Colm Keena, Public Affairs Correspondent

IRELAND SHOULD consider becoming involved with a Nato-sponsored centre for cyber defence based in Tallinn, the president of Estonia, Toomas Hendrik Ilves, has said during a visit here.

He said all countries that acquired considerable income from intellectual property, including Ireland, were being subjected to constant economic cyber espionage.

Companies were being "sucked dry" by cyber thieves, who access knowledge that may constitute many years' work and very considerable investment.

"Ireland is probably being raided all the time," Mr Ilves told The Irish Times.

The FBI's top cyber crime investigator, Shawn Henry, has recently cited an instance where an unidentified company had work worth $1 billion (€755,840), which had been developed over a decade, stolen by hackers.

Estonia was one of the first countries to be subjected to a political cyber attack. In 2007 a large number of the country's major sites were subjected to concerted attacks during a period of tense relations with Russia. Because of this, and the extent to which Estonians use the internet, the country has developed a focus on combating cyber fraud.

A year after the cyber attacks on Estonia, seven Nato countries set up the Nato Co-operative Cyber Defence Centre of Excellence in Tallinn. While the centre is under the aegis of Nato, non-Nato countries are also involved.

Mr Ilves said Ireland should become involved. "You are being attacked whether you are neutral or not. All of us countries that develop new products and inventions are at risk."

Western intelligence agencies estimate that information worth up to $1 trillion is stolen annually through cyber crime.

Mr Ilves said countries tended to treat the problem as a defence issue and for this reason don't share information to the extent they should. What was needed was more co-operation between countries, between the private and public sectors, and within the private sector.

He said it was generally known where most of the cyber attacks were coming from, "even down to the dorms in certain universities".

However, with certain countries declining to sign up to international agreements targeting cyber crime, there were limits to what the international community could do about it. (China is outside such international agreements).

"It is hard enough to keep just one step behind" the thieves, he said.

The "bad guys" make huge profits from their activities and can attract some very capable people.

Meanwhile the "good guys" get very well paid jobs in business. This made it very difficult for modern police forces to hire the type of people needed to address the problem.

Estonia has a section of its Home Guard where IT specialists, after they have been subjected to security screening, work on a voluntary basis on developing anti-virus software.

Countries that pay attention and co-operate in the fight against cyber crime would "come out ahead". Those who do not "will lose".

There were "probably no uncompromised computers in the world", he said. The headquarters of Skype, which was founded by four Estonians,was being attacked "around the clock".

Original article here .