GCSCC welcomes newest regional partner in South Africa and moves to online training

In light of the Covid-19 pandemic the University of Oxford and thousands of other educational institutions have moved to online teaching. The Global Cyber Security Capacity Centre (GCSCC) – normally not as involved in teaching activities as many others in the department – found itself involuntarily being one of the first movers in this regard as part of the centre’s contingency planning. One of the first actions was to change travel plans for a visit to South Africa and Uganda to train participants on the deployment of its Cybersecurity Capacity Maturity Model for Nations (CMM).

But let’s start from the beginning: In January this year the Global Constellation of Regional Cybersecurity Capacity Research Centres, which has been established by the GCSCC over the last years, welcomed its newest partner, the Cybersecurity Capacity Centre for Southern Africa in South Africa. C3SA (‘Ceesa’) is the second regional partner since the Oceania Cyber Security Centre (OCSC), in Melbourne, Australia, became partner in 2017 with funding from the Government of Victoria. C3SA is based at the University of Cape Town (UCT) and is a consortium between the GCSCC, UCT’s Department of Information Systems, Research ICT Africa, a digital policy think tank based in Cape Town, and the Norwegian Institute of International Affairs (NUIP). The funding for this two-year project comes from the Ministry of Foreign Affairs of Norway. The three centres of the Global Constellation, GCSCC, OCSC and C3SA, aim to drive regionally informed cybersecurity capacity research and lead the deployment of the GCSCC’s CMM, in their respective regions, and sustain the CMM’s impact from the past six years.

‘Collaboration on cybersecurity is crucial to all of us,’ said Sadie Creese, Professor of Cybersecurity at the Department of Computer Science, and founding Director of the GCSCC. ‘Our work with colleagues at the new C3SA is aimed at enhancing cybersecurity capacity-building in the Southern African region. It will not only contribute to building cyber-resilience for the countries involved, but also to further the academic excellence in cybersecurity across South Africa and the wider region. We welcome this addition to the growing constellation of partnerships around the world.’

Cybersecurity capacity plays a crucial role in Africa, even more so during a global pandemic when more and more activities move online and users are more exposed to the risks in cyberspace. According to Enrico Calandro, Co-Director of C3SA and Senior Research Associate at Research ICT Africa, ‘cyber threats and risks are particularly challenging for African countries and nations affected by structural inequalities, conflicts and fragility. Having, generally, developing digital and physical infrastructures, weak institutional arrangements and governing mechanisms compounded by limited resources, the digitalisation of these countries is often characterised not only by low levels of connectivity, digital inequality, and limited opportunities, but also by insufficient security which places societies and individuals at a high risk of further marginalisation.’

The establishment of a research centre focusing on the region, C3SA provides ‘a platform for governments, intergovernmental organisations, the private sector, and civil society organisations to leverage cyber capacity research in their efforts towards building more equal,

continued on next page
inclusive, safe, and resilient digital economies and societies. C3SA will achieve its objectives by conducting regionally-focused research on cybersecurity capacity by deploying the CMM that provides countries with a baseline for capacity-building and resource allocation, and by developing and implementing locally-informed educational programmes’, says Enrico.

Professor Wallace Chigona, Co-director of C3SA, adds, that ‘C3SA will achieve its objectives by taking a multifaceted approach to cybersecurity capacity maturity advancement. This approach includes: Train-the-trainer activities to prepare our local researchers to deploy the CMM; the completion of national-level assessments to better understand what constitutes national cybersecurity capacity from an African perspective; capacity-building initiatives in the form of post-graduate training; and analysis and dissemination of findings to ensure that lessons learnt can have an impact on cybersecurity policy-making’.

The CMM facilitates the assessment of the maturity of a country’s cybersecurity capacity across five dimensions. The deployment of the CMM is a quite intensive process which is led by the GCSCC or its partners and was described in the Winter 2018 edition of Inspired Research (issue 13). It includes research and facilitation skills, but also requires a very good understanding of cybersecurity as a multidisciplinary subject which relates to political, social, economic, technical and also psychological issues. Therefore to ensure C3SA fulfills its objectives and as part of the ‘onboarding’ activity for the GCSCC, there are plans to train researchers who come from different disciplines in the deployment of the CMM. Each CMM consists of desktop research, but the core part of the assessment process involves 10 focus group discussions over three days for which the research team travels to the country on invitation by the government. The researchers speak to no fewer than 200 stakeholders from the government, private sector, critical infrastructure, civil society and others. Afterwards the researchers draft a report including recommendations for each of the dimensions which is submitted to the respective host government. Therefore, detailed training is needed to produce high quality reports.

The CMM Deployment training is normally done in two parts: in-person sessions and ‘learning on the job’ during a CMM review. This was the intended approach for the new colleagues in Cape Town and a team from Oxford had been booked to travel to South Africa in March to attend the launch event of C3SA and to conduct training for the researchers affiliated to the Centre, including two research fellows and two PhD students, as well the outreach staff and other members of UCT who are affiliated to the project.

The week afterwards the teams from Oxford and Cape Town would have travelled to Kampala to conduct the first joint CMM on invitation of the Ugandan government. However, both South Africa and Uganda were amongst the first countries to impose travel restrictions for incoming visitors due to the COVID-19 pandemic and therefore the launch event had to be postponed indefinitely. However, both partners decided nevertheless to proceed with the planned train-the-trainer activities and jointly decided to move the training online.

Over March and April in 20 online sessions the GCSCC team facilitated the C3SA researchers to understand the GCSCC and the Constellation’s purpose and aims, and the context of this global project. Through presentations by the researchers and the members of the GCSCC’s Technical Board they took a deep dive into the CMM, its rationale and structure and how it enables countries to have a benchmark for cybersecurity capacity building and investment. Through interactive and home exercises they learned in theory how to deploy the CMM, conduct focus group discussions, and to plan, organise, and conduct a CMM review – from the agreement with the host government, to data collection and report drafting, to the publication of the report by the government. The training also included an introduction to the global data set that the GCSCC has built with the input of over 80 CMM assessments since 2015, and the qualitative research arising from it. The training was conducted using Microsoft Teams, which turned out to be a stable system considering the quality of the Internet connection.

Self-study was also part of the training. The participants looked into the GCSCC’s resources including the CMM document itself but also the CMM Deployment Manual, a CMM Structured Field Coding Tool, various example reports, academic publications along with online resources such as the Cybil Portal, a global knowledge resource on cyber capacity building that the GCSCC has developed with international partners. Colleagues of the Oxford Cyber Security centre supported the training and shared lessons they have learnt from their work with the GCSCC and the CMM.

Overall, this part of the training worked well considering that everyone involved had been pushed into remote format on quite short notice. This online format also had the nice side effect that it allowed our new colleagues to ‘virtually’ meet everyone who is involved in the GCSCC – and it also was an opportunity for the GCSCC to get to know the C3SA which is in South Africa, Malawi and Zimbabwe.

The joint country visit, which is the second (and most crucial) part of the training, needed to be adapted and required a new approach to the usual CMM methodology. With the Ugandan government, who are going through the CMM process for the second time, this has been a challenge that GCSCC and C3SA has taken in consultation with the Technical Board of the GCSCC. Between May -July 2020, the researchers from Cape Town will conduct detailed desk research about the Cybersecurity capacity of Uganda based on the 2015 CMM report, followed by online expert interviews and focus groups with key Ugandan stakeholders. The outcome will be a preliminary CMM report that GCSCC and C3SA will submit to the government later this year which will also complete the CMM training for C3SA.

Despite the challenges this training imposed on the team, it was a good learning experience and when the whole process has been completed and evaluated, this online programme may inform future CMM training activities for partners and stakeholders.