Cyber warriors sound warning on working from home

October 14 2020, by Polina Kalantar

'Large scale use of remote work has attracted spies, thieves and thugs,' says Jaak Tarien, head of NATO's Cooperative Cyber Defence Centre of Excellence

Cyber warriors on NATO's eastern edge are warning that the growing number of people working from home globally due to the pandemic is

increasing vulnerability to cyber attacks.

The Baltic state of Estonia hosts two cyber facilities for the Western military alliance—set up following a series of cyber attacks from neighbour Russia more than a decade ago.

"Large scale use of remote work has attracted spies, thieves and thugs," Jaak Tarien, head of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), told AFP in an interview.

The increased amount of information travelling between institutional servers and home networks is creating new challenges for employers.

"Tackling these new challenges is complicated and requires a lot of resources as well as a different kind of approach," Tarien said.

"We are likely only scratching the surface in assessing the magnitude of malicious activities taking place in the COVID-era busy cyberspace."

An EU-wide survey in September found that around a third of employees were working from home.

Boom in online courses

The concerns are echoed at NATO's Cyber Range—a heavily-guarded facility protected by barbed wire in the centre of the capital Tallinn run by Estonian defence forces.

The NATO Cyber Range CR14 centre was set up after a series of cyber attacks on Estonian websites in 2007

The server rooms inside serve as a platform for NATO cyber security exercises and training.

"Specialists have set up the work infrastructure, but they cannot control the way people use their home internet or how secure it is," said Mihkel Tikk, head of the Estonian defence ministry's cyber policy department.

Tikk said the latest cyberattacks have targeted Estonia's health sector and Mobile-ID—the mobile phone based digital ID.

The coronavirus pandemic has also affected operations at the cyber

facilities themselves, forcing the cancellation of offline exercises.

But the NATO Cyber Defence Centre said the silver lining is the growing popularity of the cyber security courses it is putting online.

The online courses include "Fighting a Botnet Attack", "Operational Cyber Threat Intelligence" and "IT Systems Attack and Defence".

There were 6,411 students by September 1 and the centre is aiming for 10,000 by the end of 2020.

'A massive mistake'

The Cyber Defence Centre was set up following a series of cyberattacks of unprecedented sophistication on Estonian websites in 2007.

The unit's base in Tallinn, Estonia, is heavily guarded

The Russian pro-Kremlin youth organisation Nashi later claimed responsibility.

These days, Estonia faces a "continuous flow of attacks" and repelling them requires constant work, Defence Minister Juri Luik told AFP.

But he said the country was in "a pretty good situation" since it has had time to learn from past experience.

"We have worked diligently to guarantee that the computer networks are difficult to break in and the communication is encrypted –- both military but also civilian communication.

"So I think it is relatively more difficult to harm Estonia than many other countries who perhaps are not so used to working via cyberspace and haven't given too much attention to cyber defence," he said.

The minister underlined that all this work would be for nothing without basic cyber hygiene, including password protection.

"This is extremely important and should be remembered—especially now that many people work from home via computer.

"At home you might let your guard down and that's of course a massive mistake."