Protecting Digital Economies

As world leaders gather at the G8 Summit in Northern Ireland this year, they will be considering and debating some of the most pressing global issues of our time. Some of us that specialise in the cyber space arena hope that they will also have time to address the deeply worrying trends that threaten the economic and social benefits that the Internet can deliver to mankind.

Many nations are only just beginning to understand the strategic importance the Internet can deliver to their future economic stability and growth. Advanced economies have just started to invest in protective measures, but we are all playing catch-up.

The most significant threats to our digital economies that we face collectively fall into two broad categories:

- *Nation States that carry out industrial espionage to steal intellectual property for economic advantage, and,*
- *Organised criminal groups that wage war on businesses and consumers for financial gain*

For the purposes of this article, I will concentrate on the second of these threats.

International Engagement is not working

We all know that online crime transcends national boundaries; that criminal groups and loners who organise and carry out this 21st Century criminality act in a way that allows them to take advantage of the international lethargy that typifies governments' response to this phenomenon.

Governments have been struggling to find ways in which they can collaborate effectively to defeat online crime. Some of the early signs of international engagement have centred around the Council of Europe's Budapest Convention on Cyber Crime. Unfortunately, progress to encourage countries around the world to become signatories or accede to the Convention have been slow, despite great efforts by Council of Europe staff to evangelise the benefits of joining this cyber crime fighting initiative.

The Convention is opposed by many countries that see it as a purely European measure which fails to meet their needs. This view is somewhat disingenuously supported by Russia and China who would prefer to take decades to reach a UN-style Treaty whilst they attempt to introduce measures which would give them control of the Internet in and around their

territories – a concept which is alien to most of the rest of us around the world who want to see a free, open and unregulated Internet, with certain exceptions.

Governments need to find common ground in order to move this global stalemate and inaction to a point where we can start to strike back against online crime which harms all nations, all businesses and, most importantly, billions of citizens around the world.

These common points of interest centre around two of the most prolific Internet activities:

- *The eradication of images and videos of child abuse being shared online amongst paedophile groups*
- *Fraud and criminal financing – which includes funding terrorist operations*

There are a great many superb initiatives which are being undertaken globally to address the first of these vile practices. There exists a common purpose which unites governments, businesses, law enforcement agencies, academia and citizens around the world. We all wish to see children protected and those who would exploit them brought swiftly to justice.

We should use this area of agreement to collaborate on addressing the other key issue which damages all economies around the world – online fraud and the illegal funding of criminal and terrorist activities and operations.

Outlaw Alternative Online Payment Mechanisms & Confiscate the Proceeds of Online Crime

Many of the stakeholders that are successfully addressing the online child abuse issue have colleagues who are engaged in trying to defeat online financially-motivated crime. Billions of dollars are sitting in bank accounts around the world which are the proceeds of online crime. This is where the authorities can strike.

Governments around the world could take two measures that would have a significant and long-lasting effect on the ability of online criminals to secure their ill-gotten gains:

1. *Outlaw alternative payment mechanisms for trading currencies online, and,*
2. *Introduce legislation to confiscate the proceeds of online crime*

As we have seen with the latest US initiative to arrest some of the suspects involved in money laundering through "Liberty Reserve" (a group that ran a US$6 Billion world-wide operation out of Costa Rica), alternative payment mechanisms, such as Bit Coin and a host of others enable criminal and terrorist groups to launder and fund their operations. Governments have the ability right now, to ban these payment mechanisms. At the heart of this initiative is a simple premise – at one end of the transaction, a user must "buy" the"

Internet currency" and at the other end, the criminals must turn the currency into real money. If Treasuries and financial institutions around the world were to block those transactions and permit only legitimate currencies to be used on the Internet through regulated payment service providers and cards (Visa, MasterCard, AMEX etc), the flow of many US$ Billions to criminal groups would be closed down.

Furthermore, if those same countries introduced, if necessary, additional legislation to confiscate the proceeds of such online crime, these funds could be either returned to those who had been defrauded, or used to fund projects which internationally, could bring about a more safe and secure Internet environment for all citizens.

Calling on the EU and USA to take the lead

If we could convince EU leaders and those in the US to take a lead on these initiatives – that would be a huge contribution to making the Internet a safe place in which to transact financially, whilst striking a blow against those who would try to destroy the fabric of our future well-being.

We at the International Cyber Security Protection Alliance (www.icspa.org) stand ready to work with governments who are interested in taking these hugely cost effective and sensible measures.

John Lyons is the Chief Executive of the business-backed not for profit International Cyber Security Protection Alliance (ICSPA) whose remit is to work with governments and law enforcement agencies round the globe, in the fight against cyber crime.