EU defence ministers put to test in mock cyberattack

September 7 2017, by Damon Wake

NAGO chief Jens Stoltenberg (2ndL) said the alliance had seen a 60 percent increase in cyber attacks on its networks over the last year

A major cyberattack targets European Union military structures, with hackers using social media and "fake news" to spread confusion, and governments are left scrambling to respond as the crisis escalates.

This was the scenario facing a gathering of EU defence ministers in

Tallinn on Thursday as they undertook a exercise simulating a cyber assault on the bloc—the first mock drill of its kind at such a senior level in Europe.

With countries around the world heavily reliant on computers for everything from defence systems to hospital equipment to critical infrastructure such as power stations, the cybersphere is seen as the next major theatre for conflict.

NATO now considers cyberspace to be a conflict domain alongside that of air, sea and land.

Alliance chief Jens Stoltenberg, who attended the exercise in Tallinn, said NATO had seen a 60 percent increase in cyber attacks on its networks over the last year.

In Tuesday's exercise, the 28 EU defence ministers were presented with an escalating crisis during an operation in the Mediterranean Sea similar to the current Sophia naval mission against people-smuggling networks.

"First a drone went down after a problem with the server at the military headquarters, then another drone was intercepted and then a more serious threat with a worm (computer virus)... and then more serious still with the loss of communications with our ships in the Mediterranean," Belgian Defence Minister Steven Vandeput explained.

The ministers were given tablet computers to answer multiple choice questions about how to respond to each fresh development.

"We are not creating programmers from the ministers but we want them to understand that these quickly developing situations could demand quick political decisions—that's the idea of the exercise," Estonian Defence Minister Juri Luik said.

'Exciting' exercise

Estonian officials said the aim was to improve ministers' understanding of the kinds of target that could be hit by a cyberattack, the effects such an attack could have and how they could respond—as well as the need for clear, coordinated communication with the public on what can be a complex issue.

German Defence Minister Ursula von der Leyen said the two-hour exercise was "extremely exciting".

"The adversary is very, very difficult to identify. The attack is silent, invisible... it is cost-effective for the adversary because he does not need an army, but only a computer with internet connection," she said.

Estonia has made digital issues one of the priorities of its EU presidency, which runs until the end of this year, and Thursday's exercise was over a year in the planning.

Leyen said the drill showed the importance of "informing each other and to include the economy in case a major cyber attack spreads in critical infrastructure of the EU economy".

Russian threat

The devastating WannaCry ransomware attack that hit more than 200,000 users around the world in May, causing chaos in Britain's National Health Service and halting production at numerous factories, was a stark signal of hackers' power to wreak havoc.

But NATO and the EU are also on their guard against Russia deploying so-called hybrid tactics—combining cyber warfare and misinformation

as well as conventional boots on the ground—as it did in Crimea to destabilise and ultimately annex a region.

In the last couple of years Lithuania and Latvia have warned they were coming under hybrid attack, accusing Moscow of waging a propaganda campaign to sow dissatisfaction among ethnic Russians in their territory.

Estonia itself was hit as far back as 2007 by one of the first major cyberattacks, suffering a blistering assault on official state and bank websites. The onslaught was blamed on Russian hackers, though the Kremlin denied involvement.

While getting ministers to think of cybersecurity at a strategic level was the key aim of Thursday's practice, Estonian officials stressed that proper resilience to hacking requires education across the whole population.

The vast majority of hacking attacks begin with a security breach from human action—someone opening an email attachment or clicking a link that lets a virus infect their computer network.

Tanel Sepp, a senior cyber expert at the Estonian defence ministry, said children should be taught the priniciples of online safety in the same way they are taught to cross the road safely.

Citation: EU defence ministers put to test in mock cyberattack (2017, September 7) retrieved 23 July 2024 from https://phys.org/news/2017-09-eu-defence-ministers-mock-cyberattack.html