Copyright © 2008 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891
January-June 2008, Vol 2 (1): 256–270

SPECIAL PAPER

Bangkok International Summit (2007) Declaration on Policing Cyberspace

K. Jaishankar[1]
Manonmaniam Sundaranar University, Tirunelveli, India

Bessie Pang[2]
The Society for the Policing of Cyberspace (POLCYB), Canada

Stuart Hyde[3]
Assistant Chief Constable, West Midlands Police, United Kingdom

Abstract

The Bangkok International Summit (2007) declaration on Policing Cyberspace is an outcome of the 7th Annual Policing Cyberspace Summit of POLCYB held at Bangkok, Thailand during 5-9, November 2007, in collaboration with Council of Europe (COE), and co-hosted with the International Law Enforcement Academy (ILEA), Bangkok Thailand. The Society for the Policing of Cyberspace (POLCYB) was incorporated as a not-for-profit, international society in June 1999. It is based in British Columbia, Canada. The Mission of the Society for the Policing of Cyberspace is to promote cyber security through enhancing and developing global international partnerships to prevent, detect, and combat cyberspace crimes. Its goal is to enhance international partnerships among public and private professionals to prevent and combat crimes in cyberspace. This paper arose at focus group meetings following the annual international POLCYB conference. This paper proposes many recommendations including development of a secure online repository of information, and a secure communications forum for use of international professionals who are engaged in preventing and combating cyber crime.

Key words: International Summit; Policing cyberspace; Cyber crimes; Malware; Phishing.

[1] Editor-in-Chief, International Journal of Cyber Criminology; Senior Lecturer, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli 627 012. Tamil Nadu, India. Email: drjaishankar@gmail.com URL: http://www.drjaishankar.co.nr

[2] Executive Director, The Society For The Policing Of Cyberspace, British Columbia, Canada. URL: http://www.polcyb.org Email: polcyb@polcyb.org

[3] Assistant Chief Constable, West Midlands Police, Birmingham, United Kingdom and Board Member, The Society For The Policing Of Cyberspace, British Columbia, Canada.

Introduction

The International Conference on Policing Cyberspace of POLCYB,[4] first held in Vancouver, British Columbia, Canada in 1999, has become a premier international forum for the presentation and discussion of advances in Policing cyberspace and the multifaceted issue of cyber crimes. In view of recent scientific advances and the ongoing consideration of policy options for addressing the cyber crime problem, the Seventh Annual International Conference in Bangkok, Thailand on November 5 - 9, 2007, presented a timely opportunity to address key questions concerning policing cyberspace. The technical program for the conference contained a diverse and multidisciplinary assemblage of more than 100 abstracts submitted by authors from many countries, contributing to the global scientific effort on prevention of cyber crime.

Forty experts, assembled into four groups, at the International Law Enforcement Academy, Bangkok, Thailand, worked after the conference at the Post-Summit Digital Evidence focus group discussions. The focus groups addressed a series of key, policy-relevant questions concerning Policing Cyberspace such as Emerging Future Trends and Technologies/Malware, Financial and Organized Crime, Trusted Communities and Protocols, Child Exploitation. The focus groups presented their findings on 9th November 2007. Summaries of these findings were available for viewing by all registered conference participants in the POLCYB website. Collectively, the four focus group summaries provided the foundation for the Conference Declaration, a summary document that was endorsed unanimously by members of the four expert groups.

Theme and Sub-themes of the Summit

The Summit Theme was, ***"International Policing and Policy Perspectives on Countering Cybercrime"*** and the sub-themes were:

- Challenges in Collection and Application of Digital Evidence.
- Digital Identity - New technologies; best practices and challenges in development of standards and frameworks; policy gap analysis.
- Current International Cyber crime Trends / Threats - Investigation & Prosecution perspectives.
- Data Protection, Privacy, and Identity Management.
- Building "Trusted Communities" in the Virtual World.
- E-Money Laundering in Financial Sectors: Legal Obligations of International Banking.
- Disrupting International Organized Crime.

[4] The Society for the Policing of Cyberspace (POLCYB) was incorporated as a not-for-profit society in June 1999. Based in British Columbia, Canada, its goal is to enhance international partnerships among public and private professionals to prevent and combat crimes in cyberspace. POLCYB international network includes practitioners from all organizational levels in the public and private sectors. POLCYB partners ranges from professionals who work in the areas of law enforcement, criminal justice, corporate security, and academic institutions. POLCYB strive to facilitate information-sharing between and among executives, administrators, and front-line professionals through seeking expert advice among our global and diverse membership. POLCYB also provide public education on information protection and internet safety to raise public awareness of cyber crime, including those committed against children and youth. To promote our objective, we regularly host Quarterly Meetings, Annual International Conferences, and public education forums. More about POLCYB can be found in their website is http://www.polcyb.org

- Child Exploitation.
- Pharmaceutical Crime on Internet.
- Economic Crime / Organized Crime:
    - Counterfeit Products / Intellectual Property
    - Spam, Phishing, Botnets
    - Identity Theft
    - Hack & Harvest
    - Pharmaceutical Crime on Internet
    - Online Games
    - Online Trading/Banking
- Risk assessment of Converging Technologies and Emerging Technologies
- Challenges and Best Practices in Development of "Trusted Communities"
- Privacy
- Child Exploitation
- Response from Multinational Companies to "Hack and Harvest" incidents and other cyber threats
- Training and Accreditation (Forensic Investigator; Forensic Analyst; Forensic Accountant, etc.)
- Cyber Intelligence (Honey Pot, Email Spamming, etc.)
- Counter cyber intelligence (technologies that thwart computer forensic investigations)
- Best Practices in investigation and prosecution using Digital Evidence (Incident Reports, Lab Management; Digital Evidence Recovery; Network Forensics, etc.)
- Protection of Industrial Infrastructure
- Homeland Security / Critical Infrastructure Protection / Cyber-terrorism
- Drafting Principles / Impact / Enforcement of Legislations and Polices relating to Cyber crime / Information Security / Communications / Privacy
- Integrated Approach to Management of Hi-tech Offenders
- Considerations for developing communication protocols to build "Trusted Communities".

BANKOK *INTERNATIONAL SUMMIT (2007)* DECLARATION *ON POLICING CYBERSPACE*: BASED ON THE FACILITATED FOCUS GROUP DISCUSSION

Objectives of the Focus group discussion:

- To share information on challenges in the collection and application of digital evidence in terms of social, legal, economic considerations.
- To share best practices in training, prevention, detection, and response.
- To build an international network of contacts of colleagues dealing with cyber crime and digital evidence issues throughout the world.

Summit delegates who attended the 2-day discussion participated in one of the four special interest groups described below in the Facilitated Group Discussion section. Each group comprised two co-facilitators, and international members from criminal justice, industry, and academia to facilitate effective inter-disciplinary discussions. Case examples were used by co-facilitators to stimulate discussions on the pre-assigned questions relating to international collaboration issues relating to the gathering, identifying and introduction of digital evidence in criminal prosecutions. Group discussions took into account legal, social, and economic challenges faced by the respective special interest groups in relation to the collection and application of digital evidence. Response and recommendations were discussed.

The Focus Group Discussions facilitated an invaluable face-to-face contact for practitioners to explore challenges in training, investigation, and prosecution of cyber crime in different countries with reference to a wide variety of pertinent issues. Issues discussed included, but were not limited to: international legislations, information security policies, privacy legislations, international collaboration –and with particular reference to the Council Of Europe Convention of Cybercrime, and the development of proactive measures to thwart cyber crime and foster effective computer forensic investigations.

Facilitated Focus Groups

- *Group 1: Emerging Future Trends and Technologies/Malware*
- *Group 2: Financial and Organized Crime*
- *Group 3: Trusted Communities and Protocols*
- *Group 4: Child Exploitation*

These groups identified key challenges on various issues of cyber crimes, provided steps to be taken and proposed recommendations to POLCYB.

GROUP 1. EMERGING FUTURE TRENDS & TECHNOLOGIES/MALWARE

Key Challenges

This group discussed about a number of issues that were now impacting in various degrees on the use of technology. A list of "Top 12 Malware Threats" to date was compiled by the group[5]. It is fair to say that whilst expertise is available for a number of the below threats they are not necessarily organized in one easily accessible location – physical or virtual - and that data on quantum of incidents is difficult to identify.

1. Spyware hiding behind rootkits
2. Deployment of key loggers
3. Bogus digital certificates
4. Network configuration attacks (micro to macro) to redirect web/email traffic
5. Self morphing malware
6. Infection via Peer to Peer network (myspace, youtube, facebook)
7. Script-based attacks for web 2.0
8. Client side exploits expanding from web browser to Word, Excel, and PowerPoint.
9. Zero day exploits in word and excel macros
10. Privilege escalation attacks in non Vista machines.
11. Really big botnets (supercomputer at the disposal of criminals)
12. Move to mobile platform, PDA and iPod, iPhone

[5] The "Top 10" Malware Threats identified and discussed by this group are available to POLCYB Members and 2007 Summit Delegates in the full version of "POLCYB International Summit 2007 Summary of Focus Discussions". The Summary is available from POLCYB upon request.

Some Conclusions from the discussions

Mutual Authentication using smart card will help reduce phishing and other ID thefts. Whilst very technical attacks using digital product created a menace and a threat, it was still possible to use "human-ware" to initiate attacks. This could be attained by convincing the user that the site or relevant software is what it purports to be. There was debate about the need to support human intuitive responses, which could be influenced with something more dynamic and objective such as a requirement for a mutual authentication process.

Consumers are reluctant to use 2-factor authentication. The group discussed authentication and whilst acknowledging some difficulty with a number of processes found no conclusions as to why such "common sense" approaches could not be sustained. Educate policy makers on the inadequacy of single factor authentication and the
issues of privacy and function creep of using smart cards ID. Users could be influenced by a number of issues including cost, speed and efficiency in deciding which authentication they felt could be used. However, the impact of policy makers could be a factor in increasing public confidence and trust in such processes.

Better form factors (such as VISA card with embedded smart card) or national ID card will help consumer acceptance. This needs to be balanced against the central control of data and the risk of data loss on a grand scale. Within the UK recent cases of data loss have reduced the citizen's confidence in the state's ability to hold and manage data. However objectively the wider use of chip enabled data cards was seen as a preferred option.

New hardware should have smart card readers built in. The use of smart readers will grow as more authentication and dynamic connection between user and machine is of greater significance. As such consumers will be looking for facilities that will enable them to protect valuable and vulnerable data as well as protecting them from illicit activity.

When a real time international bank transfer happens, then the problem of cyber crime will escalate. Currently there is a delay in the movement of funds which sometimes provides an opportunity for preventative measures. However with the use of real time movement and the speed with which access points and accounts can be created and folded, either a much more dynamic approach is required or legislation to support the new speed of operation.

The brick and mortar ATM machine fraud is larger than cyber frauds at this time. Traditional human ware fraud using stolen ID or convincing users of authenticity are still in their ascendancy not least because they often involve less risk and do not leave much of a digital signature. The human user can be fooled or convinced of authenticity in circumstance that would not be possible with a machine.

Identity Theft is the real problem. False application of credit cards with fake ID. Creating a new or false person or abstracting someone's details for use in impersonation is not particularly difficult and is an extension of historic masquerading and basic fraud. Creating a document that purports to be what it is not is easier perhaps in some circumstances than creating a digital existence or entity with appropriate authentication.

GROUP 2. FINANCIAL & ORGANIZED CRIME

Key Challenges

The group identified a Common Goal of making the Internet a safe place for trade, and an unsafe place for organized crime. Some regions were considered and the group created a comprehensive overview that identified a number of local issues.[6] The group felt that the methods of committing crime were similar in many regions. As such, common approaches could be created to address them.

Some Conclusions from the discussions

The group examined those constraints which were considered to be mutual.

Tracing of the suspects within various environments is challenging. Using international approaches for identifying and locating offenders was expensive and often difficult or impossible logistically or through economics, even before issues of corruption are discussed.

A debate centered on the capacity within the various Policing Agencies and the various Prosecuting Authorities to address these issues and the ability of agencies to work across international boundaries.

Capacity could be restricted by:

- Technological issues such as the availability of basic technological functions, including software and hardware, as well as a lack of understanding of process.
- Systems (Supply and Demand). Current investment in Hi Tech crime is not at the same pace as the growth in the use of technology to commit crime. As such, a debilitating influence could be the availability of someone who understands, can access and then manage an investigation in a time frame and location that makes it effective.

<u>Transnational Co-ordination is imperative, taking into consideration the restraints placed by the various legislative environments</u>

The speed of International Agencies to respond to allegations of crime is of paramount importance and directly related to its capacity and capability of resolving the allegation. Public sector enforcement agencies can be limited in their approach owing to budgetary or organizational barriers. However this does not prevent protection being offered by the private sector. Money can buy investigative capability and capacity, but this does open the question of whether that can include the use of coercive powers.

States and their enforcement agencies also have differing values and cultures based on their history and development, as well as the socio-economic and political environments in which they exist. In trying to tackle electronic crime these issues need to be addressed.

Whilst Anglophone counties can more easily co-operate (although there are some discrepancies) language can become a significant barrier if interpretation is required. In some public bodies interpretation can substantially slow down any corporate activity.

[6] Further information is available upon request from POLCYB via email to: polcyb@polcyb.org.

Relationships assist the facilitation of acquiring information in certain instances but the question is whether the acquiring of the information through this means will be admissible in a court / prosecution.

Within the international community there are legislative Gaps between different countries making life complex, particularly for companies that exist across a number of continents, time-frames and political systems.

Even if time and legislation is not a barrier technological capacity, system or the environment can be. An allegation made in one country may not achieve the same level of response as another. In fact the same circumstances may not be an offence in another country.

- **Jurisdiction** – where the crime occurred in one jurisdiction, especially within share trading schemes and electronic crime, legislation in the country where the incident has occurred might not criminalize the crime or incident. The primacy of legislation also impacts on the way in which a crime can be reported or solved. The question is often where has the offence been committed?
- **Targets** – Most national Governments hold their respective agencies to account financially and operationally through a series of core identified objectives. These have associated targets to support them and ensure that each agency understands what it is trying to achieve and how. This management technique is driven by statistics which could in certain instances also impact on the willingness to undertake an investigation – especially transnational in nature. Where there is a correlation between the offence disclosed and central targets then it is not a problem, or if the disclosure is supported by a political or public will. However where there is dissonance between the type and nature of the offending and an adverse impact on achieving targets (by diverting resources) achieving an investigation could be difficult if not impossible.
- **Transnational Crime** – there can be multiple methods of committing crimes or multiple locations that add a greater level of complexity. Likewise where time zones conspire with multi layered offending, achieving resolution can become very difficult.

Government Issues

- Priorities are often different when dealing with specific crimes.
- Budget constraints can stop international investigations.
- Methods of information gathering, data storage and court readiness can differ considerably.
- Agencies may not have the physical capacity to address the offence.

Non Governmental

- There are a number of national bodies that represent business interests and can protect those who have been offended against. Some examples are:

South Africa:

- SABRIC (South African Banking Risk Information Centre)
- BAC (Business Against Crime)

Hong Kong:

- Hong Kong Banking Union

Thailand:

- No specific bodies in the business sector exist.

International Associations (NGO) :

- PSI (Pharmaceutical Security Institute)
- QBPC (Quality Brand Policy Committee)

Training and Development

Training – is often limited to National training of the country concerned, and might not cover a broad array of international issues from an international perspective. Transnational training is important, but there would also be constraints with the physical implementation thereof.

- Some would consider it venturing into the unknown, particularly if investigations need to be flexible and can involve multiple countries.
- One-off training is rarely effective unless it is supported by a competency approach and refresher facilities.
- Differing technological platforms might create an unnecessary barrier
- Selection processes can often lead to those inappropriate being trained and then being lost to other sectors.

Awareness

Experience of managing e-crimes can vary. It is possible that a country or jurisdiction has limited experience of certain offending and therefore it can become problematic in managing the response. As such some effort needs to be invested in managing expectations and the ability to translate offending to different countries. This creates an opportunity to spread the word amongst states as to type and nature of offending behaviour and how it impacts on countries, or their citizens.

Short Term

In the short term it is vital that all those involved in working with e-crime understand what training is available and how it impacts on Law Enforcement.

- What resources and to what capacity and capability would be available that could be used?
- Whilst all investigations cost resources, the provision of some data to law enforcement should add value and should be seen as an investment, rather than an overhead.

Training – The Business Sector would benefit from training and educational opportunities to enable it to participate in law enforcement activities to help reduce opportunities for e-crime, deter and reduce occurrences as well as playing a key role in investigation.

– As part of this debate there was a call for volunteers amongst POLCYB membership to establish Project Groups.

Identify – Center of Expertise

Regional

- A 'repository of data' which is placed on websites that POLCYB members could research for information and their own development should be made available. This could also include documents that have been written by investigators.

- POLCYB members to identify organization/s (Websites, viz Anti Phishing Working Group) that they can refer other members to turn to for information. Ask members who they turn to when they need information and have this information available to all members.

POLCYB to invite Eastern Bloc Law Enforcement Agencies.

- It was felt that work with the old Eastern Block countries(now EU states) should be expanded particularly as this area was opening up for expansion, development and integration in the EU. An invite should be made through our existing EU contacts

Training – POLCYB (Web) to establish a centre of expertise (members) that could assist with training of Law Enforcement and NGO.

Information sharing – POLCYB Network

In our view there is a clear need to collect case laws etc from various jurisdictions and to establish a reference manual (PDF) available to all members. This will be a fast finder for practical topics and trends with reference to what was said in the courts around the world.

GROUP 3: TRUSTED COMMUNITIES & PROTOCOLS

Key Challenges

Policies of countries do not react sufficiently to the rapid growth of cyber crime as the extent of this growth is frequently underestimated. Separate statistics showing the significant increase in cyber crime are often not available as usually only general statistics concerning crime are available. In addition there is insufficient e-crime reporting at a national level. Cyber crime is often neglected as electronic offences are 'unseen'. Insufficient funding may prevent law enforcement from carrying out all necessary investigations and may also hamper co-operation between all those involved. In particular there are not enough persons with technical knowledge to carry out investigations.

In spite of the various structures which exist to fight cyber crime there may be considerable gaps in the protection provided. Legislation may be piecemeal and the procedures to fight cyber crime may be insufficient. The collection of evidence may be difficult because of the lack of rules and understanding. Training and education to fight cyber crime may be too limited. Prosecutors, lawyers and judges do not always have sufficient understanding of problems and the applicable procedures.

Steps to Be Taken

Appropriate practical measures and policies should be taken in sufficient time to enable cyber crime to be fought effectively. Meaningful statistics on cyber crime should be available in order to enable countries to adopt, in good time, appropriate practical measures and policies. The public and private sectors, including the NGOs, should promote a greater awareness of the problems of cyber crime and encourage better co-ordination.

More human and financial resources should be devoted to fight cyber crime. Collaboration should be strengthened between disciplines. Joint research and co-operation agreements should be promoted both in countries and between countries (e.g. law and computer science schools, industry, law enforcement) including guidance concerning best practices). Training for professionals should be improved, increased and adapted to take accounts, as far as possible, of new technological developments in particular the collection of digital evidence.

The laws and procedures of States should be updated in the light of the standards contained in the Convention on cyber crime. Standards need to be co-coordinated and improved in order to fight more efficiently cyber crime. Of particular interest is the standard road map of the ITU. More steps should be taken to prevent cyber crime by taking measures such as promoting campaigns in schools, providing advice to the public and assisting victims of cyber crime. The private sector should provide customers with easy-to- use tools to protect them against cyber crime and provide clear information about the risks of using cyberspace elements and ways of reducing these risks.

GROUP 4: CHILD EXPLOITATION

This group defined the follow activities as constituting child exploitation:

- Physical abuse of children whether recorded or not
- Sexual abuse of or towards children
- Child pornography, possession distribution or making.
- Bullying/cyber bullying
- Trafficking of children for illicit or illegal purposes
- Prostitution of children
- Physical abuse
- Sexual abuse
- Child pornography
- Bullying/cyber bullying
- Trafficking
- Prostitution

Key Challenges facing law enforcement and industry

- Public awareness and education to help
- Define the problem
- Scope of the problem
- Understand the Gravity of the problem
- Communication
- Cross-border/cross-agency coordination, information sharing

- The ability to transfer data about offenders and victims
- The need to work in real time
- Training
- The need to train and educate staff
- The provision of effective technology
- Understanding new ways that offenders use to communicate
- Awareness of senior management and government officials
- Provision of appropriate resources to meet demands (staff, budgets, technology)
- Understanding of the complexity and context of the problem
- Cultural differences
- Understanding differences of legislation and culture
- Social issue versus law enforcement issue
- Understanding that offending in one country may not be offending in another
- Privacy legislation
- Properly design privacy legislation so that the public is protected but that enforcement can protect people
- Paradigm Challenge: jurisdiction
- Internet is a medium with no real structure or borders, so who ultimately has jurisdiction?
- Collaboration between academics, NGOs, and law enforcement is sometimes difficult

Key Challenges

a) Public Awareness and Education

There is a lack of public awareness about the scope and also the severity of the problem (example: what child pornography really is) among the public and among senior law enforcement. Children must also be taught about what they can do.

b) Communication

Investigators need to know who they can talk to across borders and within other agencies. A lack of information sharing and competition among agencies (particularly in the United States and Canada where there are different levels of law enforcement – local, state/provincial, and Federal) create unique challenges.

c) Training

Investigators need to know and understand the issues. A major problem is also a lack of understanding by unit heads/chiefs of police. Law enforcement needs training on technology, forensics, preservation of evidence, and investigations as well as how to identify the problem itself. Line officers must be trained to recognize the problem.

d) Awareness of Senior Management and Government Officials

It was suggested that the Swedish and Norwegian models be highlighted as good examples of responsibility coming from the top down in terms of information sharing and addressing the problem of child exploitation.

e) Understanding Cultural Differences

In India, for example, child physical abuse is not seen as a big deal. It is part of family life, although corporal punishment has recently been banned in schools. There is no "one size fits all" solution to cultural differences and cultural shifts/changes are slow to happen. There needs to be an understanding, but not necessarily an acceptance of these cultural differences.

f) Public Awareness and Education

There is a lack of public awareness about the scope and also the severity of the problem (example: what child pornography really is) among the public and among senior law enforcement. The term Child Pornography is seen as belittling the offending behaviour, and that terms such as "Child Abuse Images" better reflect what the offence is about. Children must also be able to protect themselves when online particularly as they have greater involvement through social networks.

g) Communication

Investigators need to know who they can talk to across borders and within other agencies and who they can trust. A lack of information sharing and competition among agencies (particularly in the United States and Canada where there are different levels of law enforcement – local, state/provincial, and Federal) create unique challenges.

h) Training and Education

Investigators need to know and understand the issues. A major problem identified by the group was a lack of understanding by unit heads/chiefs of police. The consequences were that individual investigators were carrying the burden of the investigation and expectations of the victim without the backing of the organization. Law enforcement needs training and education on technology, forensics, preservation of evidence, and investigations as well as how to identify the problem itself. Line officers must be trained to recognize the problem and be provided with the technologies to investigate and the welfare support to work effectively and without danger to themselves or others.

i) Awareness of Senior Management and Government Officials

It was suggested that the Swedish and Norwegian models be highlighted as good examples of responsibility coming from the top down in terms of information sharing and addressing the problem of child exploitation.

j) Understanding Cultural Differences

For example, child physical abuse could be dealt with more in a social context rather than legal in some societies. It can be managed as part of the family unit culturally, although corporal punishment in most countries has been banned in schools. There is no "one size fits all" solution to cultural differences and cultural shifts/changes are slow to happen. There needs to be an understanding, but not necessarily an acceptance of these cultural differences.

k) Social Issue versus Law Enforcement Issue

There may be a denial of the problem in some cultures, even though it is a problem that affects all cultures (it may just be more underreported or more underground). In some areas, abuse of children is predominantly an issue worked on by NGOs and not by law enforcement. Senior level officers view this as being a low priority issue, and instead focus on "bigger" problems. The local media often focuses more attention on the issue, so progress can being made. In many law enforcement agencies, there are competing priorities and resources are diverted to other "more serious" crimes.

Another "social" issue to be examined is why there is the demand in the first place and what can we do about it. This is where COPINE can contribute, along with POLCYB. COPINE has conducted extensive and high quality work within the European Union in terms of offender and victimization profiles. POLCYB could consider facilitating the extension of COPINE's work to, and this work needs to be extended to other regions by soliciting interest from. POLCYB can facilitate this, perhaps in conjunction with Correctional Services Canada. POLCYB can recommend to different regional correctional services and the International Association of Chiefs of Police (IACP) facilities that collaborative research be undertaken, perhaps using what COPINE has found as a basis. This may be something the International Association of Chiefs of Police (IACP) may be able to sponsor. However, it is important to keep in mind that it is next to impossible to change the psychological predilections of offenders; therefore, demand is going to be hard to change.

l) Privacy Legislation

When a sex offender is released, most communities do not have registration and notification of offenders. Even when registration and notification are legally allowed, they are not required in all circumstances and there are many non-compliant offenders. Privacy legislation is vital to a civilized society as it protects the individual from the state and others. However this should not be to the detriment of preventing or investigating crimes. A balance is required to ensure both objectives.

m) Paradigm Challenge: Jurisdiction

When there is not one national police force, but rather local, state, and Federal, Internet investigations can be "big" and seemingly without jurisdiction; therefore, smaller jurisdictions may not have the ability to focus their energy and resources on such cases (and they are also not going to get much money to investigate these kinds of cases; money is given for crimes that occur within borders). Norway is in the process of setting up a "police station on the Internet," and the government is funding it. One possible solution may be "identity centers." Web 3.0 is using artificial intelligence built into requests for information. The problem may be solved by requiring true identity and the use of that true identity.

Prioritized Challenges

The top three all have a common thread: they are people oriented, not technology oriented:

I. Public awareness, education, and training (combination of points 1 and 3 above) of several target audiences: parents, children, and law enforcement;
II. Communication between law enforcement agencies; and
III. Collaboration between industry, academics, NGOs, and law enforcement.

CONCLUSIONS OF ALL FOUR GROUPS AND POLCYB Action Items

1. The recommendations of all four focus groups should be published in the International Journal of Cyber Criminology (www.cybercrimejournal.co.nr).
2. A database of contacts, experts, and resources must be created and maintained.
3. Develop a suitable and effective training package with a training provider;
4. Survey current projects and gaps (capability-gap analysis) and identify where our energy would be best spent;
5. Promote adoption of current technologies/computer forensic tools among police chiefs;
6. POLCYB Executives to request for a meeting with the appropriate IACP sub-committee to develop strategies that address training needs, etc.;
7. Establish regional and local working groups on the issue to encourage information sharing; and
8. Create "community policing" materials.
9. Collect case laws from various jurisdictions and to establish a reference manual (PDF) available to all members. This will be a fast finder for practical topics and trends with reference to what was said in the courts around the world.
10. Include regular e-news flashes and an on-line journal on the POLCYB website and consider the possibility of publishing a cyber crime review.

Acknowledgments

The authors profusely thank all the contributors of the conference, especially the Conference Organizing Committee, Panel Chairs, Focus Group Moderators and Rapporteurs, without them this publication would not have materialized.

Special Thanks to

1) Kevin McQuiggin, Inspector, Forensic Services Section, Vancouver Police Department, CANADA
2) Jessica Sarra, Director of Operations, International Centre for Missing & Exploited Children (ICMEC), USA
3) Harry Petrakis, Head of Forensic and Fraud Investigations, Operational Risk Management, First National Bank (FNB) Corporate and Transactional Banking, SOUTH AFRICA
4) Andrew Simpson, Business Development Manager – Evidence, Eden Technology Pty Ltd, AUSTRALIA
5) Margaret Killerby, Head of Law Reform Department (DGHL), Council of Europe, FRANCE
6) Ken Rabey, Director, School of Computing and IT, University of Wolverhampton, UK
7) Nicholas Fong, Industrial Technology Advisor, Industrial Research Assistance Program, National Research Council Canada, CANADA
8) Anthony Teelucksingh, Senior Counsel, Computer Crime & Intellectual Property Section, United States Department of Justice (USDOJ), USA

The Conference Organizing Committee:

Summit Programme Committee Co- Chairs:

1. Bill Boni, Vice President, POLCYB; Corporate Vice President, Motorola, USA.

2. David Lytal, Programme Director, ILEA- Bangkok, Thailand.
3. Margaret Killerby, Head of Law Reform Department (DGHL), Council of Europe, France.
4. Bessie Pang, Executive Director, POLCYB; Canada.
5. Scott Warren, Director, POLCYB; Managing Director, Business Intelligence & Investigations, Kroll International, Japan.

Programme Sub-committee Members:

1) Bill Cotter, President, Cotter Services Inc., Canada.
2) Stuart Hyde, Assistant Chief, West Midlands Police, UK.
3) Gene McLean, Vice President & Chief Security Officer, TELUS Communications Inc., Canada.
4) Steve Palmer, Executive Director, Canadian Police Research Centre, Canada.
5) John Revitt, Sgt., Vancouver Police Department, Canada.
6) Paolo Rosa, Head Workshop and Promotion Division, ITU-Geneva, Switzerland.
7) Betty Shave, Assistant Deputy Chief for International Computer Crime, USDOJ, USA.
8) Joseph Springsteen, Trial Attorney, Computer Crime & Intellectual Property Section, USDOJ, USA.
9) Bill Sykes, Inspector, Transport Canada, Canada.
10) Anthony Teelucksingh, Senior Counsel, Computer Crime & Intellectual Property Section, USDOJ, USA.

Summit Panel Chairs:

1. Michael Eisen, Chief Legal Officer, Microsoft Canada, Canada.
2. Stuart Hyde, ACC, West Midlands Police, UK.
3. Margaret Killerby, Head of Law Reform Department (DGHL), Council of Europe, France.
4. Gene McLean, Vice President & Chief Security Officer, Corporate Security, TELUS Communications Inc., Canada.
5. Andrew Simpson, Business Development Manager- Evidence, Eden Technology Pty Ltd., Australia.
6. Anthony Teelucksingh, Senior Counsel, Computer Crime & Intellectual Property Section, USDOJ, USA.
7. Scott Warren, Managing Director, Business Intelligence & Investigations, Kroll International, Japan.