completed none of them. Although campus is now open, it still might not feel safe to everyone to be travelling every day if it is not totally necessary. I have found myself doing almost all my write-up therefore by myself in my flat, or in nearby libraries. One of my colleagues wrote a blog about looking after your mental health while working remotely, so for more on this read here.

To combat this, I set up many writing sessions and bootcamps with a few other members of my cohort to foster mutual write-up support. During these sessions we would use The Pomodoro Technique for writing, chatting between ourselves during the allotted breaks. I am not sure I would have a completed the first draft now if it was not for these meetings. They helped engender a feeling of solidarity and support, both academic and emotional, and I would highly recommend this to anyone in the final stages of their PhD.

Some advice!

a. Your PhD will not always turn out the way you planned, and this is okay!

My PhD took many unexpected twists, for example, it now includes research regarding cyber security during the pandemic; something I could never have anticipated. However, this has allowed me to contribute and add value to other research areas. Your PhD is meant to be informed by your PhD journey, embrace changes, and lean on those around you.

b. Work with your supervisor

Your supervisor wants to support you, but they might not always know how best they can do this. It is important to have an open conversation about how often, when and where you need support.

c. Manage expectations of yourself

Set yourself realistic goals, and work on these with your supervisor, so you are on the same page about what is expected of you.

d. Celebrate small achievements

Make sure to enjoy the little things and do something fun when you do. After I finished my methods chapter, I took a day (or two) off to celebrate and recover. These small things help your wellbeing during this process. When writing up, The Pomodoro Technique is your friend, celebrate 25 minutes of writing with a 5-minute break!

e. Get involved!

Some of the best experiences I had during my PhD were not directly linked to my thesis. Go to conferences, collaborate on papers, take on internships or consultancy work and get involved in competitions. This will all benefit your PhD experience, and you might find these experiences help your thesis and future career post-PhD.

But… also know when to say no, don’t feel pressured to do something you don’t want to do.

f. Help others

All PhD students will struggle at some point, whether someone needs your expert knowledge on a topic or someone to sense-check their paper, it is always good to get involved. Not only are you helping that person and adding value to research, but you might also need help at some point, and it is good to have people you can rely on.

Cyber 9/12 strategy challenge special

The Cyber 9/12 competition provides an opportunity for mixed-discipline teams to demonstrate their understanding of technology, policy, strategy, law, international relations, and national and organisational cyber incident response, through a challenging but realistic scenario.

This year's plot line evolved around a climate activist group seeking to use cyberspace for activism. The event this year was delivered as a virtual event on 15th and 16th February, and students from our CDT participated in all forms. We had a team of first-year students who entered the competition as team Polymath. We had a second year student coaching a team of Information Security Group MSc students, and a third year student who was invited to be one of the judges for this annual competition.

Below we hear from them with their perspective of this competition.

Team Polymath

In mid-February of this year, our team (First year CDT students, Rebecca Hartley, Alex Hodder-Williams, Sasha Lapiha, and Taylor Robinson) participated in the Cyber 9/12 strategy challenge. Our team was coached by former Cyber 9/12 participant and coach Nick Robinson and received additional valuable assistance from Ian Slesinger. The annual event, which was virtual this year, requires competitors to propose policy options to a panel of judges (acting as if they are from the Prime Minister's offices) responding to a fictional scenario involving a cyber threat. The competition aims to provide participants with an understanding of the technical, social, political, and economic impacts of cyber security events.

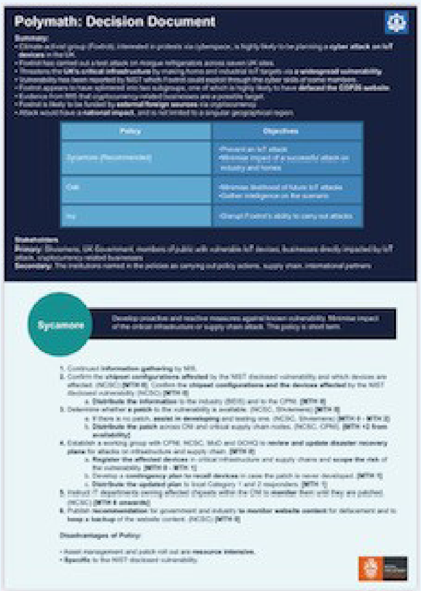
Our team entered under the name "Polymath" which we wanted to reflect the multidisciplinary backgrounds of our members, representing many disciplines ranging from maths, computer science, international relations, and business.

This year's fictional scenario evolved around a climate activist group seeking to use cyberspace for activism. To do this, they found and exposed a vulnerability in an IoT chipset, which would allow them to shut down an unknown amount of industrial and home IoT devices. During the first round, the group carried out a test attack on morgue fridges at seven different sites across the UK. In the two weeks leading up to the competition, our role was to develop policies to anticipate and respond to the future escalation of the group's actions and any effects it may have on global supply chains.

After successfully making it into the second round of the competition, our team was provided with the second intelligence packet that informed us that the activist group successfully attacked chips in industrial air conditioning units in a "Whamazon" data centre located in the UK. These actions produced a cascading effect on related businesses, disrupting supply chains and simultaneously causing a variety of public responses on social media. Our team worked overnight to develop three more policies that responded to other potential attacks and threats to the supply chain. After approximately 2.5 hours of sleep, we successfully presented our policy decisions to the second panel of judges. Unfortunately, despite positive feedback, we did not make it into the final round of the competition.

Although we did not make it into the final round, we collectively found the competition a positive experience - especially from a team-building and research perspective.

As a team, we learnt greatly from each other's expertise. There were many instances that we disagreed on how to respond to certain information provided in the intelligence briefings. Our different interpretations made our team stronger and allowed us to think about the scenario more thoroughly. Real-world policymakers work with various sectors and disciplines daily, so having a multidisciplinary team allowed us to experience the benefits and challenges that policymakers face. This further established the essential need for public, private, and global collaboration to overcome cyber threats. Additionally, the time-pressured environment was a fulfilling experience. We were able to get a taste of how policymakers have to cope under pressure during an emergency.



Polymath: Decision Document

Summary:

- [illegible] **cyber attack on IoT devices** in the UK.
- Foxtrot has carried out a test attack on morgue refrigerators across seven UK sites.
- Threatens the **UK's critical infrastructure** by [illegible] **vulnerability**.
- Vulnerability has been reported by NIST which Foxtrot could exploit through the [illegible]
- Foxtrot appears to have [illegible] **defaced the COP26 website**.
- [illegible]
- Foxtrot is likely to be funded by **external foreign sources** via cryptocurrency.
- Attack would have a **national impact**, and is not limited to a singular geographical region.

Policy	Objectives
Sycamore (Recommended)	•Prevent an IoT attack •Minimise impact of a successful attack on industry and homes
Oak	•Minimise likelihood of future IoT attacks •Gather intelligence on the scenario
Ivy	•Disrupt Foxtrot's ability to carry out attacks

Stakeholders:

Primary: [illegible], UK Government, members of public with vulnerable IoT devices, businesses directly impacted by IoT attack, cryptocurrency related businesses

Secondary: The institutions named in the policies as carrying out policy actions, supply chain, international partners

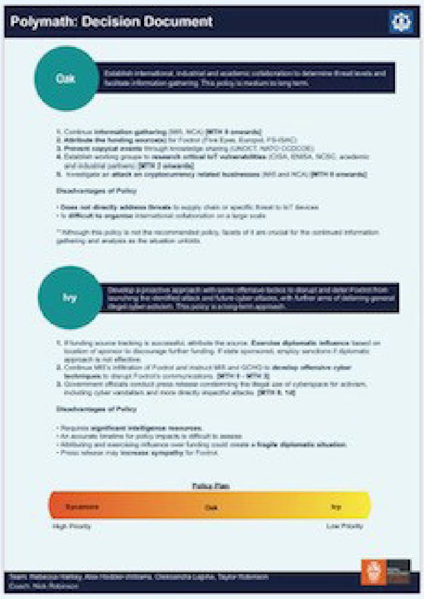
Sycamore

Develop proactive and reactive measures against known vulnerability. Minimise impact of the critical infrastructure or supply chain attack. This policy is short term.

1. Continued **information gathering** by MI5.
2. Confirm the **chipset configurations affected** by the NIST disclosed vulnerability and which devices are affected. (NCSC) **[WTH 0]**. Confirm the **chipset configurations and the devices affected** by the NIST disclosed vulnerability. (NCSC) **[WTH 0]**
   a. **Distribute the information** to the industry (BEIS) and to the CPNI. **[WTH 0]**
3. Determine whether **a patch** to the vulnerability is available. (NCSC, [illegible]) **[WTH 0]**
   a. If there is no patch, **assist in developing** and testing one. (NCSC, [illegible]) **[WTH 0 - WTH 2]**
   b. **Distribute the patch** across CNI and critical supply chain nodes. (NCSC, CPNI) **[WTH +2 from availability]**
4. Establish a working group with CPNI, NCSC, MoD and DCMS to **review and update disaster recovery plans** for attacks on infrastructure and supply chain. **[WTH 0]**
   a. **Register the affected devices** in critical infrastructure and supply chains and scope the risk of the vulnerability. **[WTH 0 - WTH 1]**
   b. Develop a **contingency plan to recall devices** in case the patch is never developed. **[WTH 1]**
   c. **Distribute the updated plan** to local Category 1 and 2 responders. **[WTH 1]**
5. Instruct IT departments owning affected chipsets within the CNI to **monitor** them until they are patched. (NCSC) **[WTH 0 onwards]**
6. Publish **recommendation** for government and industry **to monitor website content** for defacement and to **keep a backup** of the website content. (NCSC) **[WTH 0]**

Disadvantages of Policy:

- Asset management and patch roll out are **resource intensive**.
- **Specific** to the NIST disclosed vulnerability.



Polymath: Decision Document

Oak

Establish international, industrial and academic collaboration to determine threat levels and facilitate information gathering. This policy is medium to long term.

1. Continue **information gathering** (MI5, NCA) **[WTH 0 onwards]**
2. **Attribute the funding source(s)** for Foxtrot (Five Eyes, Europol, FS-ISAC)
3. **Prevent copycat events** through knowledge sharing (UNOCT, NATO CCDCOE)
4. Establish working groups to **research critical IoT vulnerabilities** (CISA, ENISA, NCSC, academic and industrial partners) **[WTH 2 onwards]**
5. Investigate an **attack on cryptocurrency related businesses** (MI5 and NCA) **[WTH 0 onwards]**

Disadvantages of Policy

- **Does not directly address threats** to supply chain or specific threat to IoT devices
- Is **difficult to organise** international collaboration on a large scale

**Although this policy is not the recommended policy, facets of it are crucial for the continued information gathering and analysis as the situation unfolds.

Ivy

Develop a proactive approach with some offensive tactics to disrupt and deter Foxtrot from launching the identified attack and future cyber attacks, with further aims of deterring general illegal cyber activism. This policy is a long term approach.

1. If funding source tracking is successful, attribute the source. **Exercise diplomatic influence** based on location of sponsor to discourage further funding. If state sponsored, employ sanctions if diplomatic approach is not effective.
2. Continue MI5's infiltration of Foxtrot and instruct MI6 and GCHQ to **develop offensive cyber techniques** to disrupt Foxtrot's communications. **[WTH 1 - WTH 3]**
3. Government officials conduct press release condemning the illegal use of cyberspace for activism, including cyber vandalism and more directly impactful attacks. **[WTH 0, 14]**

Disadvantages of Policy

- Requires **significant intelligence resources**.
- An accurate timeline for policy impacts is difficult to assess.
- Attributing and exercising influence over funding could create a **fragile diplomatic situation**.
- Press release may **increase sympathy** for Foxtrot.

Policy Plan

Team: Rebecca Hartley, Alex Hodder-Williams, Oleksandra Lapiha, Taylor Robinson
Coach: Nick Robinson

Finally, during our preparation for both rounds we learnt about how current preparation and research is being conducted on the potential for a real life incident similar to Cyber 9/12.

Overall, we enjoyed the teamwork and simulated scenario of Cyber 9/12 and encourage future teams to get in touch for more information.

Kyra Mozley – coach

This year I had the pleasure of coaching team Cyber Royale, a group of four master's students (Zeinab Mohammed, Emna Haddouk, Prateek Ashok Kumar, and Ashwini Sridhar) for the Cyber 9/12 strategy challenge. After participating in the competition myself last year, it was fascinating to see it from another perspective. Not only did the team impress me with their performance and growth throughout, but they clearly impressed the judges as they made it to the final and took the third-place trophy.

Back in December, the group were eagerly trying to find someone to coach them, but following their lack of success finding staff members who could coach them, they approached me on the day of the application deadline asking if I'd be willing. Despite being part of the winning team last year, as I'm only a 2nd year PhD student whose research area has nothing to do with cyber policy, I felt highly unqualified to be their coach. However, since I knew how valuable an experience the event is, I did not want them to miss out - so I stepped up and agreed to coach them.

Coaching is a very different experience from being part of the team. For example, after reading the scenario pack, I had my own ideas about the threats and policies the UK should propose. However, it was essential that I kept these to myself and let them present what they came up with. So, instead of directly suggesting what I thought, I decided it was best to ask them questions such as 'why do you believe that' or 'what will this policy achieve' constantly, meaning they could justify their recommended policies perfectly.

Another critical task of being a coach, alongside making sure the team works well together, is to provide encouragement and support. Therefore, in times of stress, to keep their spirits up, I'd share memes I had made about the competition, resulting in a bit of laughter and a boost in motivation.

I was super proud of my team throughout the two days as they consistently got great feedback, particularly on their teamwork and how professionally they presented themselves - all while having had no sleep since they worked on the semi-finals all through the night. The excitement each time they progressed through to the next round was immense; apparently, their whole accommodation block could hear the team's scream of cheer!

It was such a rewarding experience, and I highly recommend it to anyone. You don't necessarily have to come from a policy background or have been a coach before. All that matters is enthusiasm and the ability to keep asking 'why' till they're sick of you.

So a big congratulations to team Cyber Royale, and I'm very much looking forward to joining them at the winners' reception at the BT tower later this year.

Nicola Bates – judge

Now in its fifth year the UK Cyber 9/12 Strategy Challenge is an amazing way for university students to experience how policy and strategy concerns come together when dealing with complex cyber issues. Within the competition teams analyse the threats and risks posed by a fictitious but realistic cyber attack scenario and then propose effective mitigating actions before briefing judges.

The competition is designed to mimic real-life with new events and information (sometimes conflicting) being released as the rounds progress. This encourages the participants to focus upon prioritisation and pragmatic recommendations which they must explain clearly and concisely (within a strict 10 minutes) to convince the judges what they should do next. After this they then spend a further 10 minutes answering questions from a panel of judges who will delve deeper into the proposed recommendations!

This was the second year in a row that the competition took place online. Whilst it's a shame we weren't back in BT Tower the organisers didn't let it dampen the excitement and took advantage of the virtual nature pulling in a wealth of high-quality speakers from across the UK and internationally. Fourteen 'day in the life' talks were hosted covering a wide variety of careers for cyber security professionals along with other beneficial training activities including: mentoring sessions, a careers fair, recruitment and interview sessions, CV workshops and three in depth area focussed workshops. And keynote speeches from BT, NATO, GCHQ, Beasley and the Cabinet Office interspersed throughout the two days held everyone's interest providing insights across the cyber landscape.

A new addition this year was also a 'working in and with neuro diverse teams' discussion panel. This explored some of the challenges for neurodiverse individuals (with a focus on autism) working as part of a team or in an office environment. The three panellists discussed their experiences of being diagnosed as autistic later in life and the challenges they faced. The aim of the panel was not only to raise awareness of these trials but also share good strategies to enable individuals to reach their full potential - whether as an autistic individual or in support of colleagues.

Cyber 9/12 strategy challenge special

It was fascinating to hear the speakers' experiences and the ways they found to manage different aspects of the workplace and cyber sector in a way everyone – both neurodiverse and neurotypical - could relate to and take learnings from.

This years' fictitious scenario involved a climate change activist group seeking to shut down industrial and home IoT devices. This was my second year of being a judge and as last year the standard of entries was very high; the teams had clearly given each aspect of the initial scenario a lot of thought, teasing out relevant insight and linking back to practical policy solutions and actions they could take – and where they should hold back, monitor the situation and not over-react!

As the rounds advanced new information came to light suggesting the attacks were intended to have a cascading effect on related businesses. It was encouraging to see how quickly new ideas were formed, old plans adapted, and new ones made – all calmly and concisely presented back.

The uniqueness of Cyber 9 / 12 is that it seeks to build the next generation of cyber security leaders who can competently blend strategy, policy and technological thinking and understanding to provide strategic level advice and thinking. It really is a great event to get involved in and I would encourage others to take part whether as a competitor, coach, judge or being on the organising committee.

A big thank you to Rob Black for inviting me back to be on the judging panels again this year and for putting together such an amazing event.

Cumberland Lodge event

The CDT recently hosted a hybrid engagement event at Cumberland Lodge in Winsor Great Park. This was an exciting event for us to host as it provided an opportunity for us to bring together students from across the cohorts (many meeting for the first time), to reconnect students and staff, and for everybody to share what they've been up to.

We had great attendance at this event with many staff and students choosing to join us in-person (following covid measures), and others joining in online. There was a packed programme, full of student talks to update us on their research, some interesting presentations from students who have recently returned from internships, and some engaging sessions from some of our recent graduates in which they delivered an inspiring message and words of wisdom to those who are just at the beginning of their CDT journey.

Below we hear from Professor Chris Mitchell, Head of Information Security Group at Royal Holloway with his thoughts on the event.

I had the great privilege to attend and participate in the CDT showcase event on 25th and 26th November 2021, held at Cumberland Lodge, Windsor. This was a particularly welcome occasion, as it had not been possible to hold a corresponding event in 2020 because of the Covid-19 pandemic. It was well-attended by both CDT students and academic staff;

I would estimate that at least 50 people were present during the two days. In additional, a number of current and former CDT students attended online, e.g. from where they were engaged in internships.

This was the first time that many of the CDT students had been able to present their research in person to a large audience because of Covid-19, and a large number of informative and entertaining presentations were packed into the two days. Of particular note was an impressive team presentation by the newest cohort of students on a group project they have performed involving a technical, ethical and privacy-related analysis of a novel Apple scheme to try to detect and mitigate the use of iCloud for storage and sharing of illicit child-related images. More generally, the presentations were lively and provoked more questions than could be fitted into the time available. The CDT clearly remains able to recruit widely varied cohorts of extremely talented people, and is able to stimulate their research interests in many different ways.

Cumberland Lodge, as always, looked after us all extremely well; thanks to excellent organisation of the event by the CDT team, we even managed to squeeze a brisk organised walk in the park between sessions – indeed, it needed to be brisk, as although it was sunny it was also bitterly cold. I certainly greatly enjoyed the entire two days, which I found both educational and entertaining, and I hope to be invited back for the next showcase event.

Return from Internships

The CDT in Cyber Security for the everyday encourages students to complete an industry or academic internship during the course of their 4-year PhD. These placements can either involve a study break, known as an interruption, in which the student is paid by the provider of the internship, or no study break, where the student remains financially supported by the CDT. Students on paid placements offer the opportunity to branch out and explore other topics, whist activities for 'uninterrupted' students on internship must align with the student's research.

If you would like to find out more about hosting a student on internship, please get in touch.

Below we hear from some students who have recently returned from internship.

Georgia Crossland: Facebook. June-September 2021

In the summer of 2021, I completed an internship as a qualitative user experience (UX) researcher at Facebook on the Advertising Business Products team. Despite the internship being remote, I fully enjoyed the experience and came away from it feeling prepared for post-PhD life.

UX research refers to the practice of studying user interactions with technology, to assist with the design of human-centred products and experiences. UX researchers use a range of methods to do this, such as usability testing, interviews, ethnography, surveys, diary studies and more. While, quantitative and mixed methods researchers also work in this field, my UX research experience at Facebook was qualitative. UX researchers at Facebook work with product teams to apply their learnings from different studies to help manage design on their products as well as push boundaries in new immersive technologies. Interns are treated as full-time employees and are given many responsibilities – which engenders a feeling of accomplishment!

My projects included research with small to medium sized businesses, conducting usability testing and interviews, as well as writing reports for a privacy focussed workstream. Not only was I able to experience what it's like to work in a large organisation and learn new skills, I felt I was able to apply the knowledge gained from my PhD to the job at hand - largely that relating to usable cyber security and psychology. I greatly enjoyed the work I did here and accepted a returning full-time offer. The possibility of a returning offer is another advantage of an internship at Facebook or many other large tech firms.

In addition to the research, I had the benefit of working within a great team, and alongside other UX research interns, who were also in the process of completing PhDs. This has given me an extra support network beyond that of the 3-month internship. I further found it encouraging to intern in an organisational culture that encouraged dialogue and debate about the company's products and policies.

I am very grateful to the CDT for allowing me this opportunity. Studying within a doctoral programme that actively encourages internships in industry, to equip students with a mindset to tackle issues outside of academia, significantly improved my PhD experience.

Jodie Knapp: Thales: July – October 2021

I commenced a three-month internship with Thales UK from July to October 2021 and have come away from the experience with a positive outlook post-PhD. I have spent my time in the CDT enjoying research, however, I was keen to experience research in a business context with more emphasis on designing practical protocols.

The internship saw me working on a specific project within the very welcoming and supportive cryptographic research team. I highly enjoyed interacting with different people in the business, working in a group and polishing skills such as programming. Further, I developed my speaking skills and gained confidence voicing my opinions and contributing to the project. Whilst I was only able to attend my internship in person a couple of days out of the working week, the balance of home versus office work was not an issue as I had as much support at home as I did in person.

Upon returning to my research I found I had renewed motivation to keep up with the pace of working at Thales and structure my working days in an efficient, productive way. Completing an internship outside of my area and comfort zone has been productive and beneficial to my PhD and thoughts towards a future career.

Robert Markiewicz: F-Secure. June - September 2021

F-Secure is a global company with a rich history in the field of information security and anti-virus (AV, developing the first heuristic-based scanners for AV as well as the first anti-rootkit products. Following several acquisitions and developments in its offering, F-Secure provides industry-leading cyber-security consulting services globally. Part of this development includes a strong summer internship programme I had the privilege of attending.

The 12-week Cyber Security Consulting Internship, as well as F-Secure as a whole, places a strong emphasis on training and skills development. For the first four weeks, I along with the other interns attended a series of seminars and workshops on the most prevalent areas of cyber security, such as application security, network security, cryptography etc. These included working with real-world examples, with up to date threats outlined, analysed, and reproduced to gain a complete understanding of their impacts and how to detect such threats on a clients infrastructure.

My remaining time at the company was dedicated to a brief research project proposed by fellows (F-Secure's name for employees) within the company. With a background in machine learning, I set out to detect malicious JavaScript automatically using common classification techniques. This included engineering the complete data collection pipeline for both malicious and benign samples, processing and storing of samples, feature engineering and finally classification and statistical analysis of collected samples. The result was a pipeline that allowed for any new websites to be scanned for javascript, and with an accuracy reaching 99% detect if the JavaScript contained within was malicious or not.

Return from Internships

Undertaking a remote internship during a covid lockdown is not something many would hope for, but my worries were quickly quashed once I experienced the remarkably positive work culture at F-Secure. Online chat rooms were constantly bustling with conversations ranging from the deeply technical to endless streams of cats. These "water cooler" moments we all miss from in-person working were had despite it all, and the openness and friendly disposition of all at the company made my time there a real pleasure. So, to anyone who is thinking about going ahead and either taking an internship with F-Secure or a full-time role: do it!

Nathan Rutherford: HP Labs, Bristol: April - October 2021

HP is a global leader in providing enterprise and personal computing products, ranging from laptops with built-in security protections, to management services for managing and monitoring the security for a fleet of enterprise solutions. HP Labs role within the organisation is to focus on anticipating medium to long-term problems that will impact HP customers, identify opportunities for innovation through early-stage proof-of-concept prototyping, and communicate these to the core business units (Anticipate->Innovate->Communicate). Each lab focuses on a specific area of interest for HP, these include 3D printing & Microfluidics, Digital Manufacturing and more importantly for my work, Security. I was based in HP Security Labs in Bristol, which has three broad areas of focus for research; Device Security (end-point-devices), Infrastructure Security (including cryptography, and supply chains), and Security Management (malware analysis and various topics in data-science). While each one of these areas deserves an article in their own right, I will stick to my experiences working with the device team alongside the incredible systems researcher Chris Dalton.

From April 2021 to November 2021 I was a Security Lab Intern at HP Labs, Bristol. As a member of the Device Security team I was focused on anticipating how we might better use hardware to support security solutions implemented in software, so that we can make more clear assumptions about what the software can and cannot be trusted to do. My day-to-day activities were not so different to what I would expect from my PhD research. I spent a lot of time reading about novel methods published in security conferences, and implementing a PoC solution as a communication tool. The difference and potential for growth as a researcher really came down to how I evaluated the potential utility or impact of the academic research presented at a conference for our industry use-cases. Industry research was (in my opinion) much more grounded in the reality, ensuring there is a balanced focus between advancing the 'state-of-the-art' and considering how the research could potentially improve the experience of HP partners and customers. While a subtle shift in mindset, I found this to be immensely valuable in developing my constructive criticism skills when evaluating research. I also got the opportunity to attend meetings held by HP leadership, which gave me a valuable insight to how research is viewed by top executives in the tech industry.

Of course due to the COVID pandemic I was based remotely for the duration of my internship. However this did not detract from my experience working at HP Labs at all, which I credit to the incredible culture cultivated by Simon, Kayte, Boris, and Jonathan. Everyone at the lab was very friendly and welcoming, going out of their way to setup one-on-one zoom calls to get to chat with me about what I was doing throughout my six month tenure. Kayte encouraged and facilitated coffee chats between all of us interns, many of which were based over seas and shared stories about their work and life experiences. The lab was its own research community, with teams sharing what research they had been up to, and weekly tech-talks by individual researchers about a topic they have been researching. Jonathan's weekly poet of the week was also a personal highlight of mine, and really set the atmosphere for the labs collectivist culture.

My personal view is that I benefited greatly from my six month internship at HP Labs, and would encourage anyone thinking of doing an industry research internship to take the opportunity. On a technical level I gained experience with many tools that are common within systems research both in industry and academia. As a researcher I gained more confidence in my ability to evaluate and communicate research ideas. It also allowed me to 'round out' my professional knowledge, giving me insight into how tech companies are managed, operated, and potential career tracks available outside of academic research. Overall I found it to be a fulfilling experience, and glad that this is something that is encouraged as part of my PhD.

Cyber Security PhD winter school

Taylor Robinson. 2021 cohort

In late 2021 and early 2022, I had the privilege of co-designing and running an interactive student session for the 2022 Cyber Security PhD Winter School. The session was designed alongside Rob Pell and Sarah De'Ath. Rob is a third-year PhD student at the University of Surrey researching dynamic protection frameworks for 5G networks against APTs. Sarah is a part-time PhD student and a lecturer in Digital forensics at De Montfort University.

I first met Rob and Sarah in early November 2021 to brainstorm ideas for the Winter School. During our meeting, we collectively expressed a desire to create a session that would be both fun and informational. After discussing several options, Rob decided to take a leadership role and develop an interactive session based on his research interest – ATPs. Inspired by games like Cluedo, we created a game where teams solved a "mystery" to successfully identify an APT threat group based on a series of intelligence briefings.

As a first-year CDT student with limited technical knowledge, I was apprehensive about becoming involved in a session entirely outside my comfort zone. However, with additional explanations from Rob and some independent research, I learned about an unfamiliar and exciting topic within information security.

During the development stages, I was responsible for designing five attack group profiles based on the MITRE ATT&CK framework. This process involved studying threat groups and their characteristics listed on the MITRE ATT&CK website and subsequently creating five fictional groups for our game scenario. I also assisted in writing the intelligence briefings for each round, which gave teams clues on the characteristics of the game's targeted fictional threat group. Further, my non-technical background became beneficial while designing the game, ensuring that we created a session that all participants, regardless of academic background, could successfully participate.

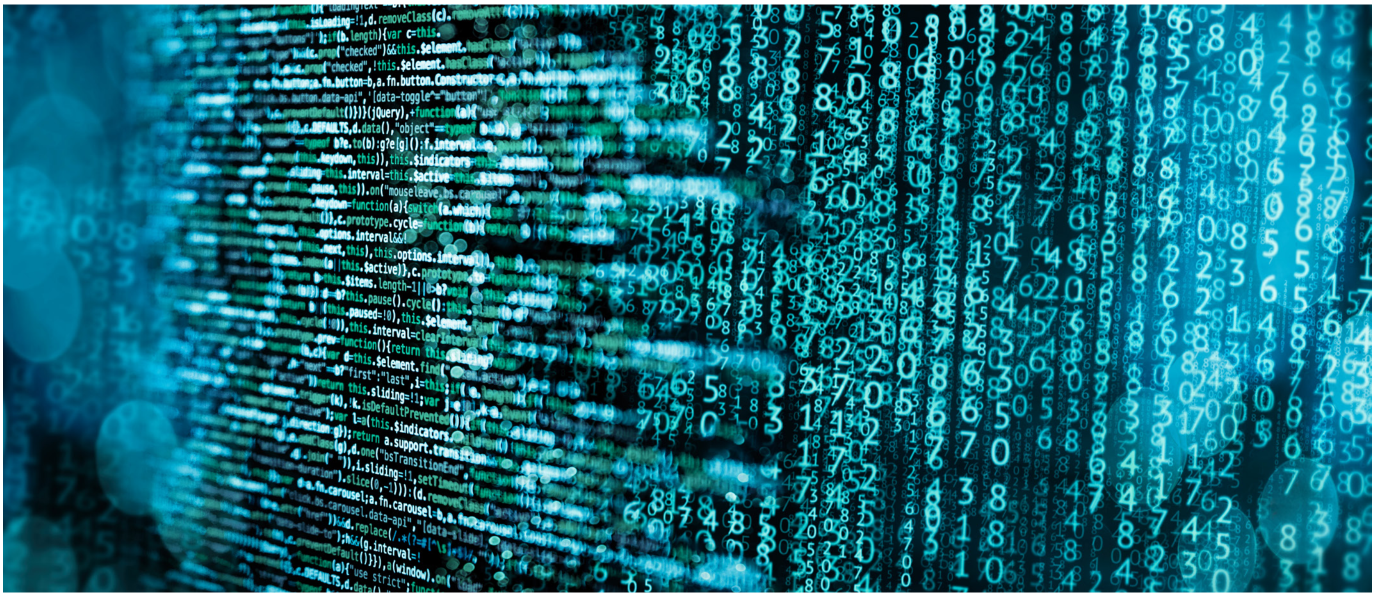
On the day of the Winter School, participants were placed into mixed teams from different universities and academic backgrounds. Rob and I were responsible for introducing the session, giving a brief overview of ATPs and the MITRE ATT&CK framework, and providing the intelligence briefings.

Once the game began, the teams were provided with an intelligence report every 15 minutes about the ongoing actions of an APT group. Following these briefings, the teams had to analyse the threat group's TTPs, campaign motivations, and threat objectives to determine the best course of preventative action. After a few moments to analyse each brief, the teams were provided several options to allocate resources and defend against a perceived threat group. At the end of each round, the team was informed if they successfully prevented the threat from occurring. If they guessed correctly, they became one step closer to identifying the correct attack group. The game extended several rounds, unfolding differently within each group depending on the selections made by the specific teams. At the end of the game, the teams used their accumulated knowledge to guess which attack group was responsible from the provided list.

After the game ended, Rob hosted a session explaining the answers to each round and answered any remaining questions from participants. We also listened to feedback from students. Students gave a few recommendations to improve future game iterations, but the overall feedback was positive, and students seemed satisfied with the session.

Upon reflection, I realise that participating in the Winter School was a truly unique and fulfilling experience. I stepped out of my comfort zone and am very proud to have assisted in developing a successful session for the Winter School. I was also able to collaborate with researchers who are more advanced in their PhD journey, which was beneficial from both an ideation perspective and, more broadly, to receive advice and support regarding the PhD journey.

The Winter School allowed me to work on a project and with a team that I would never have been exposed to otherwise. It was a challenging, creative, and fun opportunity that I feel very grateful to have experienced.



CDT Newsbites

Graduation

It's been a pleasure for CDT management to attend the graduation ceremonies of a growing number of CDT alumni over the years. The global pandemic however has prevented us from holding a graduation ceremony for many of our recent graduates - but we were delighted that Royal Holloway was able to host a winter graduation ceremony in December 2021 and that some of our students were able to return and celebrate their successes.

Many congratulations to

Dr Lydia Garms, Dr Amit Deo and Dr Jake Massimo

Farewell to Professor Carlos Cid

We would like to wish Carlos Cid all the very best as he moves on to his next adventure. Carlos was part of the team who successfully bid for funding and then set up the CDT back in 2013, going on to act as CDT Director. Carlos has been instrumental in helping the CDT develop into the centre that we know today - from the first cohort of 10 students in 2013, to a thriving centre with over 50 students and 25 graduates.

Carlos helped architect the CDT training, governed the spreadsheets with financial wizardry, and cared about every single student - following their fortunes and supporting them whenever he could. Carlos has been committed to the CDT project throughout, and the contribution and wealth of knowledge he continually demonstrated will be missed by all.

If the hard work and dedication to the CDT shown by Carlos is anything to go by, we know he will be a success in his new post. Carlos, it has been a pleasure to work with you - with a heavy heart we say goodbye and good luck - but are sure that we will remain in touch.

2022 entry: We are now open to receive applications for students to start their PhD studies in September 2022

To be awarded one of the four-year fully funded 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.

For more information on how to apply and a selection of potential research topics, see our website **royalholloway.ac.uk/CDT**

8602 03/22

UKRI 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