INTERPOL CYBER RESEARCH AGENDA

WORKSHOP REPORT

INTERPOL

Editors

Prof dr Kim-Kwang Raymond CHOO (unisa.edu.au)
Prof dr Pieter HARTEL (tno.nl/utwente.nl/tud.nl)
Prof dr Anupam JOSHI (umbc.edu)
Christian KARAM (interpol.int)
Prof dr Wee Keong NG (ntu.edu.sg)
Dr Madan OBEROI (interpol.int)
Petra PRONK (tno.nl)
Silvino SCHLICKMANN (interpol.int)
Kimmo ULKUNIEMI (interpol.int)
Matteo VACANI (interpol.int)

Co-organised with

NANYANG TECHNOLOGICAL UNIVERSITY

TNO innovation for life

INTRODUCTION

The Interpol Global Complex for Innovation (IGCI), Nanyang Technological University (NTU) and the Netherlands Organisation for Applied Scientific Research (TNO) jointly organised a workshop comprising participants from law enforcement, academia, private sector and public policy making bodies to establish the international cyber research agenda for law enforcement.

METHOD

An equal number of participants from law enforcement, academia, private sector and public policy making bodies of different countries were invited to discuss the cyber focussed research needs of law enforcement.

The participants worked in small groups with the help of a facilitator. As a structuring tool, each group was suggested to consider the stages before a cyber related incident, during and after a malicious cyber incident.

The results of the discussions from the small groups were categorised in themes to help frame individual research ideas. These themes were then prioritised and outlined in this first report.

RESULTS

The full day workshop took place on 10th of March 2015 in Singapore. Many nationalities were represented and most of the participants are working for international companies and organisations in Singapore. All in all we believe that the participants formed a reasonable representation of the relevant stakeholders in Southeast Asia. Appendix A lists the attendees of the workshop who gave us their permission to list their names.

After a short briefing, the participants discussed the cyber related research needs of law enforcement for about 3 hours in 4 small groups of 10-12 persons each. A professor with research expertise in the field of Cyber Security acted as the facilitator of each group, challenging and working with the participants to come up with ideas and at the same time record the findings of the group

In total about 60 ideas were coined by the four groups. Each group reported its findings in a plenary session to validate the preliminary results. These 60 ideas were then synthesised into a set of research questions under 14 research themes by the facilitators of the four groups and Interpol staff. The 14 themes were then presented in a plenary session for further validation.

The editors of this report finally combined a number of the research themes into a smaller, more manageable list of 8 themes presented below.

The workshop participants identified the need for a cyber research group sponsored by Interpol to consolidate state of the art, to identify emerging trends, and to promote new research. The meeting was informed that the general assembly of Interpol had passed a resolution in Nov 2014 to constitute a Global Cyber Expert Group and it has been proposed to have a subgroup under this dedicated to cyber research.

1. DIGITAL FORENSICS

There are many specialized digital forensics tools on the market, but the main problem is that tool development has difficulties keeping up with the pace of technological innovations [NRC09] and the significant increase in the volume and sources of evidential data to be analysed in digital forensic examinations. This gives rise to a number of research questions such as:

a) How to evaluate and validate digital forensics tools?
b) How to manage e-evidence, and deal with the significant increase in the number and volume of digital devices seized and lodged with digital forensic laboratories for analysis (i.e. big forensic data)?
c) How to design technologies that facilitate a fast review of items of importance, reduce data storage requirements for archival and retrieval purposes, and provide a capability to undertake intelligence analysis of digital forensic data?
d) How to promote forensic readiness for emerging (consumer) technologies?
e) How to achieve forensic-by-design?

2. MEASURING AND FORECASTING CYBERCRIME

Official statistics is often a useful starting point as it provides a measure of the international and domestic efforts and yield detailed information about the extent of malicious cyber activities. A recent report by UNODC [UNO13] shows that measuring cybercrime is difficult. The main reasons are that there are many definitions of cybercrime, and that there are even more methods of counting incidents, assessing damage etc. Before any scientific progress on reducing cybercrime can be made, we must understand better how to measure cybercrime , and what the impact is. The next challenge is to make appropriate models of the present incidence of cyber crime and to predict the future. For example, crime hotspots are physical locations where incidents have happened in the past and where they are likely to happen again, given the right circumstances. Such knowledge is invaluable for the efficient deployment of police capacity. This leads to the following research questions:

a) What current definitions, units of measurement and crime categories are used for malicious cyber activities?
b) How to define cybercrime such that it is measurable?
c) Which agencies are involved in collecting data on malicious cyber activities in the various countries; and what systems are and should be used to collect statistics on malicious cyber activities in a uniform manner?
d) How to measure the incidence and cost of cybercrime?
e) How to model and forecast cyber crime?
f) How to improve the situational awareness on the basis of forecasts?
g) How to improve cyber crime readiness?
h) How to improve the prevention and anticipation of incidents?
i) What legislative reforms are needed to respond to emerging challenges?

3. IMPROVING ATTRIBUTION

Businesses and government rely on identification and authorisation technologies and processes for building trust. However, some of these technologies and policies are inadequate and/or often used inappropriately. For example there are too many certificate authorities that cannot all be trusted; misuse of privacy enhancing technologies challenges the attribution of a crime to a specific offender; many current technologies hinder the collection of forensically sound evidence. This leads to the following research questions:

a) How to design a trusted certification infrastructure?

b) How to design a WHOIS database and procedures relating to its use that are useful to law enforcement?
c) How to design technologies and products which facilitate attributions in case of need?

4. IMPROVING CYBER HYGIENE

Almost all modern police organisations are modelled on the concepts proposed by Sir Robert Peel in the 1830s when he created the Metropolitan police as a response to the breakdown of law and order during the industrial revolution. The Internet revolution may not require a complete overhaul of the police but certainly demands fresh approaches to policing and the manner in which society responds to new technologies. This leads to research questions such as:

a) How to raise the awareness of cyber hygiene amongst the judiciary, prosecution, legislators, and the general public?
b) How to educate the "digital natives" and how to promote a cyber hygiene culture amongst the "digital immigrants"?
c) How to list all the available actors and processes available to them in order to improve cyber hygiene?

5. BALANCING PRIVACY AND SECURITY

The Internet is now an established technology but it is probably the tip of the proverbial iceberg, with many emergent technologies on the way. New technologies pose new challenges to law enforcement. For example money laundering via virtual currencies poses a challenge, as does the spreading of disinformation, rumours, untruths, misinformation and smears (DRUMS) on social media. New technologies also pose problems to our privacy defined here [War1890] "the right to be left alone". This fundamental right is often perceived as conflicting with security. Managing the balance between the two concepts gives rise to a number of research questions, such as:

a) How to design security and privacy into emerging technologies, such as Internet of Things, Critical Infrastructure Protection systems, virtual currencies, and social media networks?
b) How to perform efficient data analytics and visualisation for those new technologies?
c) How to endow data analytics with "responsible disclosure" (in the sense of revealing relevant data if and only if there is an incident)?
d) What are the different approaches to managing the balance between security and privacy?
e) How to develop new and robust technology that allows stakeholders to manage the balance (i.e. legitimate use minimally constrained, but illegitimate use prevented or discouraged)?
f) How to manage the perception of the balance?

6. CAPACITY BUILDING & TRAINING

Training is essential to enjoy the benefits of new technologies to the full. This applies to everyday use of new technology of as well as professional use. Policing has been a branch of the social sciences and as such its practitioners are not optimally prepared for an increasingly technological society, nor for an increasing use of technology in police work. This leads to the following research questions:

a) How to prepare a standardised modular course portfolio for cyber crime investigation and establishing a digital investigation baseline for law enforcement?
b) How to combine the best of the worlds of cyber expertise and policing skills?
c) How to coordinate and de-conflict capacity building?

7. IMPROVING INFORMATION EXCHANGE & SHARING

The Internet has connected the world and in essence it has obliterated all national boundaries in cyber space. Governments, organisation and individuals have been trying to erect new boundaries but an alternative paradigm is one of sharing. For example organisations that are subject to the same threats would benefit from sharing threat intelligence. The challenge is to share criminal intelligence and evidence without harming the integrity of the organisations involved. The Mutual Legal Assistance Treaties (MLAT) allow police organisations to share information but the process is time consuming and does not scale. The following research questions seem appropriate:

a) How to create shareable threat intelligence?
b) How to automate decision-making and information sharing?
c) How to incentivise all the relevant stake holders from the public and the private sector in the information sharing process?
d) What sharing and protection of information processes should be used to facilitate cyber security research?
e) How to harmonise operating procedures to make them interoperable?

8. CYBER CRIMINOLOGY

Cyber criminality is not a monolithic threat, and the diversity of attack vectors and threat actors necessitates enhanced interdisciplinary and international knowledge base. There is a need for an interdisciplinary response from the research-active academy that would involve experts from both computing sciences as well as those from the humanities and social sciences, in partnership with the public and private sectors across all levels. Only by working interdisciplinarily can we begin to tackle cyber spatial threats as it would allow us to better address the knowledge and research gaps in the existing evidence base and contribute to the strategic, operational and policy vacuum; and help to ensure that developments in technologies, political, geographical, socioeconomic, legal and regulatory, etc. are well understood and can be used to refine policy strategies and operational responses. For example, criminologists have studied the behavioural and situational determinants of offences in general, but are sometimes hesitant to study offences where technology plays a prominent role. This gives rise to the following research questions:

a) What theories from criminology and hitherto disparate disciplines can be collectively used to explain and mitigate malicious cyber activities, and reduce the opportunities for the different types of malicious cyber activities to occur and enhance guardianship?
b) What are the differences and similarities in behavioural and situational determinants of offences in cyber space and physical space?
c) What strategies would help to establish social norms as to what is acceptable and unacceptable behaviour in cyber space?

RECOMMENDATIONS

All research questions are to be interpreted in an international, law enforcement context. In particular when we use the word security with the usual meaning of "protection from harm" we implicitly consider the role of law enforcement, because after all, the core business of law enforcement is the protection from harm.

Most research questions are best addressed by multi-disciplinary teams of social and technical scientists, because however big the role of technology, in the end it is people who commit offences. Technical solutions can provide effective protection against many of the existing cyber security threats, but technology alone cannot provide a comprehensive solution. We would be limited in dealing with malicious cyber activities if we do not understand the interplay of the threat actor(s), the environment (e.g. the contemporary international and domestic environment, and the cyber and physical environment) and the targets and victims.

We have identified many research questions. Addressing all of these will probably exceed even the most generous research budget so we offer a prioritisation of the 8 themes. First we offer a prioritisation from the point of view of law enforcement, academia, the private sector, and policy making bodies. Then, giving each of the four prioritisations equal weight, we conclude with an overall prioritisation as shown in the last column of the table below.

The top three are thus "Improving Attribution", "Measuring and forecasting cybercrime", and "Improving Information Exchange and Sharing".

	PRIORITY				
THEME	Law enforcement	Academia	Private sector	Policy makers	**Overall**
1 - Digital forensics	4	3	4	8	**5b**
2 - Measuring and forecasting cybercrime	5	2	7	2	**2**
3 - Improving Attribution	1	5	2	3	**1**
4 - Improving cyber hygiene	6	6	6	1	**5a**
5 - Balancing Privacy and Security	7	4	1	6	**4**
6 - Capacity Building & Training	3	7	5	7	**6a**
7 - Improving Information Exchange and Sharing	2	8	3	4	**3**
8 - Cyber criminology	8	1	8	5	**6b**

REFERENCES

[NRC09] Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. Strengthening Forensic Science in the United States: A Path Forward. U. S. Department of Justice., Aug 2009. http://www.nap.edu/catalog/12589.html

[UNO13] UNODC. Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, Feb 2013. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[War1890] S. D. Warren and L. D. Brandeis. The right to privacy. Harvard Law Review, 4(5):193-220, Dec 1890. http://www.jstor.org/stable/1321160

PARTICIPANTS

The following participants attended the workshop.

Last Name	First Name	Organization/Country
AYOB	Nuru Azhar	Ministry of Home Affairs
BUENAVENTURA	Andres	IGCI, INTERPOL
CACIULOIU	Alexandru	IGCI INTERPOL
CHAN	Edwin	Infocomm Development Authority of Singapore
CHAN	Joe Soon Chee	DBS Bank
CHOO	Raymond	Univ. of South Australia
CHOW	Andy	RBS
CHURCH	Christopher	IGCI, INTERPOL
DURAND	Christophe	IGCI, INTERPOL
ERTEN	Mustafa	IGCI, INTERPOL
FARELO	Antonio	IGCI, INTERPOL
GOH	Su Gim	F-Secure
GUEVARA	Maria Katrina	NTU
HARTEL	Pieter	TNO / U Twente / TU Delft / IGCI INTERPOL
HEINL	Caitriona H.	Rajaratnam School of International Studies
HOO	Chuan Wei	BT Global Services
JOSHI	Anupam	University of Maryland, Baltimore County
KAMLUK	Vitaly	Kaspersky / IGCI INTERPOL
KANG	Meng Chow	CISCO Systems Inc.
KANSIL	Timo	IGCI, INTERPOL
KARAM	Christian	IGCI, INTERPOL
KAWAMATA	Tsunehisa	NEC
KONG	Wai Kin Adams	Nanyang Technological University

NG	Wee Keong	Nanyang Technological University
LIM	Hwee Kang	National Research Foundation / PRIME MINISTER'S OFFICE
LU	Rongxing	Nanyang Technological University
MARDEN	Bradley	IGCI, INTERPOL
MATHUR	Aditya	SUTD
MORI	Takuya	NEC
KIPSOI	Moss	IGCI, INTERPOL
OBERS	Stephan	Australian Federal Police
OGAWA	Ryuichi	NEC
PAN	Jonathan	Ministry of Home Affairs
PANG	James	IGCI, INTERPOL
PARTHASARATHY	Arun	PAYPAL
PHILLIPPS	Tim	Deloitte
POH	Robert Sin Hock	FS-ISAC Singapore
ROY CHOUDHURY	Abhik	NUS
SASIK	Rastislav	IGCI, INTERPOL
SEEK	Connie	Singaporean Police Force
SCHLICKMANN	Silvino	IGCI, INTERPOL
SHU	Su Yen	National Research Foundation / PRIME MINISTER'S OFFICE
TANI	Masahiro	NEC
ULKUNIEMI	Kimmo	IGCI INTERPOL
VACCANI	Matteo	IPSG, INTERPOL
VAN DER HEIJDEN	Ferry	ING Bank
VIRMANI	Sanjay	IGCI, INTERPOL
VOLKERT	James	FBI
WIJAYATUNGA	Champika	ICANN
WONG	Allan	IGCI, INTERPOL