

## Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity

[Canadian Centre for Cyber Security](#) | May 26, 2020

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the Canadian Centre for Cyber Security (CCCS)'s knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. CSE's foreign intelligence mandate provides us with valuable insight into adversary behavior in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our key judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

<https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity>

## 2020 Annual Security Refresher Training

Please don't wait until the end of 2020 to complete this required training!

The **REQUIRED** 2020 Annual Security Training is being offered on-line at this current time. ORS is hoping we can offer in person presentations this fall. April McMeans will be sending emails starting May 1. Once you receive your email, you can then move forward with completing your refresher training.



## COVID-19 NEWS: Defense Department Must Keep R&D On Track

By: [Connie Lee](#) | National Defense Magazine | April 15, 2020

The COVID-19 pandemic can't put a stop to the Navy's research and development enterprise, a senior service official said April 15. "We're already amending some of our business processes, things where we were taking perhaps more time than we needed or not aggressively going after something as [much as] we could," Assistant Secretary of the Navy for Research, Development and Acquisition James "Hondo" Geurts said during the Navy's League's Sea-Air-Space conference, which is being held virtually this year because of safety concerns surrounding COVID-19. The Navy is "understanding how to collaborate better as opposed to having duplicating functions."

The Defense Department is speeding up early research-and-development efforts by working closely with academia and switching to a distributed research model, which will allow multiple organizations to work on initiatives more easily, he said.

"The big industrial initiatives are definitely important, but so are the small research-and-development ones," he noted. The Navy hopes to "speed up cash flow" for R&D efforts by possibly awarding contract awards for Small Business Innovation Research grants earlier than expected, he noted.

"What we can't afford to do is take a year or two off of research and development, lose those key performers because they are key to our readiness five and 10 years from now," he said. "We're looking to be as aggressive with them, if not more so, than we are with our more traditional defense partners."

<https://www.nationaldefensemagazine.org/articles/2020/4/15/coronavirus-to-have-lasting-impact-on-defense-acquisition>



## The Continuing Danger of Academic Espionage

By: [Suzanne Folsom and Robert Garretson](#) | Inside Higher Ed | May 5, 2020

Enviied the world over, U.S. institutions of higher learning have taught millions of undergraduate and graduate students, nurtured scores of scientists and entrepreneurs, advanced medical science, and incubated many leading technology companies -- all of which makes them top targets for foreign intelligence services and nongovernmental actors. As America and the world start to reopen for business, and college and university leaders are rightly focused on the safe and healthy reintroduction of students and faculty members to campuses, the perfect opportunity for the resumption -- and, more likely the acceleration -- of widespread academic espionage has materialized. College and university leaders will lack the time, attention and potentially the budget to zero in on this critical issue. But this is exactly the time for the greater higher education community to strengthen its commitment to ensuring that adequate controls and monitoring are in place to stem the tide of academic espionage.

<https://www.insidehighered.com/views/2020/05/05/threat-academic-espionage-should-not-be-overlooked-even-time-pandemic-opinion>

### **OFFICE OF RESEARCH SECURITY STAFF**

**DENISE SPILLER**

Security Administrator

824-6444

denise.spiller@uah.edu

**JANINE WILSON**

Associate Security Administrator

824-3025

janine.wilson@uah.edu

**APRIL MCMEANS**

Assistant Security Administrator

824-6048

april.mcmeans@uah.edu

**CAITLYN SCHOENIG**

Security Assistant

824-4717

caitlyn.schoenig@uah.edu

**RYAN WILKINSON**

Student Specialist I

824-4818

ryan.wilkinson @uah.edu