The Role of INTERPOL in a Geneva Convention or Declaration for Cyberspace

Report from the INTERPOL Global Cybercrime Expert Group Meeting, and INTERPOL World 2017, Singapore, July 5 -7, 2017

by
Stein Schjolberg
Chief Judge (Ret.)
Norway[1]
www.cybercrimelaw.net

1. Introduction

I was invited by INTERPOL as a participant at the INTERPOL Global Cybercrime Expert Group (IGCEG) Meeting in Singapore on July 5-7, 2017. Participants were also invited to attend the INTERPOL World 2017. Both events were held at the Singapore Suntec Convention Centre.

2. INTERPOL Global Cybercrime Expert Group (IGCEG)

2.1. This cross-sector group brings together experts from different cyber-related fields to provide advices including cyberstrategy, research, training, forensics and operations.

The purpose of the IGCEG is advice the INTERPOL General Secretariat in policy formulation and project implementation, regarding programs and operations related to the cyber arena. The objectives of the Group would thus be to serve as a forum for exchange of information and good practices, to assist the General Secretariat in developing strategy on cyber issues and to serve as advisory body to the General Secretariat on projects related to cyber matters.

2.2. The IGCEG Meeting was opened and delegates welcomed by the Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation, Singapore.

The Meeting before lunch break on July 5, included presentations on previous meeting recommendations and subsequent implementations, overview of the partnerships process and current outcomes, and a panel discussions.

---

[1] Judge Stein Schjolberg was an Ass. Commissioner of Police before he was appointed as judge. He served as a judge from 1984 and chief judge from 1989, including a Court of Appeal Judge from 2010 until he retired in August 2013. He was the Chairman of the High Level Experts Group (HLEG), at the United Nations International Telecommunications Union (ITU) in Geneva (2007-2008). He was the chair of the EastWest Institute (EWI) Cybercrime Legal Working Group (2010-2013). He was also a member of World Economic Forum´s - Partnering for Cyber Resilience (PCR) project (2012-2013).
See www.cybercrimelaw.net

The sessions after lunch break on July 5 and the whole day of July 6, included break out sessions for discussions in Sub-Groups. The discussions in each group were introduced by a Subject matter Expert introductory presentation.
I was invited to the discussions in the Research Sub-Group.

The July 7 Meeting included a plenary session and the presentation of reports from each Sub-Group, wrap up and conclusions by the Chairman of the IGCEG Mrs. Catherine Chambon, France, and Cybercrime Director Silvino Schlickmann.
Before closing the Meeting, the IGCEG Statutory updates was presented.

2.3. The Breakout Session for the Research Sub-Group continued for one and a half day of the IGCEG Meeting. The Sub-Group included members with both technical expertise and legal expertise.

2.4. Remarks: The IGCEG Meeting had more than 55 participants. The discussions for one and a half day were organized in 4-5 separate Sub-Groups where only members of each group could participate.

3. INTERPOL World 2017

The 2nd INTERPOL World 2017 was held on July 4-7, 2017, and with participation of 250 companies from around the world.
The event was presented as follows:
INTERPOL is uniquely positioned to provide a neutral multistakeholder platform at the international level to bring together the law enforcement community and industry sector to improve the effectiveness of policing strategies designed to prevent and investigate transnational crime. In its second edition in 2017, INTERPOL World (IW) will continue to be a strategic platform for the public and private sectors to discuss and showcase solutions to evolving global security challenges. This year, INTERPOL World aims to taket his principles of public, private cooperation forward by fostering a structured dialogue session between law enforcement, solutions providers and academia so that better methods and solutions of addressing the evolving crime landscape can be found.

The biennal four day event aims to connect lae enforcement, government bodies, academia and international security professionals with security solution providers and manufecturers. The event forsters mutually beneficial collaboration, information sharing, innovation and solutions to ensure faster and more accurate responses to security threats and foster innovation in policing. This event is supported by the Singapore Ministry of Home Affairs and the World Econimic Forum.

INTERPOL World 2017 was opened on July 4 with a Session called INTERPOL World Dialogue. It was a panel session to establish risks and opportunities in emerging technology in Cyberspace, and correlation between technology, connectivity and crime.

Remarks: The role of INTERPOL in global public-private partnerships was definitively confirmed in an outstanding way at the INTERPOL World 2017 in Singapore. More than 250 companies participated, including US companies such as Microsoft, Cisco and Symantec.

4. Proposal for a Geneva Convention or Declaration for Cyberspace

Cyberspace has created new opportunities for global cyberattacks on the infrastructures of sovereign states. The global cyberattacks may even constitute a threat to international peace and security, and need a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations.

Dialogues and cooperation between governments on norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient. International law is necessary to make the global society able to respond to cyberattacks.

In order to reach for a common understanding, a proposal for a United Nations Convention or Declaration for Cyberspace that includes solutions aimed at addressing the global challenges has been presented.[2] A Convention or Declaration for Cyberspace may be an initiative in Geneva by the International Telecommunication Union (ITU), and could be adopted by States at a Ministerial Summit in Geneva. ITU has the global leading role in coordinating international efforts on cybersecurity. A set of norms, rules, and standards in a Convention or Declaration for Cyberspace that should be discussed includes:

- *Standards for international cybersecurity measures;*
- *International coordination and cooperation through INTERPOL in investigation of transnational serious cybercrime;*
- *Standards for global partnerships with the private sector for the investigation and prosecution of serious cybercrime;*
- *Harmonize cybercrime laws;*
- *Establish an International Criminal Court or Tribunal for Cyberspace;*

A proposal for A Digital Geneva Convention has also been presented by the private sector. Microsoft¨s President Brad Smith, USA, has in February 2017 made the following statement:[3]

Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet's first responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust.

---

[2] Stein Schjolberg and Solange Ghernaouti: *A Geneva Convention or Declaration for Cyberspace,* VFAC Review, No. 12, October 2016, Korean Institute of Criminology, see https://eng.kic.re.kr and www.cybercrimelaw.net

[3] Brad Smith, President of Microsoft: *The need for a Digital Geneva Convention*, RCA Conference, San Francisco, February 2017, see https://blogs.microsoft.com

5. International coordination and cooperation through INTERPOL in investigation of transnational serious cybercrime

INTERPOL has since the The First Interpol Training Seminar for Investigators of Computer Crime, in Saint-Cloud, Paris, December 7-11, 1981,[4] been the leading international police organization on global prevention, detection and investigations of cybercrime.

INTERPOL is committed to be a global coordination body for the prevention and detection of cybercrime through its INTERPOL Global Complex for Innovation (IGCI) in Singapore. INTERPOL seeks to facilitate global coordination in cybercrime investigations, and provide operational support to police across its 190 member countries.

It is very important that the investigators of cybercrime may swiftly seize digital evidence while most of the evidence is still intact. It is vital that the police have an efficient cross-border cooperation when cyberattacks involves multiple jurisdictions. The Executive Director Noboru Nakatani, INTERPOL Global Complex for Innovation in Singapore, made in 2016 the following statement:[5]
"Due to bilateral relations between Russia and USA, a joint task force is not feasible, but through Interpol, it happened. Under the umbrella of Interpol, people are motivated to work together to combat cybercrime. Combating cybercrime is not about competition, its about cooperation and collaboration."

INTERPOL organizes international conferences together with Europol on cybercrime every year, and these INTERPOL-Europol Cybercrime Conferences was first held in The Hague in 2013.

The last INTERPOL-Europol Cybercrime Conference 2016 was held in Singapore on September 28-30. 2016. It was especially emphasized the following statements:

- *Law enforcement agencies and private sector companies to consider and find solutions to address respective constraints when investigating cybercrime.*
- *Supporting user-focused initiatives such as 'No more ransom', a multi-stakeholder project which aims to help victims of ransomware retrieve their encrypted data without paying their attacker.*
- *INTERPOL and Europol to support existing entities in their establishment of regional cyber centres via capacity building and information sharing.*

The next conference will be held in The Hague on September 27-29, 2017.

---

[4] The conference was organized by Interpol in co-operation with Ass. Commissioner of Police Stein Schjolberg, Norway, and was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.
[5] Nakatani, Noboru, January 2016 Statement at the Emtech Asia 2016,
see http://scamsurvivors.com/forum/viewtopic.php?f=4&t=42714

6. Standards for global partnerships with the private sector for the investigation and prosecution of serious cybercrime

The possible development of a Geneva Convention or Declaration for Cyberspace should include a common understanding of the need for standards on global public-private partnerships for the investigation and prosecution of global cyberattacks and other serious cybercrime.

Preventing and combating cross-border or cross-regional cybercrimes, demands coordinated and collaborative public-private partnerships across nations. Law enforcements and prosecutors should have the power through INTERPOL to seek the most efficient assistance and partnership from experts, established with key stakeholders in the global information and communications technology industry, financial service industry, private sector, non-governmental organizations, and academia. Partners and experts in the investigation and prosecution of global cyberattacks and other cybercrime should be working together in a strong partnership, to coordinate, integrate and share information for the prevention and effectively combating global cybercrimes, especially for delivering real-time responses.

A basic platform must be the coordination and open sharing of knowledge, information and expertise between the stakeholders that may result in fast and effective investigative measures. A partnership should avoid dealing with classified information, in order to share information and knowledge more freely with the private sector.

INTERPOL understands that the cyber expertise in the future will be external to law enforcement, and are found in the private sector and academia. INTERPOL describe the role in private partnerships as follows:
As criminals are constantly evolving and adapting their tools and methods, INTERPOL works to develop new cutting-edge policing tools in consultation with partners in the cyber industry, and tests new private technologies with a view to their use by law enforcement.

INTERPOL Global Complex for Innovation in Singapore has established Strategic Partnerships[6] with some public and private institutions:

- *Entrust Datacard Group, a U.S. based company;*
- *Kaspersky Lab, headquarters in Moscow, and registered in UK;*
- *Morpho, a company based in France;*
- *NEC, Corporation, a company based in Japan;*
- *Trend Micro, a company based in Japan;*

At the Cyber Fusion Centre in Singapore, several partners and other experts from the private sector and academia are working together, from such institutions as Barclays Bank, Cyber Defense Institute, Kaspersky Lab, LAC, NEC, SECOM, Trend Micro, Univeristy of South Australia, and University of Waikato, New Zealand. A partner agreement was in July 2017 also signed with the PaloAlto Networks, California, USA.

---

[6] See www.interpol.int/About-INTERPOL/International-partners/Strategic-Partners

These partnerships are necessary to accomplish a goal that would be impossible to achieve independently, and provide expertise that would not otherwise be available to INTERPOL member countries.

INTERPOL and Europol Cybercrime Center (EC3) have in cooperation been organizing the INTERPOL - Europol Cybercrime Conference each year since 2013. More than 350 cyber experts from around the world, including many from the private sector and academia are attending the conferences. Several of the speakers are also representing private companies, such as Barclays Bank, SNS Bank, Symantec Corporation, and Microsoft.