Parliamentary Intelligence-Security Forum Webinar

"Artificial Intelligence Security Challenges"

Tuesday, March 23rd, 2021, 10AM US EST

The European Commission defines artificial intelligence (AI) as systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.

The life-changing power of AI is very clear to see.

As a tool, AI will transform any aspect of our lives and the way we organize as a society.

AI could become one of the most powerful technology humans had ever access to.

In the hands of bad actors, AI can become a powerful destructive tool to attack our economies, the democratic values, the rule of law and our defense capabilities.

The benefits and challenges of AI are intensified by the multitude of ways AI can be deployed.

The situation is more complicated by the highly complex nature of modern algorism being probabilistic, data driven and whose internal logic is often extraordinarily difficult to unravel even for seasoned data scientists.

AI's black box or opaque nature creates important trust issues.

We all want AI to be employed in ways to do good in the world and keep the bad actors from interfering.

Like the digital transformation of the world, AI could be a blessing,

However, the long and not successful fight against cybercrime and cybercriminals does not bode well for the chances to keep AI technologies from being used by bad actors.

After so many years, cybercrime and cyberattacks are still commonplace plaquing online users.

A recent security hole at a major software house has demonstrated the weakness of our cyber defenses.

The vulnerabilities created by the security hole were immediately exploited by criminal gangs, rogue state actors and script kiddies globally.

In the US alone an estimated 30,000 organizations are believed to have been hacked by a group from China.

The group was attempting to steal information from US targets, including universities, defense contractors, law firms and infectious-disease researchers.

A recent study from the European External Action Service (EEAS) identified Russia's systematic disinformation campaigns against Germany.

No other EU Member State is attacked more fiercely through disinformation campaigns than Germany.

Since the start in 2015, the EU database on disinformation has collected over 700 cases of Russia targeting Germany.

With AI support Russia's disinformation campaign and the ensuing polarization of society could reach destructive level only comparable to an act of war.

AI-technologies in the hands of bad actors could deal a deadly blow not only to our economies but also to our democratic values, the rule of law and our defence capabilities.

80-90% of all critical infrastructure in western countries is owned and operated by the private sector.

They are the first targets of a hybrid campaign by rogue state actors.

Given NATO's heavy reliance on the private sector to provide logistics and communications capabilities during a crisis, these vulnerabilities can have far-reaching negative effects.

The current unpredictable security environment has led NATO to renew the focus on civil preparedness.

NATO and its member states must be ready for a wide range of contingencies, which could severely impact societies and critical infrastructure.

In the hands of criminal organizations and launderers AI can be a strong facilitator of money laundering and the financing of terror. However, used by good actors, AI could be an extremely effective tool to fight money laundering and the financing of terror as the people from SAS have demonstrated.

Instead of reacting to old and developing threats we need to get ahead of the curve again by developing superior state of the art technologies and prevent their proliferation to our enemies.

It takes a stakeholder approach between politics, administration and the civil society to successfully fight the truly international cross-border threats emanating from rogue state actors.

I would like to thank Congressman Pittenger and the Parliamentary Intelligence-Security Forum for their work to provide expertise and collaboration among Parliamentarians and government officials to tackle the threats that will affect us all.