

THE IMPORTANCE OF INTERNATIONAL CO OPERATION IN PREVENTING CYBERCRIME

Introduction

By its very nature cyber crime is international. It is essential that countries assist each other in the provision of evidence and that investigators and prosecutors are aware of the mechanisms that exist to obtain such information. My aim is to demonstrate the importance of mutual legal assistance in the investigation and prosecution of cyber crime and to highlight some of the practical steps that may help to ensure the request is effective.

Terminology

Mutual Legal Assistance (MLA)

Strictly speaking this term relates solely to formal methods of obtaining assistance from other jurisdictions, however I also use the term to describe enquires between police officers outside of or independent of a formal request.

Letter or Request or Commission Rogatoire (LOR)

The formal request transmitted between states usually pursuant to a bi or multi lateral international convention or treaty but at least so far as the UK is concerned can be submitted where no formal instrument exists.

Underpinning principles

MLA is predicated on mutual respect and understanding and on a willingness to commit resources where there exists no or only a tenuous link to the jurisdiction.

Case study

OPERATION CATTERICK

Concerned the extortion of on line gambling companies between May and October 2004

A number of criminal groups were responsible, with individuals moving between groups.

The criminals would send a demand for money to a company threatening to execute a Distributed Denial of Service (DDOS) attack on their website if they failed to pay. A DDOS attack is where many thousands or hundreds of thousands of computers from all over the world visit a website at the same time, the effect of so many persons seeking to access the site causes the site to crash.

The gang executed DDOS attacks in order to prove to the companies that they had the capability.

The DDOS were executed using a BOTNET. This is a network of computers which have been infected with a virus that allows the BOTNET controller to activate them and have them visit a website at the same time. The owners of these infected, or Zombie computers are unaware of the fact that their computer has been compromised.

57 companies were attacked worldwide 10 UK based companies who lost in excess of £30m

In addition to the effect on the websites themselves the amount of data being directed along a section of the internet backbone came close to causing it to collapse

The investigation

Note this is a very brief overview of what was and is a complex and long running investigation

Initially the investigations were initiated by UK and US law enforcement -

Police to Police enquires lead to Latvia and this was followed by an LOR

The Latvian police launched a covert surveillance operation, as a result 10 people arrested who were suspected of being involved in money laundering, these couldn't be extradited and a local investigation with a view to prosecution was initiated –,that investigation is ongoing

A compromised computer was located and a copy of the malicious code taken from it .That led to an Internet Relay Chat (IRC) channel, officers monitored those chat rooms and found that botnet controller would enter the channel to launch his attack. Individuals in those channels were identified.

Example .eXe

A person with the nickname eXe was using an IRC channel ##[eXe]## .He was seen to offer a new version of attack software in one of the channels and this offer was accepted , from that his IP address was found .He was also found on ICQ channels discussing hacking .

The IP address was in a range allocated to Balakovo in Russia .

In the channels eXe said he was 21 years old , male, named Ivan , he was Russian, a student of French and engineering and that he had received payment for DDOS attacks.

It was also discovered that he used other nicknames;

~x3m1st

NASA

X890

x

Key

An e mail account with the name ~x3m1st@security-system.cc had registered a domain name - security –system.cc using the details

Fizitheskoe lico

Makasakov Ivan

Balakovo

The malicious code also revealed a server located in the US which had been rented using a stolen credit card was used to host IRC chat rooms and to launch DDOS attacks.

The FBI in the USA seized the server .An IP address was recovered which had connected to the server on a number of occasions. The IP range resolved to Balakovo Russia.

An examination of one of the infected machines revealed that it connected to ##[eXe]## and logged real users in the channel. We knew they were real users because they were seen to issue specific commands. One of these who logged on as NASA!~x3m1st@as-dia058.balakovo.sans.ru (also known as eXe) was seen to launch an attack , he issued the command “Logon” then “auto” then “!port commands”

The bots replied “port flood ip” at which they began to attack an online gaming company.

Letter of request to Russia .

LOR sent to Russian which initially met with little response. The aim of the request was to have the Russians commence an investigation with a view to prosecution, it being quickly realised that extradition would not be available.

Following a visit to UK by V Putin our foreign minister had a quiet word with him following which Moscow police initiated an investigation of their own which became effectively a joint investigation ; if the suspects were Russian nationals they could not be extradited to UK so would have to be prosecuted in Russia

Use of supplementary LORs

The Russian investigation was focused primarily on the perpetrators of the DDOS attacks .The Russian Police and UK police worked closely together with a UK officer spending a considerable amount of time in Russia

In June 2004 a number of arrests were made and computers seized.

In December 05 the trial commenced of 3 men in Moscow .A UK officer was a key witness The trial process took 10 months and each was convicted of extortion and deploying a computer virus and sentenced to 8 years which was recently upheld on appeal

Conclusion

We regard this operation as a partial success- The DDOS attacks against UK companies have stopped – the UK is now regarded as a hard target and cyber criminals like any other criminal looks for a soft target – what we have achieved is displacement – they are still engaged in this activity in other parts of the world and have varied their tactics – i.e. hacking into the computers of business encrypting their data and then making a demand for payment before de encrypting it.

MLA and Cybercrime. Keys to success.

- There is a clear need to secure commitment from all countries. We have found that you achieve the best results when informal , police to police contact is made and followed up with a formal request where and if required.
- The LOR'S need to be as detailed as possible identifying the precise enquires to be undertaken and the format in which the evidence is required.

- Only make a formal request if you have to – it saves yours and everyone else's time.
- If you make a formal request and no longer require the information let the county know
- Keep requests to a minimum and specify as precisely as you are able to what it is that you want
- Establishing one to one contact reaps rewards events such as conferences or via Interpol or Europol or pick up the phone (may need interpreter of course) but generally police officers and lawyers speak the same technical language
- Consider carefully whether a police officer really needs to travel in connection with a request. There are resource implications for the requesting state who may need to provide a chaperone or interpreter but in a technical investigation the officer in the case will be best placed to know what evidence is needed and can assist where suspects are interviewed.

Security of Information

How do you ensure the confidentiality of your requests?

It will frequently be the case that to make a formal request for assistance you will have to include in the letter sensitive information, which, if it fell into the wrong hands, could compromise the investigation/prosecution or endanger someone's life.

The prosecutor will need to be alive to the fact that not only the contents of a letter of request but also the mere fact that an investigation is under way could be enough to alert a suspect.

When issuing a letter or request that will of necessity involve the inclusion of sensitive information the prosecutor should advise the agent that the system for obtaining mutual legal assistance is inherently insecure and, depending on the foreign state being requested, there is a risk of unwanted disclosure.

Practical steps to protect sensitive information

- It may be possible for the police to obtain the evidence by way of mutual assistance, without having to disclose the sensitive information.
- It may be that the letter can be drafted without having to disclose a piece of sensitive information.
- Alternatively it may be possible to submit a vague (sometimes referred to as an 'open' letter) and to supply in addition another document ('closed' letter) or perhaps an oral briefing.
- Some European jurisdictions for example have to disclose documents that are on their open file but are able to withhold those on the closed file.
- The appropriate methodology should be discussed with the requested state in advance. Practises differ and it is not possible to provide comprehensive guidance here.
- Does the treaty or convention help?
- In some cases it is possible to make a conditional request for assistance, that is one that is only being made if the requesting state is able to execute the request without disclosing some or all of the information in the letter.
- Where there are concerns about sensitive information being disclosed, it is good practice to explain in the letter of request what they are and why you do not want the information passed on to anyone not involved in the execution of the request.

Emergency situations need for speed

Does the LOR have to be transmitted via a central authority or can it be send direct to either a court or prosecutor?

Again Informal methods first – locate your prosecutor or judge and let him know in advance that it is coming .If no time can the local police use own investigative powers to seize or secure evidence pending a formal request?

It's all about finding ways and means

Other considerations

Should the defendant or suspect be notified of the enquires you are making or allowed to be present when they are being made? Should they be alerted to sources of evidence that may be transitory and which they may wish to explore in order to prepare their defence.

In the UK we have a well established system concerning the disclosure of material that though not used by the prosecution should be disclosed to a defendant in order to ensure he has a fair trial. Each case is different and procedures obviously differ between countries I raise it simply as another matter that may need to be considered.

Prosecutors discretion to issue a letter of request

Prosecutors and investigators need to evaluate the benefit of a request for MLA to the case or investigation. Formal international enquiries are expensive, for both the requested and requesting states.

Factors to consider:-

- The value to the case of the enquires
- Whether a prosecution can be justified in terms of the cost of a formal international enquiry;
- The consequences of issuing a letter of request, e.g. whether it is worth risking the security of a police operation by broadcasting sensitive information;
- Whether, realistically, there is time to obtain the evidence;
- Whether, realistically, there exists the prospect that the evidence can be obtained;
- Whether there would be a realistic prospect of conviction were the evidence to be obtained;
- Whether it would be in the public interest to prosecute or continue with the prosecution;
- The likely admissibility of the requested evidence.
- Also don't forget Open Source material there is a lot of material available on the Internet that doesn't need an LOR

Russell Tyner

Specialist Crown Prosecutor

Crown Prosecution Service

Organised Crime Division London