CDT Newsletter

EPSRC Centre for Doctoral Training in Cyber Security

Summer 2020

CDT update

Director's report

What a difference a few months make! It was all going so well…

Firstly, we hope this newsletter finds you and your family healthy and coping through these challenging times. As I write this, Royal Holloway is effectively a virtual place of work and it seems unlikely that the campus will be buzzing with life for the foreseeable future. But the university is very much alive and active, as is the CDT in Cyber Security for the Everyday.

The lockdown is disruptive, but the timing has not been disastrous. When lockdown commenced we had already completed the bulk of the first-year training activities and students were preparing to commence summer research projects. However, we had not yet made any of our "Cyber Security in the Wild" excursions, so plans to visit a number of our CDT partner organisations have been placed on hold. We also had to postpone the hugely popular two-week Network Security Practice Laboratory sessions. These events will be rearranged as and when life returns to a semblance of normality.

In theory, at least, studying for a PhD can be conducted within a lockdown environment. Everyone still has access to the internet, the web, and incredible communication tools. In practice, it's not quite so simple. While some people have even reported finding PhD life easier, with fewer distractions and more flexibility of time, others have been struggling with the isolation and the necessary motivation to keep going. I suspect we are all discovering things about ourselves at a time when our own personality traits play a significant role in how we approach the challenges of lockdown. Genuine difficulties have been created for students who were about to take part in visits, internships, and field trips to gather essential research data. Some of these can be conducted virtually, but not others. Some PhD students towards the end of their studies have experienced stress as they lose focus at a time when submission deadlines are looming and funding is running out. Others, already nervous about upcoming vivas, have had to prepare for the additional challenge of defending their thesis over the internet, rather than during a face-to-face meeting.

We welcome the announcement from the EPSRC that they will be offering funding extensions to students who have been adversely affected by the situation – this is very helpful and has provided comfort to some students. I am also pleased, from my own perspective, to be reading close to final drafts of a number of excellent CDT theses, and to have celebrated several successful outcomes from virtual PhD vivas since the start of lockdown.

The majority of our students seem to be coping well. There are many ways everyone is staying in touch. One of the most enjoyable is a fortnightly Zoom pub quiz, superbly run by Tabby and Jenna from the current CDT first year. I like to think that the fact our staff team is crushed every two weeks is not because we aren't worldly-wise and knowledgeable, but rather because CDT researchers are just much smarter! We are clearly getting something right during recruitment!

Life goes on, PhDs go on, and we hope very much that we will all be back on the campus as soon as it is safe to return.

Professor Keith Martin

Inside the cohort

Conducting research during lockdown

Wrenna Robson

Life in lockdown at first was pretty tough, what with some existing health issues that I was sorting out at the start of March, plus the general level of bluurrgghh!

In an ideal world, my cohort would have been continuing with the first-year training programme now, moving away from a very structured start into the scary world of real research.

We've had to enter into that much more quickly, since we're now all focusing on our first-year projects. I'm quite lucky, though, since I had already been thinking about my project before everything became a lot harder to sort out. I've got a supervisor, and some external parties who were the ones who originally suggested the project topic. After making some virtual introductions over e-mail, I've been planning some video meetings, reading some papers – there's been a lot of back and forth and that's been good. And I've been learning some new stuff, including some new programming languages – that's pretty exciting!

While it's been hard, I'm getting used to the new normal now, and time is starting to have some meaning again. I'm putting some structures down, and that's really good. I'm excited to bury myself in my work because it's a distraction from what's happening outside. That's nice – in fact it feels great.

Stay safe everyone, stay well, stay indoors. I will see you on the other side!

Lockdown life as a PhD student

Erin Hales

Last week, I tweeted about a day in my life as a PhD student during lockdown. In many ways my life during lockdown doesn't look that much different to my ordinary life. I read some papers, met my supervisors, and attended some conference talks.

Over the last couple of months I have really struggled with concentration. I felt the pressure from many news articles telling me that I should be inventing calculus or writing King Lear! Obviously this is nonsense. How can we possibly concentrate with everything that is happening?

I found (as ever) talking to the other CDT-ers and my supervisors so helpful. It is great to have people around me acknowledging that things are difficult and sending pictures of their cute pets. Some of us even began doing group study sessions online together. Knowing that other people were 'there' and being able to chat together in breaks helped me to move forwards by just doing a few things.

As the weeks have gone on, I've found some of my concentration powers returning. Especially after I deleted the Twitter app from my phone and started limiting how much I watched the news. In some ways I've embraced the online life, enjoying the CDT pub quiz and attending conferences online that I otherwise wouldn't have travelled to.

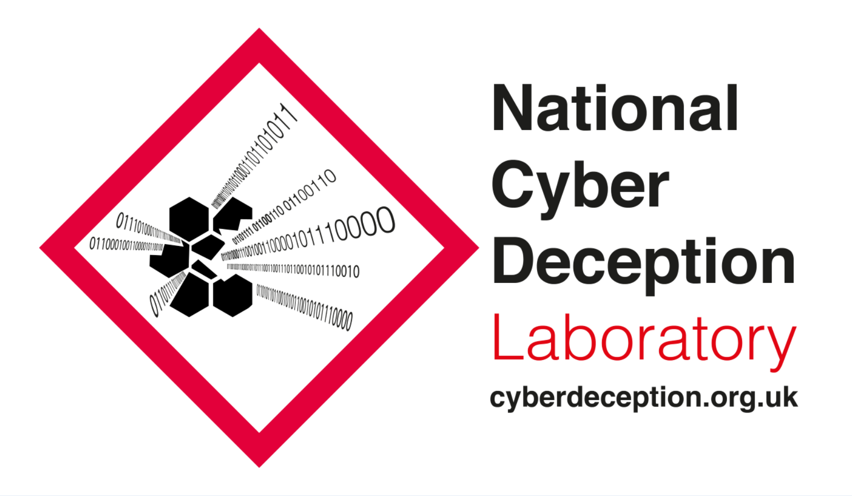
Despite these benefits of the online life, I'm excited to contemplate spending time together in person with everyone again and I look forward to being reunited with the informal space comfy chairs at work!

Erin's supervisors, Prof Sean Murphy and Dr Rachel Player

National Cyber Deception Symposium

Launch of the National Cyber Deception Lab

Neil Ashdown
Natasha Hales



On 6 November, we attended the inaugural National Cyber Deception Symposium held within the Defence Academy at Shrivenham. As early-stage researchers we felt it would be an excellent opportunity to learn about current research and thinking on deception techniques in the cyber domain. The event, which was held under Chatham House rules, attracted fantastic speakers, offering a range of views on the use of deception in cyber from industry, military, government and academic backgrounds.

The conference opened with an introduction to the new National Cyber Deception Lab. The lab is a collaborative virtual space which allows interested parties to share projects, research and events that work towards improving cyber deception as an active defence against current threats.

It was clear throughout the day that this was not a conference about the ability to 'hack back', for example by seeking to disrupt an adversary's networks in response to an intrusion. Rather, the focus was on 'active defence' conducted inside one's own networks. Deception was viewed as a key tool for shaping an adversary's behaviour, without having to cross the line and 'flip bits' on their systems.

One of the highlights of the day was a fascinating military history lesson, looking back at the use of strategic deception around the allied landings in Normandy. The discussion underlined the need for deception to be integrated and centrally directed, with a clear objective in mind.

There was also a talk considering cyber as the fifth domain of military operations. The practical upshot of this viewpoint was that – to be effective – deception must extend beyond the cyber domain into other areas of operation. Moreover, cyber needs to be seen as just one aspect of what was termed 'warfare in the information age', along with other aspects such as information operations. This realisation, it was argued, should prompt a focus on cognition as much as technology, underlining the importance of considering the psychology of your adversary.

There were some interesting questions to come from the day, such as what does building resilience and deception into technology look like? How do deception techniques differ when applied to artificial intelligence, as opposed to a human adversary? How can we build digital twins for systems and artefacts that will be convincing for adversaries, both human and machine?

A key debate was over what deception should look like for private-sector organisations compared to governments or militaries. Given the threat, it makes sense to develop 'nuts and bolts' or 'everyday' techniques that could be deployed by any organisation. However, as a deception operation increases in sophistication, it requires increasingly detailed intelligence on an adversary's decision-making processes. It is an open question how many private-sector organisations - with very different risk appetites to militaries – would want to engage in such activity, particularly given the challenges many organisations face in getting even the basics of passive cyber defence right.

The event was definitely a success, and the NCDL looks set to become an invaluable tool in the progress of developments in cyber deception techniques to build resilience in the UK. We left with an overriding sense of the importance of seeing cyber deception as one part of a wider response to the threats militaries and enterprises face, rather than a purely technical consideration to be viewed in isolation.

Collaboration between the different areas; military, government, industry and academia, is crucial to building national resilience. However, it seems certain to be a long journey in which education and culture will play a decisive role. A particularly poignant quote from that day was "the only thing that ever goes up in value is cyber security culture." We can, and do, spend a huge amount on cyber security technology. However, it is arguably the investment in education and culture that is truly important, and which may be more economically beneficial in the long term.

Away from the cohort

Pallavi Sivakumaran

Royal Holloway's CDT in Cyber Security expects that grant recipients complete an industry placement during the course of their 4-year PhD. Apart from the advantages of placements in general, for PhD students - who are normally focused on a single, narrow subject area - placements offer the opportunity to temporarily 'branch out' and explore other topics.

My industry placement was with F-Secure Consulting (originally MWR Infosecurity) – a cybersecurity consultancy with a strong research focus. The company provides vulnerability assessments and red-teaming services, but also offers more specialised security analyses of proprietary hardware and firmware. In addition, it actively contributes to the InfoSec community via technical whitepapers and open-source security tools. It was this last aspect that strongly appealed to me, as it's something fairly rare in a standard security consulting firm.

During the initial interview process, a placement duration of six months was agreed upon. I have found from past experience that completing corporate 'on-boarding' procedures and equipment setup, as well as the leaving procedures at the end of employment, can all reduce the amount of time available for doing actual work. In addition, while I wanted to learn as much as possible during the placement, I also wanted the opportunity (and time) to contribute back to the organisation. So it was decided that the first three months of the placement would be spent on training and shadowing activities, and the last three months on a development project.

Phase 01: Training and shadowing

F-Secure Consulting makes available a significant amount of training resources for its employees. While there is no formal technical training schedule, the availability of these resources alone is enough for most people. I would like to specifically mention Playground, an in-house developed cloud platform on which training labs can be run. A number of security exercises are available, targeting different platforms and technologies, as well as different levels of expertise. Several labs also offer step-by-step guidance or hints, so that beginners can learn techniques for approaching specific problems. I found Playground to be an invaluable resource during my placement.

Once I had gone through a number of training labs, I was assigned to shadow security consultants on a few projects. This, again, was very useful, as I was able to observe and often also participate in the different stages of a project, including the initial requirements gathering, preparation of the statement of work, the actual assessment itself, as well as the report write-up.

Phase 02: Development project

During the final three months of the placement, I was asked to develop a tool that would simplify the identification of Android logic bugs for Mobile Pwn2Own competitions. (For anyone who is unfamiliar with Pwn2Own, these are competitions where the goal is to execute code or exfiltrate files from various devices, usually with minimal or no end-user interaction.) Previous employees from MWR had developed a proof-of-concept that went one step towards achieving this goal. My task was to expand upon their work and develop a complete, extensible tool that could be executed with minimal effort.

The tool I developed (pre-christened Jandroid by my predecessors) allows for extendable template-based pattern-matching for Android APKs. Development was completed just as F-Secure concluded its preparations for that year's Mobile Pwn2Own, which meant that the tool could be used to verify some pre-identified vulnerabilities in the applications under test. Jandroid was made available as open-source software via F-Secure Labs' GitHub shortly before my placement ended.

Thoughts

Embarking on an industry placement in the middle of a PhD involves several practical considerations that need to be taken into account. Firstly, whether or not the organisation provides financial support will determine whether PhD funding can be interrupted, which in turn may limit the duration of the placement. The duration should also be selected to be long enough to maximise the benefits to the student and the organisation, and yet not so long that the student finds it difficult to return to their own research at the end of the placement. In addition, unless the organisation's office is situated close to the university, the student will have to decide whether to temporarily move to new accommodation or to endure potentially long commutes. As an example, I opted to remain close to the university, which necessitated a daily commute of over three hours.

Despite these challenges, I found the industry placement to be a great learning experience and is a component of the PhD that I believe students should make the most of.

Away from the cohort

Luke Stewart

I am currently interning at Thales UK, as part of their Research, Technology and Innovation Department at their headquarters in Reading. Thales are involved in everything from biometric passports to autonomous vehicles, but the focus of my internship is homomorphic encryption.

The motivation for studying homomorphic encryption is as follows. We wish to store large amounts of (encrypted) data on an external server, and subsequently require the server to perform operations on this data. However, we don't want to reveal anything about the data itself, while outsourcing the computation to the server. A possible real-world example of this is medical data – we want to be able to store large amounts of patient information, and then search this data for, say, those patients with a particular genetic condition. Homomorphic encryption provides a way to achieve this.

This is a far cry from my research 'day job' concerning key distribution. However, using the internship as an opportunity to study an aspect of cyber security that I'm not familiar with has been enjoyable and beneficial. The opportunity arose during the CDT showcase last May, which shows the value of these 'get-togethers'. Networking is not my forte, and is something I've had to practice during my time as a PhD student. Now I can say that I successfully networked my way to an internship at a global company! What's more, it was set up through a former CDT student, which shows the reach of the CDT. For me, this internship has been an all-round "win".

Feargus Pendlebury

Last autumn I was fortunate enough to spend three months interning at Facebook as part of their Abusive Accounts Detection team.

As widely known, Facebook faces a number of challenges regarding the misuse of its platforms by bad actors who try to exploit its scale and reach to propagate harmful content. To rise to these challenges, Facebook has been rapidly growing its Community Integrity organisation over the last couple of years. To tackle the root cause of abuse, Community Integrity encompasses a number of teams that specialise in detecting, tracking, and responding to fake, abusive, or compromised accounts from which harmful content originates.

The Abusive Accounts Detection team design and manage a number of pipelines for identifying bad actors on Facebook and Instagram, many of which include machine learning methods to help manage the huge scale of internet traffic that passes through the platform. The main limitation to deploying machine learning detection in a security context is that the data is adversarial in nature–attackers actively try to evade detection and will react to any changes made to the defences. This means the thing you're trying to detect morphs and evolves, sometimes very suddenly and severely, which can cause you to misclassify legitimate accounts or let malicious accounts slip through. Much of the research there aims to develop more robust, adaptable approaches that can handle the shift in distribution, or to obscure the change in signal when the defences are updated so that the attacker doesn't feel a need to change their habits at all.

My research there focused on developing novel techniques to use the shift in the data distribution (which is usually a bad thing) to instead predict how attacker behaviour was beginning to change. This would allow teams to be more proactive when updating the pipelines and less reliant on manual effort, freeing up expertise to focus on other requirements. Seeing attackers change their behaviour in real time, with real data, at massive scale, was an extremely exciting and eye-opening experience which I've found invaluable for informing the context of my subsequent research.

I had a really fun time interning at Facebook - interns are treated the same as full-time employees, given the same responsibilities, and expected to contribute to the production codebase which makes for a really cool experience. I also found it heartening to experience an internal culture that encouraged dialogue and debate about the company's policies and future direction. Overall, I'm very grateful to have been able to work with and learn from some brilliant people in the Community Integrity teams and am thankful for the CDT for enabling us to take the time out to tackle security problems from the industry perspective.

CDT journeys

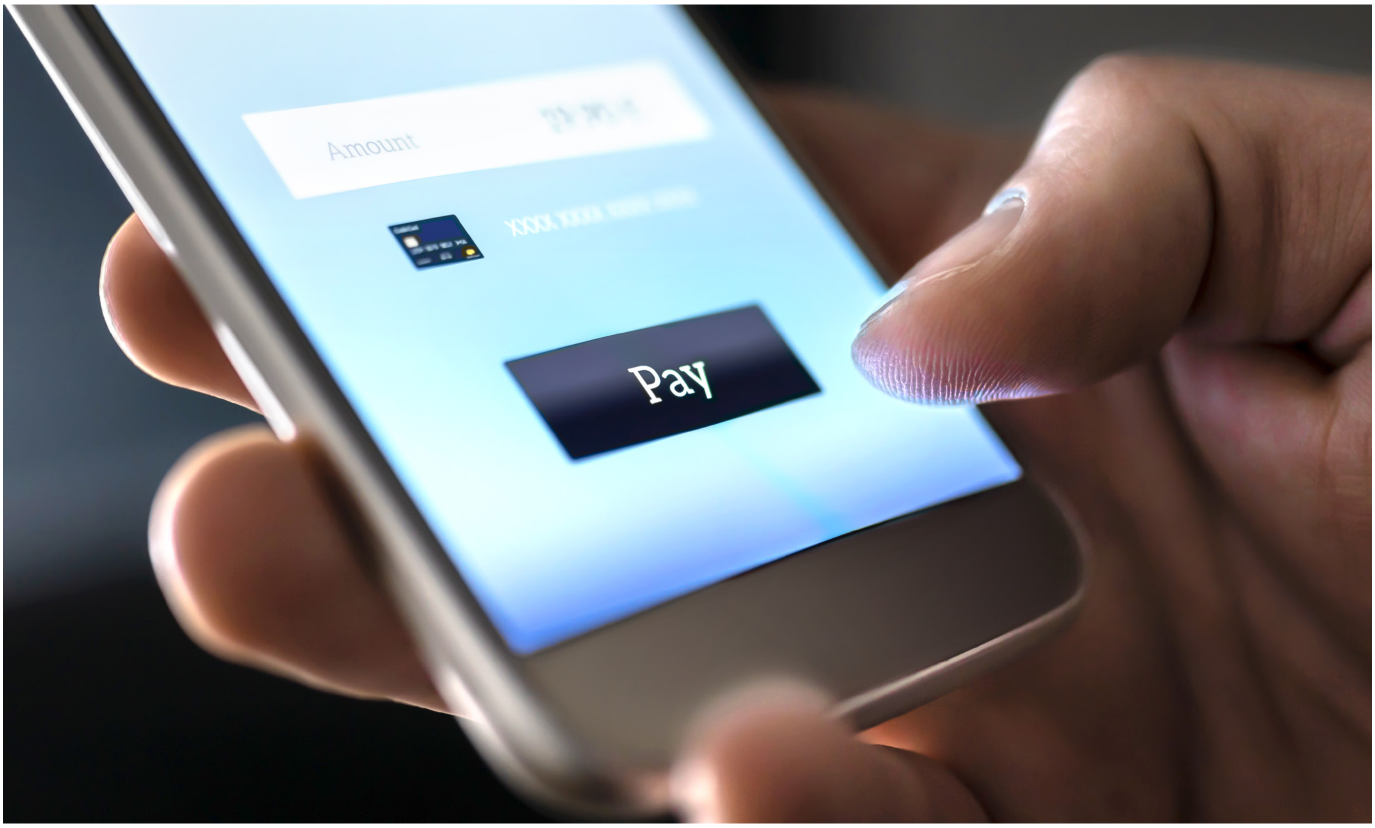
Dr Carlton Shepherd

Reflecting on my PhD experience, one of the most beneficial features of the CDT programme is that it's multi-dimensional. From the training sessions in the first year, to the various industrial presentations and visits throughout, I found it invaluable to be exposed to a wide variety of areas within information security. Studying alongside peers focussed on a diverse set of interests cryptography, systems security, programming language security, geopolitics and many others provided an endless source of interesting discussions and viewpoints that, I believe, wouldn't have been available elsewhere.

Another major benefit of the CDT, in hindsight, is the opportunity and, indeed, expectation to present one's work regularly, whether it be at the CDT Showcases, internal student seminars, or external events, such as conferences. Learning to shape presentations to diverse audiences has been invaluable following the conclusion of my PhD, where I have been required to present to a machine-learning expert one week and the Chief Technology Officer (CTO) the next. Frankly, I found presentations to be nerve-wracking before I arrived at Royal Holloway, but the experience I gained during the CDT is now paying dividends.

My background is in Computer Science and, although I started the CDT with a bit of experience in an academic research environment, it took some time to settle on an appropriate research topic. I converged on the broad topic of trusting embedded sensing devices, focussing on hardware-assisted system security measures and, in particular, trusted execution environments (TEEs). During this time, I also worked on a concurrent project in the Smart Card and IoT Security Centre on detecting relay attacks on contactless mobile transactions, e.g. payments, using smartphone sensor data as a proximity detection mechanism. This involved a substantial amount of data analysis and machine learning, which I now use on a daily basis in my job as a Research Scientist at OneSpan, where I currently work on detecting fraud from banking transaction data. In retrospect, this speaks to one of the CDT's major benefits and privileges: the flexibility to explore areas outside of your initial scope of expertise and to attend conferences and other research events for inspiration.

Much of the above stems from the generous financial support that alleviates many of the stresses and obstacles that, I know, can be a real impediment for students on traditional PhD programmes elsewhere. However, it is due largely to my supervisor, Prof. Konstantinos Markantonakis, who was supportive, accommodating and provided advice throughout my time at Royal Holloway. More generally, I found all ISG staff members to be down-to-earth and approachable, in addition to being expertly and highly professional. In short, I would have no qualms in recommending the CDT programme at Royal Holloway to any prospective student who wishes to pursue a research-oriented path in information security. The makeup of the ISG, the student cohorts, the flexibility, as well as the resulting opportunities, are something that, I believe, can't be found anywhere else.



CDT journeys

Dr Joanne Woodage

Looking back at my time in the CDT, I really couldn't imagine doing my PhD anywhere else and I feel very grateful for the many opportunities it has presented to me.

Not least that I was accepted me as a student in the first place! When I graduated from the University of Manchester with a Mathematics degree in 2013, I had no idea what I wanted to do. Having spent much of the next year failing to 'find myself' on a backpacking trip around Asia, I stumbled across cryptography and wondered if this might be a way that I could use the pure mathematics I had enjoyed in my degree in an applied context. I'd never done any formal work in cryptography and my computer science skills didn't extend far beyond a cursory grasp of Excel, so I feel very lucky that the CDT was willing to take a chance on a student with a lot of enthusiasm but very little concrete experience.

The CDT attracts students from a real mixture of backgrounds and areas of expertise, and the diverse cohort this creates is one of the group's greatest strengths.

As a complete newcomer to cyber security, my first year in the CDT was an onslaught of new concepts and three letter acronyms, and there were definitely times when I wondered how I would ever understand anything enough to produce a thesis. Our first year training was invaluable to get up to speed on the wide range of topics that fall under the umbrella of cyber security. We were also given the freedom to explore different areas before settling on a research topic, which allowed me to completely change direction away from the mathematical cryptography that I'd assumed I'd work on to provable security, an area of cryptography which draws on techniques from theoretical computer science to construct rigorous and formal proofs that cryptographic schemes achieve certain security properties.

My PhD work focused on the application of provable security to 'real world' cryptographic problems, and included analysing (and finding flaws in) standardised and widely deployed pseudorandom number generators, and developing cryptographic solutions to facilitate verifiable abuse reporting in encrypted messaging applications.

On top of the opportunity to work in a world-class research environment in the Information Security Group at Royal Holloway, the CDT was brilliant for facilitating opportunities to engage with the wider research community, in particular with industry. In our first year we had regular visits to or from companies with links to the department, which undoubtedly helped steer my research away from pure theory towards real-world problems, and the travel support we were given allowed me to present my work at conferences around the world. I was very lucky to undertake two excellent internships, spending four and a half months at Cornell Tech in New York City, and three months at Microsoft Research in Redmond. The Microsoft internship, taken to fulfil the CDT's expectation of an industry placement, was pivotal to my decision to move into industry after my PhD. I'm so glad that the CDT forced me to step outside the university environment that I'd become comfortable in and see the opportunities beyond.

Following my time in the CDT, I spent a brilliant year working at Crypto Quantique, a London-based start-up developing end-to-end security solutions for the Internet of Things. While it was nerve-wracking leaving the academic ivory tower for my first 'proper' job, I found myself pleasantly surprised by how well-prepared I was thanks to the CDT. The broad cyber security training in the first year has proven a solid foundation upon which to build deeper knowledge, and the strong engagement with industry meant that this new environment wasn't entirely unfamiliar. Most importantly, the CDT shifted my mind-set to find the things I don't know less daunting and more exciting, and has taught me that you can pick up almost anything if you stick at it long enough. In a couple of weeks, I will be joining Microsoft Research, Cambridge, and am excited for all that lies ahead.

Writing this has made me think back to the very start of my PhD and how much things have changed. Concepts that seemed utterly impenetrable at the start of my CDT studies are now things I use every day at work, and the direction my career has taken is very different to what I expected when I started, and much the better for it. The CDT has opened doors that I never knew existed and – corny as it sounds – has really changed my life. I'm very thankful to have been given the opportunity to complete my PhD studies in such a unique and special place.

Joanne on her US placement, in front of the Seattle great wheel.

Why We Fight* Learning from competition

By Robert Carolina, Senior Visiting Fellow

Once again, 2020 was a great year for CDT student participation in the Atlantic Council 'Cyber 9/12 Strategy Challenge.' The third annual competition in London was the toughest to date, starting with a competitive entry process. Of more than 30 UK-based teams who applied, only 17 (including two teams from Royal Holloway's CDT) were selected to compete. One of our teams went on to the Final Round of this year's competition, placing Third.

Convened in different locales around the world, teams comprised of four students simulate the high-pressure task of analysing available information about cyber security threats, synthesising these, and briefing senior government officials with findings and recommendations. The competition relies upon information sources assembled into a briefing pack such as (real) research reports, (real and simulated) online media, (real and simulated) private sector threat analysis, (simulated) classified government intelligence reports, and even a (simulated) television news report.

Our first CDT student team competed in Geneva in 2017, advancing to the Semi-Finals. Our next team placed First in the 2018 inaugural London competition. Three teams competed in 2019: two in London and one in Geneva. And now two more in London, including our second appearance in the Final Round. That's a lot of competition.

Students who wish to compete organise themselves into teams and recruit a coach. Participating is entirely voluntary and brings no formal academic credit.

So WHY do they do it?

It's been my privilege to coach CDT teams three times: twice in London and once in Geneva. From this vantage point, I have seen a number of benefits students can take from the competition.

Each competition forces students to make use of a wide variety of disciplines they might not otherwise encounter on their academic journey. Teams must prepare to justify their recommendations within the emerging framework of international law which now pervades state cyber operation decision-making. They are required to appreciate the risks and potential impact of hostile cyber operations and countermeasures.

Teams are encouraged to think holistically about the needs of an entire society; to prioritise both domestic and international responses; and to consider non-cyber impacts and responses. Their chances of success go up tremendously if they exhibit an appreciation of the practicalities needed to implement their recommendations, such as the length of time necessary to adopt new laws or procedures, to commission new offensive cyber programmes, to task or redeploy limited civil service resources, to leverage support from non-state actors such as the community of CISOs and security vendors, or to persuade international partners to participate in multilateral action.

Teams are forced to confront the reality of decision-making in an atmosphere of less-than-complete, potentially inaccurate, and sometimes conflicting, information. They must sift through messy and diverse sources of intelligence and synthesise a picture of threats that can be explained to non-expert decision-makers within minutes – all while being careful to assign appropriate degrees of confidence to different elements of their report. They must learn the difference between acting as an honest broker of available evidence (which is the job of an analyst) and acting as an advocate for a specific outcome (which is not).

The best teams learn and demonstrate good teamwork skills. They face difficult choices in how to allocate tasks among themselves. The time pressure of the competition begins at a relaxed pace with weeks available to produce and deliver Round 1 submissions. Those selected to advance to Round 2 are thrown into a situation in which they have a single overnight window to absorb significant new intelligence and revise their view of the situation. The very few teams who advance to the Final Round face the highest-pressure component – only 20 minutes in which to absorb a few bits of critical additional intelligence before briefing the judging panel who simulate government leaders – often comprised of persons who have served in the senior civil service roles the students are now simulating.

The competition is a labour of love for a large group of volunteers from industry, government and academia, including CDT graduate and former competitor Dr Andreas Haggman (Royal Holloway, 2019) who remains heavily involved in the London competition. The effort required to develop each competition's intelligence pack is considerable, as is the effort to recruit and coordinate large numbers of judges.

Each competition strongly reflects local values, methods, and standards. Judges in London simulate UK government officials; in Washington, DC they simulate US federal government officials; and in Geneva they simulate a multinational 'task force of European leaders' including heads of government and defence. Competitors must be prepared to make recommendations fit for the relevant environment.

Of course, no competition is perfect, no simulation is perfect, and the process being simulated is itself far from perfect. Judges and competition officials are ultimately required to rank teams. Reasonable people can disagree about aspects of the competition process, as well as the results.

But I find that the students who take the most from the competition are those who embrace it and invest in it for the learning opportunity it represents. I've watched students climb and conquer steep learning curves. I've seen cryptography students gain a better understanding of politics. I've watched students of law and international relations learn to appreciate the practicalities of cyber operations. I've seen computer science students learn how international law continues to influence this sphere of operation. And I've watched as all of them learn more about how the decision-making 'sausage' is made.

These are all good reasons to compete. And in the context of the competition, this is, I believe, why we fight.

*with apologies to Frank Capra

CDT Research newsbites

Amy Ertan presented 'International Data Transfers and Data Protection Legislation: Challenges and Opportunities for Brazilian Trade' at the PEPA Society of International Economic Law virtual conference on 19th May. The presented paper is an output of her UK-Brazil data protection fellowship with ITS Rio.

Georgia Crossland had an article published in InfoSecurity magazine titled 'Biases in Perceptions of Information Security Threats'. This looks at how the optimism bias and fatalistic thinking might impact our information security risk perceptions.

Feargus Pendlebury, together with Fabio Pierazzi, Jacopo Cortellazzi, and Lorenzo Cavallaro, have had their paper 'Intriguing Properties of Adversarial ML Attacks in the Problem Space' accepted to IEEE Security and Privacy 2020. The paper (along with a teaser trailer) can be found at s2lab.kcl.ac.uk/projects/intriguing. Feargus is currently a visitor at The Alan Turing Institute, the UK's national institute for data science and artificial intelligence research.

Amy Ertan was a 2019 FS-ISAC (Financial Service - Information Sharing and Analysis Center) Building Cybersecurity Diversity Scholarship Recipient. The award allowed the opportunity to attend - and present - at the EMEA Summit in Berlin in October, and matched Amy with a senior industry mentor (an ISG alumni, no less, who has subsequently spoken at ISG diversity events).

Fernando Virdia had two papers accepted for EuroCrypt 2020 - this is the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques.

The papers titled 'Implementing Grover oracles for quantum key search on AES and LowMC' and '(One) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes' will be presented as part of a virtual conference.

Fernando Virdia has also had a paper accepted for PKC 2020. His paper, titled 'Improved Classical Cryptanalysis of SIKE in Practice' results from a Microsoft Research Internship in 2018.

Amy Ertan had two articles published in InfoSecurity magazine: the first exploring how virtual events may increase inclusivity in the cyber security field, and the second outlining the findings of an ISG literature review into cyber security behaviours in organisations (full report available: arxiv.org/abs/2004.11768).

Erin Hales was selected to participate in a Private AI Bootcamp hosted by Microsoft Research in Redmond, USA that took place in December 2019. During the bootcamp, Erin worked as part of a small team to design and pitch a novel application of homomorphic encryption. The proposals from each team were subsequently published by Microsoft as technical reports.

(microsoft.com/en-us/research/uploads/prod/2020/02/PrivateAIBootcamp2019_TechReport-team6.pdf

Georgia Crossland and Amy Ertan have been working with other academics and behavioural scientists at CybSafe to organise the inaugural 'Impact' conference on 29 September 2020. This day conference (call for abstracts opening soon) provides the opportunity for researchers to present their work on cyber security related topics to an audience of industry and government attendees.

Winter Graduation – Dr Jonathan Hoyland

In December, we celebrated alongside Dr Jonathan Hoyland who received his award in the 2019 Royal Holloway winter graduation ceremony.

2020 entry:

We remain open to receive applications for students to start their PhD studies in September 2020. If you are interested in applying, please contact us directly to discuss your suitability for the programme.

Selected applicants are awarded fully-funded PhD studentships for four years. To be awarded one of the studentships, candidates will need to have an undergraduate and/or masters qualification in a relevant discipline.

Suitable backgrounds are (but not limited to) computer science, criminology, economics, electronic engineering, geography, geopolitics, information security, law, mathematics, philosophy, politics, psychology, software engineering and war studies. We will also consider applicants with a professional background, so long as they are able to provide evidence of demonstrable academic skills as well as practical experience.

8262 06/20

EPSRC
Engineering and Physical Sciences
Research Council

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

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