NETWORK BOX
Managed Security Services
Tel: 0800 107 6098

The State of International Co-operation on Cybercrime

Introduction

The 2001 Convention on Cybercrime recognised the need for a unified approach to tackling cybercrime, not just within the European Union (EU), but worldwide. In its preamble, the treaty says:

"…an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters."

The convention, which has since also been signed by non-EU states such as the USA, Canada, South Africa, Montenegro and Japan, was met with some criticism in America, where civil liberty groups raised concerns about the treaty giving the Government a licence to spy on American citizens for foreign governments. Concerns were also raised about dual criminality (which would permit a foreign country to apply for extradition and put an individual on trial), as some nations were permitted to opt out, making the process on-sided.

As Nate Anderson of Ars Technica reported at the time:

"The point here is not that the US is necessarily wrong, but that the Internet has made things complicated."

Cybercrime has not diminished since the introduction of the treaty, and international co-operation can be described as patchy at best. If nations want to stand any chance of bringing down levels of cybercrime, they cannot work in isolation; they have to work with other nations and with the private sector to develop a unified approach to catching and prosecuting these criminals.

One thing is certain, with the UK climbing up the virus charts, the new Government must include fighting cybercrime as one of its main criminal justice policies, as well as push for further reaching, and more effective, international co-operation.

The Current State of International Co-operation

The EU Solution

Since adopting the 2001 Convention on Cybercrime, the EU has attempted to find a unified response against cybercriminals. In 2007 the EU began to formulate policy which would improve the level of co-operation at a policing and political level between member states. Whilst also looking at legal and political co-operation with nations outside the EU. In addition to:

"…awareness raising, training and research will also be essential in attaining our goals. This policy will be effective only if a strong dialogue with industry is put in place."

After a meeting held in November 2007 to discuss next steps, Vice-President Franco Frattini commented that:

"...successful operations such as "Operation Koala" and the global hunt for the "Vico" paedophile depends on regional and international cooperation. The conclusions of today's meeting represent an important step by the EU to establish the cooperative links upon which such success is built."

In short, the 2001 treaty provides a legislative framework, but is clearly not enough.

The innovative nature of computer technology makes developments hard to keep up with, especially for complex and somewhat bureaucratic organisations such as the EU. Facebook was three years away from being launched when the treaty was signed, Twitter five years and the iPhone six. The way people work has changed, with more people working remotely from home, and an increasing number storing their business data in the cloud. These developments have all taken off within the past nine years, whilst the EU has debated, negotiated and legislated to try and find a suitable way to gain international co-operation.

Cecilia Malmström, Member of the European Commission responsible for Home Affairs, made a speech on 12th May 2010 in which she said;

"The attacks on public and private websites in Estonia and Lithuania in 2007 and 2008 were only tip of a burgeoning iceberg. The Commission will in a few months propose a new Directive on attacks against information systems.

"Cyber crime and cyber security is a new and rapidly evolving phenomenon to which Europe has yet to find a comprehensive response. And I want this to be clearly addressed in the internal security strategy."

Ultimately it may be difficult to manage this at a political level. The political process cannot keep up with the speed of technological developments, which has resulted in a stream of well intentioned legislation, but no results to speak of. In fact, 19 nations have elected to sign the 2001 treaty, but not ratify it - the UK being one of them – signaling that whilst they agree in principle to the treaty, they do not wish to be legally bound by the document.

As reported on euractiv.com the EU have now asked the European Commission (EC) to:

"…"assess the feasibility" of setting up a single centre on cybercrime to pool member states' efforts and resources to fight Internet crime."

The article goes on to list the UK, Germany and France as opposing similar schemes in the past due to fear of trampling on their own national programs. Again, it's clear to see why the EU is struggling to make an impact when some of its founding member states refuse to surrender significant authority in this area.

According to Albena Spasova, *"…there's an extraordinary lack of data on the scale of cyber crime in the EU and no unified system for reporting it. Europol is setting up a European platform for reporting crime, but officials admit that the 27 EU member states are under no obligation to provide them with information and they have no precise data on either the scale or the cost of cyber crime in Europe."*

It's not clear how the EU is expecting to increase international co-operation, when member states, some of whom are signed up to the 2001 treaty, don't have to provide basic data. Without the data there cannot be an effective remedy for the situation.

The Superpower Solution

America is one of the nations that did ratify the 2001 treaty. The National Strategy to Secure Cyberspace, published in February 2003, read:

"The United States is committed to working with nations to ensure the integrity of the global information networks that support critical economic and security infrastructure. We are also ready to utilize government-sponsored organizations… to facilitate global coordination on cybersecurity. In order to facilitate coordination with the private sector, we will also utilize such organizations as the Transatlantic Business Dialogue."

The Senate recently passed the International Cybercrime Reporting and Co-operation Act which would see the President provide an annual report on international cybercrime permitting America to suspend aid, trade and other finance programmes with the worst nations should they fail to improve. As reported by Reuters, Senator Kirsten Gillibrand said:

"Other countries aren't going after these criminals at all. We need the help of Russia and China and all of our other countries to be able to create protocols to crack down on cybercriminals."

The US is in a unique position. It's currently the only major superpower that has both economic power, and international political influence. Many nations depend on trade with and aid from them, and so cutting off this source of revenue for them may act as a more powerful motivator than a political treaty negotiated in Brussels.

The UN route

The United Nations has tried, and failed to reconcile the differences between developed nations (led by the EU, US and Canada) in talks held during April 2010.

The summit did see the UN say that it would consider conducting a study of cybercrime, legislation and law enforcement, but as Infosecurity Magazine observed, this process might take years.

The nations did agree that developed countries must provide more assistance to developing countries to tackle cybercrime, but the EU and US refused to consider the creation of a new treaty on cybercrime to replace the one signed in 2001, when the threat landscape was quite different.

Although the 2001 treaty allows police to access foreign servers with the permission of the system owners, it's a controversial issue which Russia has objected to since the US hacked computers belonging to Russian fraudsters in 2000.

The US and EU object on privacy grounds.

A treaty negotiated by the UN has a greater chance of being adopted by nations outside the EU, and would be better for developing nations, but the increased reach of the UN comes with a greater political burden. The more Governments that get involved in the process, the more politics gets in the way of progress. It is unlikely that enemies will co-operate even if there is a mutual benefit.

The Public/Private Sector Solution

The EWI Worldwide Cybersecurity Summit, which took place May 2010 in Dallas, Texas, had three goals: to launch an international awareness campaign, identify proposals for action to address threats and vulnerabilities and to facilitate joint action.

"Private discussions and public comment at the summit confirmed that there are large gaps in global arrangements to promote cybersecurity, especially where important countries such as the United States, China, India and Russia are concerned. These gaps are however part of a bigger picture of relatively weak regulation of cyberspace by the international community."

It's feasible that an initiative driven largely by the private sector will have more impact than one driven by political co-operation, mainly because the private sector realises that a valuable revenue source is being jeopardised as the risk of consumer losing confidence in the internet increases. Still, one of the areas for concern cited at the summit was:

"inadequacy of current diplomatic assets assigned to the problem, a situation which reflects a lack of political commitment or awareness at high levels"

Meanwhile, other bodies such as the IMPACT Alliance, which styles itself as a global not-for-profit public-private partnership against cyber threats, aim to work with governments and industry to fight against cyber threats. Based in Malaysia, the organisation is encouraging nations to work together. Datuk Seri Dr Rais Yatim, Malaysia's Information Communication and Culture Minister, commented on the issue at the opening of the World Information and Communication Summit in Seoul:

"The rise in cyber security attacks over the last few years reinforces the urgency to address the issue through the establishment of appropriate global frameworks for assessment and exchange of information related to cyber security."

What's clear is that there is a general awareness that something needs to be done. The problem is enforcement.

In December 2009 Lance Atkinson was ordered to pay a fine of $15m by the US courts for running a massive international spam network. The huge fine would be an effective deterrent, if it weren't for the fact that Atkinson was from New Zealand, and would only have to pay the fine if he entered the US.

UK resident Gary McKinnon's extradition to the US has recently been put on hold by the new Home Secretary, Theresa May (which may be partly due to the long running and well publicised campaign in the UK to quash the extradition). McKinnon, who has Aspergers Syndrome, broke the law by hacking into US military systems in 2001. The US waited to apply for his extradition until a new treaty came into effect in 2005 – a treaty which has been reported as appearing one sided.

As both cases clearly demonstrate, politically negotiated solutions to cybercrime are fraught with a myriad of complexities. Nations can only punish citizens of other nations if they effectively have the permission of the government of the country the perpetrator resides in – a government which has to consider its own position and the welfare of its citizens.

The Changing Nature of Cybercrime

On the face of it, cybercrime is a global problem, which needs a global solution. Individual nations make significant progress in fighting cybercriminals in their own territories, but the criminals will just move their base of operations to other countries.

The shutdown of the McColo ISP in November 2008 reduced levels of spam in the short term, but it was predicted that the criminal gangs using the service would simply shift their operations to Russia.

Russian ISP PROXIEZ-NET was taken offline earlier this year which resulted in decline of malicious activity from Russia in the May threat statistics, figures that also revealed that the top virus producers were Korea, the US and the UK.

The ease with which a botnet can be established and managed, and the lack of infrastructure needed to carry out these attacks, makes cybercriminals highly mobile and gives them the ability to switch between rogue servers and ISPs in a variety of countries. Therefore, when an individual country is successful in shutting down a McColo, or a PROXIEZ-NET, the criminals that can afford to set up operations elsewhere, do.

It's still true that most cyber gangs originate from Eastern Europe, China or the US, but the way they operate means that spam which originates from a bedroom in China, can appear as if it's being sent from countries such as India, and targets users in Europe and the US involving three or four different national judiciaries. Clearly, to successfully combat international cybercrime, there needs to be an international solution, but some nations seem willing to allow these gangs to continue operating as long as the targets remain away from home. For example, small businesses in the US are increasingly finding themselves targets of Eastern European cyber gangs.

So, What Should Governments be Doing?

The UK already has a cybercrime unit which has made significant arrests. In the US, the Department of Justice frequently prosecutes gang members, as do many other countries. But when the gang members are spread around the world, arresting a couple of members who reside in your country often leaves the rest of the gang to carry on with their illegal activities. There have been some notable examples of international co-operation suggesting that when goals coincide, countries can act together.

However, it's doubtful that nations who have poor diplomatic relations with each other will go out of their way to co-operate to develop an international solution to the cybercrime problem, which is one of the core reasons why developing a solution is proving so difficult. In the short term we have to continue looking for technical solutions to this problem but it should only be one avenue of tackling this crime, education is also required: if no one responded to Spam, then there would be no point in Spam but the push to international co-operation must be pursued even if it is not proving successful at the moment. This will provide a further disincentive to criminals who currently see cybercrime as low risk.