Vertretung des Cyber-Defence Campus am Cooperative Cyber Defence Centre of Excellence in Estland stärkt die Zusammenarbeit zwischen der Schweiz und der NATO

William Blonay, Mitarbeiter des Cyber-Defence Campus, armasuisse Wissenschaft und Technologie, wurde im Februar 2022 für drei Jahre als Vertreter der Schweiz an das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estland, entsandt. Nach einer thematischen Einführung in das CCDCOE spricht er in einem Interview über seine Erfahrungen und gibt einen exklusiven Einblick in seine Tätigkeiten am CCDCOE.

Autor: Sarah Frei und Michiel Lüchinger, Cyber Defence Campus, armasuisse Wissenschaft und Technologie

Das CCDCOE ist ein von der NATO akkreditiertes Cyber-Kompetenzzentrum. Das Ziel dieser Institution ist, die Forschungs- und Ausbildungszusammenarbeit im Bereich der Cyberabwehr international zu stärken. Umgesetzt wird dieses Ziel durch die Organisation von gemeinsamen Übungen sowie die Durchführung von Forschungsprojekten, technischen Schulungen und Konferenzen.

Die Cyberangriffe auf private und öffentliche Institutionen in Estland im Jahr 2007 haben die potenzielle Verwundbarkeit der NATO-Staaten hinsichtlich Attacken auf Informations- und Kommunikationssysteme verdeutlicht. Ein Jahr später wurde das Cyberabwehrzentrum in Estland gegründet, welches eines von 28 akkreditierten «Centres of Excellence» der NATO ist. Das CCDCOE ist nicht Teil der NATO-Kommandostruktur und hat kein operatives Mandat. Die Teilnahme steht den NATO-Staaten frei. Auch Nicht-NATO-Staaten können sich als sogenannte «Contributing Nations» am Zentrum beteiligen, wie dies Finnland, Österreich, Schweden, Südkorea, Japan, Irland, Australien, Ukraine und die Schweiz gemacht haben (Stand 15.11.2022).

Durch diese Zusammenarbeit profitiert die Schweiz seit ihrem Beitritt als «Contributing Nation» im Jahr 2019 vom Informations- und Wissensaustausch sowie von den diversen Forschungs- und Ausbildungsaktivitäten des CCDCOE. Die Teilnahme trägt ebenfalls zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) und der Strategie Cyber VBS 2021-2024 bei. Beide Strategien messen der internationalen Zusammenarbeit eine wichtige Rolle zu, die in Zukunft weiter gestärkt werden soll. Vor dem Hintergrund der veränderten weltpolitischen Lage ist es der Schweiz ein Anliegen, die internationale Zusammenarbeit, speziell im Bereich der Verteidigung, zu vertiefen.

Die Teilnehmerstaaten des CCDCOE entsenden jeweils maximal zwei Expertinnen oder Experten als Vertreter nach Tallinn, die in verschiedenen Kompetenzbereichen wie Technologie, Strategie, Operationen, Unterstützung, Ausbildung und Training sowie Recht tätig sind. Die Kompetenzbereiche verdeutlichen die Vielfalt des Fachwissens im Bereich der Cyberverteidigung und Cybersicherheit. Die Schweiz ist gegenwärtig mit zwei Personen beim CCDCOE vertreten: Mit Lisa Schauss, Mitarbeiterin der Führungs- und Unterstützungsbasis der Armee (FUB), die zum Kompetenzbereich Ausbildung und Training gehört, und mit William Blonay, Mitarbeiter des CYD Campus, der Teil des Kompetenzbereichs Technologie ist.

Die Forschenden des CCDCOE leisten einen wesentlichen Beitrag zum wissenschaftlichen Diskurs in sämtlichen Kompetenzbereichen des Cyberabwehrzentrums sowie zur praxisorientierten Ausbildung von Cybersicherheitsexperten. Ein Beispiel hierfür ist das Tallinn-Handbuch, ein Leitfaden für Politikberater und Rechtsexperten über die Anwendung des geltenden Völkerrechts auf Cyberoperationen. Gleichzeitig organisiert das CCDCOE «Locked Shields», eine der weltweit grössten Verteidigungsübungen im Bereich Cyber. Im Jahr 2022 nahmen mehr als 2000 Experten aus 32 Ländern daran teil. Die aus Mitgliedstaaten und Partnern gebildeten Teams müssen während der Übung nicht nur

Roland Meier, wissenschaftlicher Projektleiter am Cyber-Defence Campus, präsentiert an der CyCon 2019 die Studie «Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise»

Teilnehmer der «Locked Shields»-Übung arbeitet am «Stromnetz».

zahlreiche komplexe cyber-physische Systeme schützen, sondern auch in der Lage sein, strategische und taktische Entscheidungen zu treffen, Vorfälle zu melden und Herausforderungen in den Bereichen Forensik, Recht, Medienarbeit und Informationskriegsführung zu bewältigen.

Des Weiteren organisiert das CCDCOE die jährliche internationale Konferenz für «Cyber Conflict» (CyCon). Die CyCon hat sich als führende Veranstaltung auf dem Gebiet der Cyberverteidigung etabliert und bringt mehr als 600 Entscheidungsträger und Sicherheitsexperten aus 50 verschiedenen Ländern zusammen. Gleichzeitig trägt die Konferenz zum wissenschaftlichen Diskurs im Bereich Cybersicherheit bei. Der CYD Campus konnte mit bisher elf Publikationen ebenfalls zum wissenschaftlichen Austausch im Rahmen der CyCon beitragen.

William Blonay, Mitarbeiter des CYD Campus und seit Februar 2022 Vertreter der Schweiz am CCDCOE, hat unter anderem ebenfalls an der «Locked Shields»-Übung im April 2022 teilgenommen. Im folgenden Interview spricht er über seine Erfahrungen und gibt einen exklusiven Einblick in seine Tätigkeiten beim CCDCOE.

Interview mit William Blonay

Wie kam es, dass du zum Vertreter der Schweiz am CCDCOE ernannt wurdest?
Ausgangspunkt war mein Hochschulpraktikum beim Cyber-Defence Campus in Lausanne zum Abschluss meines Masterstudiums in Ingenieurwissenschaften. Während meines Praktikums beim Cyber-Defence Campus stellte ich fest, dass mir die Arbeit sehr gut gefällt und ich mich gerne über mein Praktikum hinaus mit Cyber-Defence beschäftigen möchte. An dieser Stelle bot sich die Gelegenheit, die Vertretung der Schweiz beim CCDCOE zu übernehmen, was sowohl meinen Fähigkeiten als auch meinen Interessen entsprach. Seit Februar 2022 bin ich nun der Vertreter der Schweiz in Tallinn.

Welches sind deine Aufgaben und Verantwortlichkeiten innerhalb des CCDCOE?
Als Forschende am CCDCOE erhalten wir von den Mitgliedsstaaten verschiedene Aufgaben im Bereich Cyberverteidigung, die in Form von Forschungsprojekten, Übungen und Kursen in allen Kompetenzbereichen durchgeführt werden. Im Rahmen dieser Projekte bin ich im Kompetenzbereich Technologie angesiedelt. Konkret bin ich unter anderem an 5G-Sicherheit-Forschungsprojekten und an den Übungen «Locked Shields» und «Crossed Swords» beteiligt und gehöre ebenfalls zu den zukünftigen Ausbildern für verschiedene Kurse im Bereich der Schwachstellen-Forschung.

Kannst du die «Locked Shields-Übung» und deine Rolle darin erläutern?
«Locked Shields» ist eine jährliche Übung, die seit 2010 vom CCDCOE organisiert wird und Cybersicherheitsexperten aus verschiedenen Ländern ermöglicht, ihre Fähigkeiten zur Verteidigung nationaler IT-Systeme und kritischer Infrastrukturen bei Echtzeit-Angriffen zu verbessern. Bei den Vorbereitungen für die Übung und während der Durchführung kann zwischen drei verschiedenen Teams unterschieden werden: Das grüne Team entwickelt, konzipiert und implementiert die Systeme. Das rote Team sucht nach Schwachstellen in diesen Systemen, mit dem Ziel, sie anzugreifen. Und zuletzt verteidigt das blaue Team die Systeme bei Angriffen. Im Jahr 2022 umfasste die Übung insgesamt 5500 virtualisierte Systeme, auf die mehr als 8000 Angriffe durchgeführt wurden. Die ganze Übung dauerte zwei Tage.

William Blonay, Mitarbeiter des CYD Campus und Vertreter der Schweiz am CCDCOE in Tallinn.

Meine Aufgabe im grünen Team bestand darin, ein 5G-System für die Übung «Locked Shields» zu entwickeln. Während der Übung wechselte ich dann in das rote Team, um dasselbe System anzugreifen, das ich zuvor im grünen Team entwickelt hatte.

Wie funktioniert die internationale Zusammenarbeit innerhalb des CCDCOE?
Jeder teilnehmende Staat entsendet eine oder zwei Personen ans CCDCOE und stellt dafür ein bestimmtes Budget zur Verfügung. Im Gegenzug kann jede Nation dem CCDCOE Projekte vorschlagen, die durchgeführt werden, sofern die anderen Mitgliedsnationen zustimmen. Auf diese Weise arbeiten die verschiedenen Repräsentanten an gemeinsamen Projekten, was wiederum den Zugang zu internationalem Fachwissen ermöglicht.

Weshalb ist es wichtig, dass der CYD Campus mit dem CCDCOE zusammenarbeitet?
Die Zusammenarbeit zwischen dem CYD Campus und dem CCDCOE bietet die Chance, auf internationales Expertenwissen zuzugreifen und neue Kompetenzen im Bereich der Cyberverteidigung zu erschliessen. Im Rahmen meines bisherigen neunmonatigen Engagements am CCDCOE kann der CYD Campus von technischem Fachwissen über 5G, Netzwerke und der Schwachstellen-Forschung profitieren. Darüber hinaus hat diese Zusammenarbeit die Entwicklung eines 5G-Labors auf dem CYD Campus ermöglicht.

Welchen Beitrag leistet deine Vertretung in Tallinn und was trägt diese zur Cyberverteidigung der Schweiz bei?
Die multilaterale Partnerschaft trägt dazu bei, dass die Schweiz stets am Puls der Cyberabwehrforschung ist und sich innerhalb der Cyber-Community vernetzen kann. Die Schweiz erhält durch die internationale Zusammenarbeit auch Zugang zu wertvollen Daten und Forschungsergebnissen, die sie für ihre eigenen Projekte nutzen kann. Estland ist ebenfalls ein sehr fortschrittliches Land im Bereich der Cybersicherheit, weshalb die Nutzung von Synergien und die Netzwerkbildung für die Schweiz sehr interessant sind. Darüber hinaus ermöglicht die Kooperation Synergieeffekte zwischen der multilateralen und der nationalen Ebene.

Welches waren deine bisherigen Höhepunkte beim CCDCOE?
Ich würde sagen, meine Teilnahme an «Locked Shields» 2022 als Mitglied des grünen und des roten Teams im Bereich 5G war das absolute Highlight. Aber auch die verschiedenen Bekanntschaften und der Austausch innerhalb des CCDCOE haben mich persönlich stark weitergebracht.