GOVERNMENT

Australia and Portugal join NATO cyber cooperative

Estonian Defense Forces raise the Portuguese flag at CCDCOE headquarters commemorating the nation joining the group. (Photo: Estonian Defense Forces)

Zaid Shoorbajee Apr 23, 2018 | CyberScoop

A NATO-backed group that's designed to coordinate international cybersecurity efforts is getting two new members: Australia and Portugal.

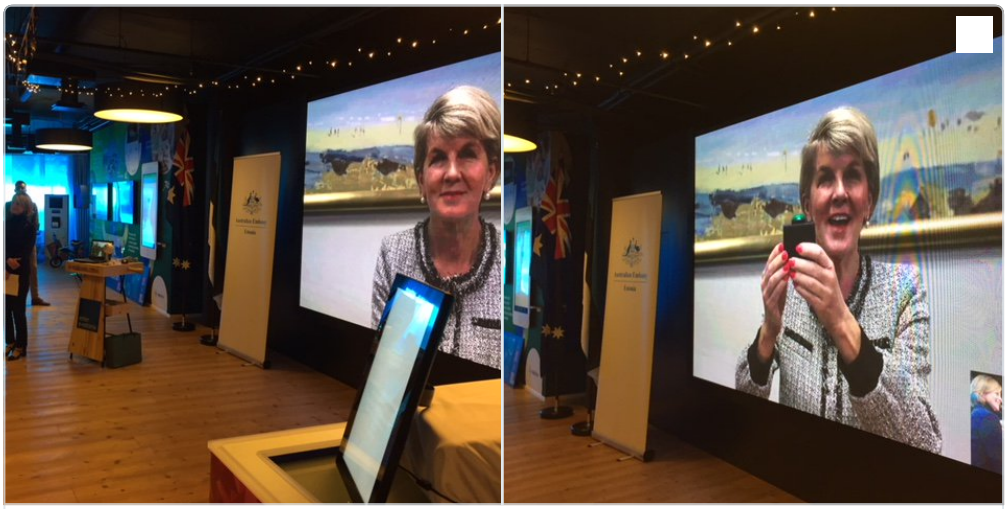
The two countries will join the Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn, Estonia, according to separate announcements on Monday. The organization acts as a think tank for the development of global cyber norms, cybersecurity training requirements and also helps communicate goals shared between different countries.

"We are glad to welcome Portugal, another strong NATO Ally joining the Centre. CCDCOE offers a unique opportunity for all NATO Allies to practice together new interdisciplinary approaches in cyber defence," Merle Maigre, director of CCDCOE, said in a statement.

The CCDCOE is known for hosting cyber warfare training simulations that are intended to build relations between member countries.

Of Australia joining the group, Maigre said: “Accession of Australia expands the reach and cooperation of like-minded nations in cyber defence beyond the Euro-Atlantic area, making our cyber defence hub truly global.”

Australia’s membership in CCDCOE will be supported by a pop-up embassy that the country opened in Tallinn on Monday. The country doesn’t have a permanent embassy in Estonia and currently operates its diplomatic mission through a consulate and its embassy in Sweden.



NATO CCD COE
@ccdcoe

Australia is joining @ccdcoe, Australia´s FM @JulieBishopMP @dfat just announced at the opening of their pop-up embassy in Tallinn that Only a year ago @JulieBishopMP visited #LockedShields Warm welcome to our family of like-minded nations!

12:57 PM - Apr 23, 2018

70 47 people are talking about this

“Australia welcomes the opportunity to deepen engagement with the world-leading cyber defence experts at the NATO CCDCOE,” Australian foreign minister Julie Bishop said in a statement. “Now, more than ever, we must engage with the international community to set clear expectations for responsible state behaviour in cyberspace. The international rules based order applies online, just as it does offline.”

One of the most prominent training exercises organized by the CCDCOE is named “Locked Shields.” The event allows member nations to practice fending off cyberthreats in real-time. The center calls it the “largest and most advanced international technical live-fire cyber defence exercise.”

Australia will be observing this year’s Locked Shields, taking place this week. It’s not clear if Portugal is participating or if they are observing in any way.

The center also maintains a guide on international law as it relates to cyber-operations, known as the Tallinn Manual. CCDCOE released the second version of the manual last year with a focus on international law governing cyber-operations during times of peace.

Australia may stick out from the group because it's not an American or European country. Japan also started taking steps towards joining the CCDCOE in January.

-In this Story-

Australia, ccdcoe, NATO CCD COE, news, portugal

RELATED NEWS

GOVERNMENT

Intel Committee blasts...

by **Zaid Shoorbajee** • 9 hours ago

GOVERNMENT

Amid ongoing geopolitical...

by **Chris Bing** • 17 hours ago

GOVERNMENT

Regulators tightening...

by **Sean Lyngaas** • 2 days ago

GOVERNMENT

Intel Committee blasts FBI for not notifying Russian hacking victims

(Getty)

Zaid Shoorbajee Apr 27, 2018 | CyberScoop

The FBI is catching heat from Congress again.

In a report released Friday by the House Intelligence Committee about their own investigation into Russian interference in the 2016 election, lawmakers argued that the FBI didn't do enough to notify victims that were targeted by Russian cyberattacks.

"The Federal Bureau of Investigation's notification to numerous Russian hacking victims was largely inadequate," the committee wrote. "The Committee is also concerned that many, perhaps even a majority, of Russia's known victims were never contacted by the FBI."

Much of the committee's notes on this subject are redacted, but the panel appears to base its assessment at least partially on reporting from the Associate Press in November 2017. The AP reported that the FBI was aware of Russian hacking group Fancy Bear attempting to break into scores of U.S. officials' Gmail accounts, but only notified a small fraction.

The committee also highlighted the fact that Hillary Clinton campaign staffer Jake Sullivan testified before Congress that he was never notified by the FBI about his email account being targeted.

Aside from failing to notify victims, the committee report states that even when the FBI did reach out, the agency failed to reach a "desired outcome." In other words, law enforcement received no assurances from these targets that they would take future preventative measures to avoid getting hacked again.

The report cites testimony from former FBI Director James Comey, saying that, in hindsight, the agency should have done more to notify potential victims.

"We would have sent up a much larger flare. Yeah, we would have just kept banging and banging on the door, knowing what I know now. We made extensive efforts to notify. I might have walked over know there myself, knowing what I know now," the report quotes Comey as saying.

In the report's recommendations, the committee said that when U.S. critical infrastructure, such as election infrastructure, is the target of foreign cyberattacks, officials should

engage victims on a more elevated level.

"Although the FBI maintained an on going dialogue with the [Democratic National Committee] related to the the Russian intrusions, engagement remained at the-working level. These interactions continued for months, despite no signs of effective mediation to the problem," the report says.

The committee faults the DNC for not handling the attacks "with the level of seriousness it deserved", but says that the onus was on the FBI to elevate its engagement with the DNC to a more senior level.

"[T]he FBI should update its internal processes to make it clear that if a victim is neither willing nor able to take remedial measures in the event of a significant national security cyber event, FBI leadership should contact the victim and engage at the leadership level," the report says.

-In this Story-

DNC, Fancy Bear, FBI, House Intelligence Committee

RELATED NEWS

GOVERNMENT

Amid ongoing geopolitical...

by **Chris Bing** • 17 hours ago

GOVERNMENT

Regulators tightening...

by **Sean Lyngaas** • 2 days ago

GOVERNMENT

Cops shut down one of the...

by **Chris Bing** • 2 days ago