School of Computing Queen's University

January 2022
Volume 1, Issue 2

Inside this issue:

Partners in Crime—Combining the Best of 2 Worlds

Queen's University & the Royal Military College (RMC)—an ideal partnership that trains students to protect our democracy, our infrastructures and our daily lives.

Few academics conduct research in cybersecurity and train HQP to innovate in operational cybersecurity in banks, government, healthcare, critical infrastructure, and businesses that operate in online environments. There is also limited capacity to educate the public to safely navigate an online world and to provide technical background to the media.

The partner list of the Smart Cybersecurity Knowledge Mobilization Network SERENE-RISC contains almost every academic with an interest in cybersecurity in Canada and numbers only 48 individuals.

Some research institutes focus on cybersecurity and several universities offer graduate courses, but there are limited graduate training opportunities in the field apart from a world-class program at the Royal Military College (RMC), which has historically admitted few civilians, until now.

Joining forces with RMC to create an "army" of cybersecurity experts, will reduce and eliminate the exponential number of cyber attacks and cyber crime that destroys our way of life. As even the most minute details of our lives now involve the internet, from our social communications to our banking to our election processes, being able to strategically deter the efforts to undermine and destroy our systems, is absolutely crucial . . . unless, of course, we want to move backwards in time.

Dr. Christian Leuprecht, Professor, Royal Military College & Queen's University, CREATE Cybersecurity Program

> ***"We're here to put a dent in the universe. Otherwise why else even be here?" ~Steve Jobs***

A CREATE Cybersecurity Education = Dream Job

Kathryn Fizzell, Experiential Learning Strategist, Career Services

Career Learning Strategists with a VISION – Kathryn Fizzell and Lilith Wyatt, Experiential Learning Strategists at Queen's **Experiential Learning Hub,** assist our students in visualizing and obtaining their future dream position in the world of cybersecurity, beginning with a pre-briefing internship workshop that lays the foundation for the ultimate path of success to reach their future career goals.

The Internship Process: Supervisors canvass their students to find out what research/interests/background they are interested in pursuing for their internship. The supervisors then reach out to their private and public sector contacts to find an internship that will benefit both the student and the host organization. (A select number of students will connect and confirm their internship with a cybersecurity organization without the assistance of their supervisor.) This process begins 7 to 8 months before the internship begins to ensure that our students and hosts are well matched and to complete any lengthy security clearances that are required by many of our host organizations.

In the early spring, the **Experiential Learning Hub** prepares and delivers a pre-briefing internship workshop in order to give our students a preview of what an internship entails, the host's expectations and the student's expectations with respect to what they wish to learn/acquire. In addition, the EL Hub explains that the purpose of the internship is to not only apply their learned skills and acquire new ones, but it also sets up the possibility of a career opportunity following graduation.

Following the student's internship, a post-briefing workshop is offered to reflect on the knowledge and experiences gained throughout the internship. A host survey requesting a commentary on the performance of the student and a student survey allows our students to comment on their experiences and offer suggestions on how to improve the internship process for future students.

These workshops are specifically designed to help students be more intentional and proactive during their internship to achieve a high performance and become more reflective of the payoffs afterwards—securing their dream job while still working towards becoming a CREATE Cybersecurity graduate.

The Canadian government assessed that Russian intelligence services and law enforcement almost certainly maintain relationships with cybercriminals, either through association or recruitment, and allow them to operate with near impunity—as long as they focus their attacks against targets located outside Russia and the former Soviet Union.

It is very likely that cyber criminals will increasingly demand ransom payments in privacy coins, such as Monero, to further conceal their identity and obfuscate their

Advisory Board HIGHLIGHTS—May 26, 2021

Dr. Skillicorn presented an overview of the CREATE Cybersecurity program that included:

Program Development	Course Development
PhD programs at Queen's University and at Royal Military College (RMC)	**CISC866 Introduction to Cybersecurity (Queen's University, core course)**
MSc by research at Queen's University	**MPA 535, 591, MBA 503** (RMC, one required by all students)
MASc by research at RMC	**CISC8xx Cryptography**
Master's of Public Administration at Queen's University and at RMC	**CISC850 Cyber-physical system security**
	CISC878 Cyberspace, data analytics, and policing
	ELEC877 AI for Cybersecurity

HQP Training by Project Year and HQP Category:

	U/G Interns	Master's	PhD	MPA
2018		2	3	0
2019	2	4	1	1
2020	2	4	1	1
2021		8	0	0

Over 80% of NSERC CREATE Cybersecurity's funding is distributed to our Master's and Ph.d students.

Student Presentation:

Lama Moukahal, a Ph.D CREATE student was commended by the board members on her professional and enlightening presentation entitled: **"Cybersecurity and the Connected Autonomous Vehicles"** concluding with **"the Way Forward:** *how to keep drivers safe from cyber attacks"*. Together with Lama's supervisor, Dr. Mohammad Zulkernine, two patents were submitted and published in IEEE Transactions on "**Vulnerability-Oriented Fuzzy Testing for Connected Autonomous Vehicle Systems".** Due to Lama's compelling presentation, a board member suggested that perhaps in the future, more students could offer presentations on their research related to cybersecurity.

Discussion:

From a program perspective, a board member felt that only one MPA student per year was insufficient to cover the ground in the sociology/human behaviour aspect of cyber criminals. He stated that this area is of concern and expressed great interest in acquiring more knowledge to fill this gap as we move forward in the program. Dr. Skillicorn responded with "unfortunately, the budget only supports one student as per the NSERC guidelines, however, since there is a demand by the students, we should explore ways to work around this requirement". A board member acknowledged the issue and said that he would be interested in pursuing other options to increase the number of students. Dr. Skillicorn felt that the partners would carry more influence in the expansion of this shortage of non-NSE students. Outcome: as a result of the board member's suggestion on the expansion of attracting more non-NSE students into the program, Dr. Skillicorn followed his advice and reached out to his contacts that resulted in 5 MPA students, supervised by Dr. Christian Leuprecht, joining the program in September 2021. Interestingly, all 5 students were women, thus boosting the NSERC requirement of 40% of women candidates to a total of 12, well surpassing the 40% requirement.

In closing:

Dr. Skillicorn thanked the CREATE Cybersecurity Board Members for their participation and requested feedback from the board *"whose role is to keep us honest and help us point our radar in the right direction, since our partners are the drivers of our program and potentially the ones that will be hiring our graduates".*

Professor Art Cockfield
CREATE Cybersecurity
Co-Contributor

Remembering Professor Art Cockfield:

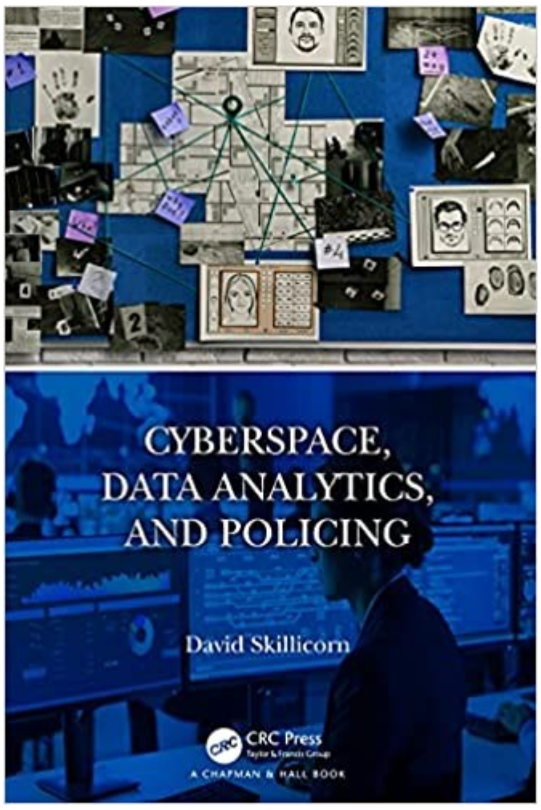
The CREATE Cybersecurity community is remembering Professor Art Cockfield, one of our co-contributors, and one of the world's leading tax law scholars, a highly esteemed and cherished teacher, mentor, colleague, and friend. He died unexpectedly on January 9 from an unsuspected heart condition. He was 54.

"Art Cockfield has left an indelible imprint on laws and policies in Canada and around the world, as well as on the Queen's Law community members near and far who've known him from student to professor," says Dean Mark Walters. "His work on comparative and international tax law was truly innovative and extremely influential. He was a mainstay of our law school, a loyal and dedicated teacher who cared deeply for his students, and a cherished mentor and friend to so many of us."

Colleagues, alumni, friends, and family have come together to establish **the Professor Arthur Cockfield Memorial Award in Law**, which will provide support for Queen's Law students with demonstrated financial need and academic achievement. Contributions may be made online.

Publications—*Nov. 18, 2021*

Cyberspace, Data Analytics, and Policing – David B. Skillicorn



Cyberspace is changing the face of crime. For criminals it has become a place for rich collaboration and learning, not just within one country; and a place where new kinds of crimes can be carried out, and a vehicle for committing conventional crimes with unprecedented range, scale, and speed. Law enforcement faces a challenge in keeping up and dealing with this new environment.

The news is not all bad – collecting and analyzing data about criminals and their activities can provide new levels of insight into what they are doing and how they are doing it. However, using data analytics requires a change of process and new skills that (so far) many law enforcement organizations have had difficulty leveraging.

Cyberspace, Data Analytics, and Policing surveys the changes that cyberspace has brought to criminality and to policing with enough technical content to expose the issues and suggest ways in which law enforcement organizations can adapt.

2nd Annual Tabletop Exercise

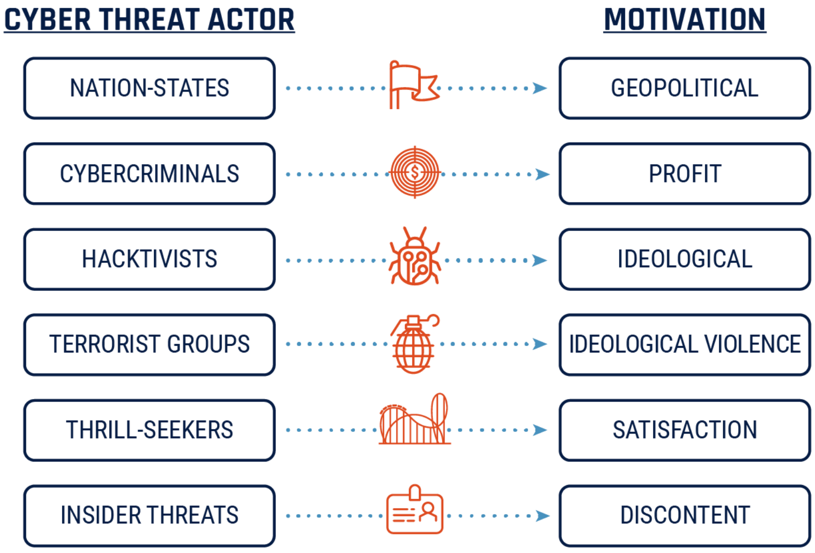
September 2nd, 2021

CREATE Cybersecurity students played the roles of senior representatives from government and industry in the Tabletop Exercise, simulating the actions of the Government of Canada Cyber Security Event Management Plan in response to a cyber attack.

Dr. Skillicorn presented the cyber incidents and breaches that quickly escalated into a potential world crisis. Working as a team, the students methodically and swiftly worked out an immediate response to thwart the perpetrators' attacks, bringing the expertise of their particular unit to deal with the emerging cyber disaster.

Dr. David Skillicorn, CREATE Supervisor, presenting the Tabletop Exercise

A pre- and post-brief helped participants to plan and reflect on their own performance and that of the group. The tabletop exercise integrates everything learned in courses, research, and internship to face a real-world problem.



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

The increased impact and scale of ransomware operations from 2019 to 2021 has been largely fueled by the growth of the Ransomware-as-a-Service (RaaS) business model, by which developers sell or lease ransomware to other cybercriminals.

PROUD TO ACKNOWLEDGE OUR GRADUATES

Dr. Mohammad Zulkernine, CREATE Supervisor

AAWISTA

CHAUDHRY

LAMA

MOUKAHAL

Dr. Mohammad Zulkernine, CREATE Supervisor

CREATE Cybersecurity Testimonial

by Scarlett Taviss

I found the CREATE program to be a very easy way to learn the essentials of the cybersecurity field, especially as a newcomer to this side of the IT world like I was.

Having graduated, I find the required cybersecurity courses in the program follow very similar education topics that many of the key certifications cover, giving me peace of mind that the material I learned was relevant and useful in the real world.

I really enjoyed the ability to take courses at RMC because it allowed me to specialize and gain hands-on experience into some more technical topics within cybersecurity that I was interested in.

I was able to find a position in the field while I was finishing my degree and although every job will be different, the CREATE program definitely gave me a good foundation of cybersecurity knowledge so that I was comfortable entering the industry after graduation.

40% of CREATE Cybersecurity students & graduates are women.

AAWISTA

CHAUDHRY

CREATE Cybersecurity Testimonial

by Aawista Chaudhry

I was admitted into the NSERC Cybersecurity CREATE program's Master's thesis stream in 2019 and graduated in 2021. This was following my successful completion of a "qualifying year" within Queen's University School of Computing. This program offers students from a multitude of backgrounds (such as my bachelor's degree in Chemical Biology) to complete a one-year "accelerated undergraduate" program and garter the necessary foundational skills in computer science. Coming in with no coding experience, this program taught me multiple programming languages, algorithms, and data structures, allowing me to successfully complete my Master's degree.

The NSERC Cybersecurity CREATE program consisted of a mix of academic and experiential learning that facilitated my transition into cybersecurity as a career. There were many interesting academic courses that provided the necessary foundations in technical and theoretical cybersecurity concepts. The program covered multiple areas such as forensics, policy, malware, incident response and network security, offered both at Queen's University and Royal Military Collage. I worked closely with my professors to customize my course deliverables to my research area of interest. The professors were always accessible and very well connected within the field. This allowed me to build upon my knowledge base and simultaneously work towards completing my thesis-based Master's.

The strong emphasis placed on experiential learning experiences throughout the program was highly useful. Developing business (soft) skills was facilitated through various workshops, seminars and courses that taught communication, presentation, and writing skills. A tabletop exercise was also conduced in partnership with IBM to simulate a cyber incident, and we played roles of various government bodies to understand how Canada would respond to a cyber incident. This high-pressured scenario was one of my fondest experiences in the program.

The final component of the program involved doing an internship within the industry, which I completed with Deloitte Canada. My learning experiences from the program immediately benefitted me in performing as a Cybersecurity Consultant. The program positioned me to quickly grasp new frameworks and concepts, and hit the ground running during my time with Deloitte.

Overall, the NSERC Cybersecurity CREATE program provides a unique opportunity for individuals from diverse backgrounds looking to transition into a cybersecurity career. Being one of the first of its kind, it provides the necessary learning to become a well-rounded cybersecurity professional within any specialization.

CREATE Cybersecurity Student Achievement

AMIN

FAKHERELDINE

Detecting Intrusions in Communication-Based Train Control Systems was accepted in the International Conference on Communications 2022. It proposes an intrusion detection system (IDS) based on Machine Learning techniques to detect attacks on traction and braking operations transmitted on the in-train networks.

The IDS is integrated in the infrastructural components placed at the side of the railroad because they receive status information about all trains. Therefore, they have the ability to detect intrusions by processing and analyzing the received information.

UPCOMING EVENTS—2022

Canadian Women in Cybersecurity 2022 March 8th, 2022 @ 7:30am EST - March 9th, 2022 @ 5:30pm EST Toronto, Ontario	7th Annual Big Data and Analytics March 22nd, 2022 Toronto, Ontario
11th Computer Science On-line Conference (CSOC) 2022 April 26th, 2022 Toronto, Ontario	IAPP Canada Privacy Symposium 2022 May 26th, 2022 Toronto, Ontario
36th AAAI Conference on Artificial Intelligence 2022 February 22—March 1, 2022 Vancouver, B.C.	Women in AI Dinner 2022 October 18th, 2022 Toronto, Ontario
11th International Conference on Cryptography and Information Security (CRYPIS 2022) July 23rd, 2022 Canada » Toronto	World Summit Americas 2022 May 4th, 2022 Montreal, Quebec

STAY TUNED for the 2nd annual GOOGLE sponsored CSR Event beginning in the spring for female identifying students!

The NSERC CREATE Medical Informatics & the NSERC CREATE Cybersecurity programs are 2 of only 98 projects across all of Canada endorsed by the Natural Sciences & Engineering Research Council (NSERC). These 2 programs, hosted by Queen's University and depicting "***the experimental spirit of the modernist vanguard***", deliver profound ground breaking knowledge and experiences that exponentially advances and protects humanity.

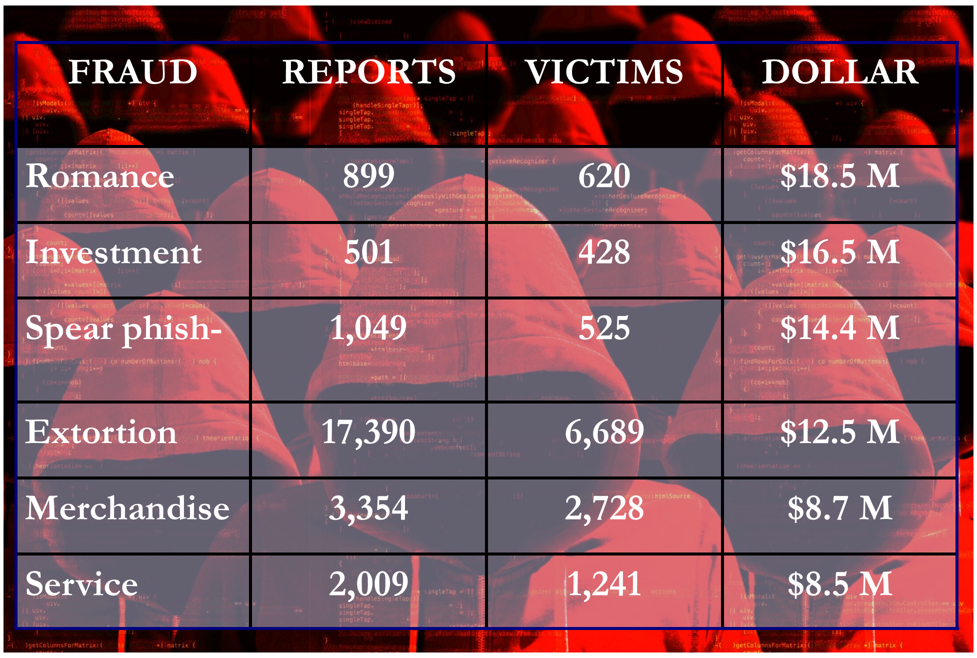
Beginning in May 2022, summer internships in the areas of Medical Informatics and Cybersecurity will be offered to a a select number of undergraduates across Canada interested in learning and contributing towards these 2 exclusive areas of research.

IN CLOSING . . . by Dr. David Skillicorn

Despite the continuing impact of covid, and the uncertainties that it creates, we are on track with student numbers, and have managed to offer all of the components of the program in virtual and online ways. The largest group so far are going on internship with our partners this summer.

As well as the components that we promised NSERC we would use to enrich the student experience, we have a number of interesting synergies that you have read about above. So, in difficult times, we are not only on track, but we are doing well.

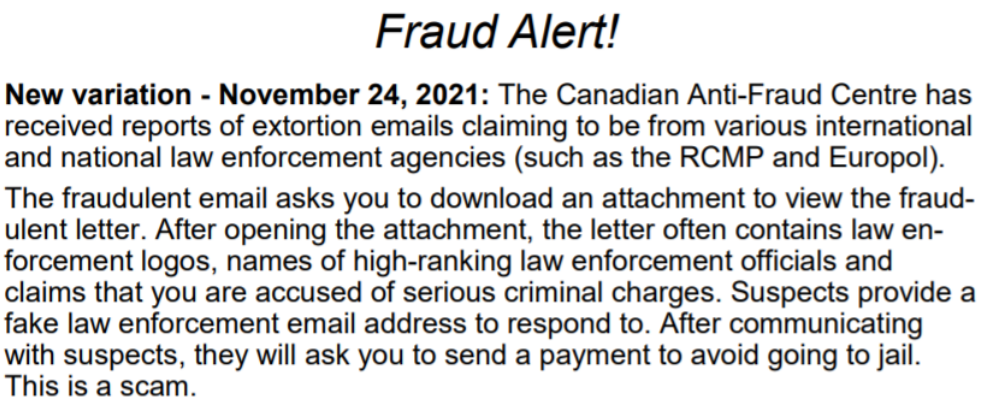
Cyber Attacks in Canada—2020



FRAUD	REPORTS	VICTIMS	DOLLAR
Romance	899	620	$18.5 M
Investment	501	428	$16.5 M
Spear phish-	1,049	525	$14.4 M
Extortion	17,390	6,689	$12.5 M
Merchandise	3,354	2,728	$8.7 M
Service	2,009	1,241	$8.5 M

Source: CAFC

Romance fraud resulted in higher total losses than any other type of fraud. 620 victims lost a total of $18.5 million (CAD) to romance and dating scams. It is thought that between January and September 2021, the amount swindled out of Canadians via Romance scams added up to $32 million CAD.



Fraud Alert!

New variation - November 24, 2021: The Canadian Anti-Fraud Centre has received reports of extortion emails claiming to be from various international and national law enforcement agencies (such as the RCMP and Europol).

The fraudulent email asks you to download an attachment to view the fraudulent letter. After opening the attachment, the letter often contains law enforcement logos, names of high-ranking law enforcement officials and claims that you are accused of serious criminal charges. Suspects provide a fake law enforcement email address to respond to. After communicating with suspects, they will ask you to send a payment to avoid going to jail. This is a scam.

Source: https://www.antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-eng.htm

Since March 2020, nearly a quarter of Canadian small businesses—many of which were forced to increase their use of online platforms during the COVID-19 pandemic—experienced some type of malign cyber incidents. The federal government assessed this amount likely to be higher than reported.

Test your Cybersecurity KNOWLEDGE

See answers below

1.

What is a "zero day" attack?

A An attack that happens before developers have a chance to address

B A hack that affects companies for less than one day

C An attack that takes less than a day to complete

D ¯\_(ツ)_/¯

2.

About how big is the global cybersecurity market estimated to be, in dollar terms?

A 1 trillion

B 700 billion

C 200 billion

D 10 billion

3.

What's the name of the company that licenses the spyware responsible for breaching iPhone's defenses on behalf of multiple governments?

A Anonymous

B DarkSide

C SpyFone

D NSO Group

4.

A Microsoft exec recently called which cyberattack the "largest and most sophisticated ever"?

A Colonial Pipeline

B 2020 Twitter Hack

C SolarWinds

D JBS Foods

5.

After breaking into crypto platform Poly Network and stealing more than $600 million in digital currencies, the hackers gave back the money.

True or False

Answers:

1. **A** An attack that happens before developers have a chance to address

2. **C** 200 billion

3. **D** NSO Group

4. **B** 2020 Twitter Hack

5. **TRUE** After breaking into crypto platform Poly Network and stealing more than $600 million in digital currencies, the hackers gave back the money.

Source: https://www.morningbrew.com/emerging-tech/stories/2021/09/15/tech-trivia-cybersecurity

OUR STUDENT INTERNSHIP HOSTS

Royal Canadian
Mounted Police

amazon

irdeto

BOMBARDIER

Deloitte.

NUNTIUM · COMPARAT · ET · CUSTODIT

COMMUNICATIONS
SECURITY ESTABLISHMENT
CENTRE DE LA SÉCURITÉ
DES TÉLÉCOMMUNICATIONS

RBC®

NCR

OUR CREATE PROGRAM PARTNERS

NSERC
CRSNG

COLLÈGE MILITAIRE
ROYAL DU CANADA
ROYAL MILITARY
COLLEGE OF CANADA

TRUTH · DUTY · VALOUR
VÉRITÉ · DEVOIR · VAILLANCE

NUNTIUM · COMPARAT · ET · CUSTODIT

COMMUNICATIONS
SECURITY ESTABLISHMENT
CENTRE DE LA SÉCURITÉ
DES TÉLÉCOMMUNICATIONS

Royal Canadian
Mounted Police

National Défense
Defence nationale

IBM®

irdeto

Public Safety Canada
publicsafety.gc.ca

Treasury Board of Canada
Secretariat

EXPERIENTIAL
LEARNING HUB

Queen’s University
School of Computing

NSERC
CRSNG
CREATE Cybersecurity

Goodwin Hall
25 Union Street

Phone: 613-533-6050
Fax: 613-533-6513
Email: cyber-info@cs,queensu.ca

www.cyber.cs.queensu.ca

A program offered by Queen’s University and the Royal Military College of Canada