
INTERPOL WORLD 2019

ENGAGING CO-CREATION FOR FUTURE SECURITY THREATS

# Final Report

# Table of contents

## INTERPOL WORLD 2019

At a glance…

- 6228 visitors to the exhibition; among them government leaders, senior law enforcement representatives, academics and security professionals from commercial sectors
- 656 attendees to Co-creation Labs, representing 52 INTERPOL member countries
- 114 speakers and moderators from 34 countries
- 45 supporting associations
- 47 supporting media organizations
- 32 Co-creation Labs
- 4 INTERPOL Working Groups

# Executive Summary

Interpol World 2019, was a leading Global law enforcement event, that drew together police, and likeminded agencies, academia, industry and government together to co-create on issues and activities that are and will impact on the public safety and security of the communities for which law enforcement and Governments are charged to protect. Unlike any other Global conference or event, this event provided a unique environment for all participants to actively engage and work with each other to scope and define the challenges that police are facing and develop actions plans for further work and activities that need to be undertaken to ensure that law enforcement under the umbrella of INTERPOL is best positions to face the challenges of the future.

The event was organised by INTERPOL Innovation Center, with a daily keynote speaker that set the stage for each of the daily focuses, drawing experts across academia, law enforcement, and industry to provide insights into the problems and challenges that exist and are evolving across society, then with the collective awareness of these problems, the participants worked through the challenges guided by expert moderators aim at developing an action plans.

A synopsis of each of he action plans are detailed in this document, with the outcomes of the four INTERPOL Working Groups. For our Police Leaders the opportunity for you now is to consider these plans, look at how you need to position your police agencies for the future, and be aware that the capabilities and capacity required for law enfocement for the future needs to be planned and actioned, Today!

INTERPOL will endeavour to action the outcomes of this event through the INTERPOL Global Innovation Agenda, but to do so INTERPOL will need the support, involvement and commitment of all 194 member countries, academia and relevant industry. Together we can make a difference.

# About INTERPOL World

INTERPOL World is a biennial event owned by INTERPOL and supported by the Singapore Ministry of Home Affairs and the Singapore Exhibition and Convention Bureau. Bringing together experts from a wide range of backgrounds, INTERPOL World is providing unprecedented opportunities for national law enforcement, border and security agencies, security professionals and academia to interact with private industry on public safety and security issues.

The two previous INTERPOL World events in 2015 and 2017 fostered a vibrant exchange of best practices, experiences and technologies. In 2019, the third edition, organized by INTERPOL Innovation Centre (IC), took place from 2 to 4 July with the theme *"Engaging Co-Creation to Prepare for Future Security Threats*." It seeks to enhance the awareness of emerging security and crime issues that the 194 member countries of INTERPOL will face by looking at:

1) Global Safety Today (Day 1)
2) Improving Security for Tomorrow (Day 2)
3) Forecasting and Planning for the Future (Day 3)

To facilitate the above-mentioned themes, INTERPOL World 2019 included the following components:

1) 32 Co-creation labs that focused on exploring solutions to particular real-life law enforcement problems. Law enforcement officers, industry experts, and academics engaged in fruitful discourse to identify challenges and innovative solutions to security threats.
2) A series of international working groups, empowering law enforcement agencies with useful data and tools to continuously improve and strengthen relationships with the communities they serve.
3) Plenary sessions for motivational keynote speakers elaborating on perspectives for the future and new capabilities aiding security and public safety.
4) Exhibition for the industry partners to present their capabilities and services.
5) Networking events

# Report Overview

This document serves as a final INTERPOL World 2019 report, prepared for the broad audience of INTERPOL's 194 member countries, law enforcement agencies, academia, and industry. It aims to present the activities which took place during INTERPOL World 2019, highlighting the key recommendations and outcomes.

It comprises six sections that correspond with the content of INTERPOL World 2019.

The first section of this report, Outcomes, enumerates the observations and findings identified from the discussions that transpired during the various activites of INTERPOL World 2019 and outlines the next steps on how to strengthen innovative and agile global law enforcement.

Section II provides transcripts of the speeches of distinguished guests who graced the opening ceremony of INTERPOL World 2019: Singapore Minister for Manpower and Second Minister for Home Affairs Josephine Teo, INTERPOL President Kim Jong Yang, and INTERPOL Secretary General Jürgen Stock.

Section III reflects on the three motivational keynote speeches delivered by Mr Richard van Hooijdonk, Dr Ayesha Khanna, and Dr Mary Aiken.

The fourth section of this report provides an overview of the discussions held within the 32 co-creation labs which are presented in accordance with the order they appeared under the INTERPOL World 2019 schedule of activities. In a novel way, the co-creation labs brought together speakers from law enfrorcement, industry, and academia to discuss new and emerging policing issues. The speakers for each co-creation lab worked hand-in-hand to translate existing theories and commercial solutions into action-ready recommendations as well as to share the ways of scaling them up to identify a range of solutions.

Section V is a summary of activities and outcomes of the four international working groups on drones, Darknet and cryptocurrencies, innovation, and AI that convened during their respective meetings at INTERPOL World 2019.

Section VI details the way ahead that needs to be progressed post this event, and introduces the Global Innovation Agenda, a coodinated program of activities that will progress the actions plans in partnership with the 194 member countries, academia and industry.

# I: Outcomes

*INTERPOL World is a global co-creation event, which engaged the public and private sectors in dialogue, in order to foster collaboration to counter future security and policing challenges.*

## Through the discussions during INTERPOL World 2019, the following outcomes emerged:

(a) The policing landscape will be more ambiguous and demanding because of the impacts and substantial influence of technology on law enforcement. An example of this is the imminent big wave of social change resulting from the rollout of 5G which connects all technologies. Thus, new forms of crime will emerge.

(b) There is an urgent need for hitherto underexposed constitutional and ethical perspectives in the field of innovation and technology.

(c) There are enormous changes and ethical challenges that Artificial Intelligence (AI) brings and thus there is a need for a global framework for the use of AI by law enforcement.

(d) There should be increased global cooperation among law enforcement, business, and academia, and INTERPOL can play an important role in this.

(e) In order for law enforcement to orient themselves strategically for the next several years and choose the right direction, a 10-year horizon scan for the future is crucial. This is linked to the necessity of knowledge gathering for new phenomena/trends with law enforcement taking a position in regard to these developments so that they can be better prepared for the future.

(f) The current (often non-digital native) leadership of the police must be inspired by young people and experts ('reverse mentorship') because otherwise they are unable to make timely and radical change and lead digital transformation.

The above-mentioned lessons learned from INTERPOL World 2019 served as a springboard for the creation of a coordinated program of activities known as the INTERPOL Global Innovation Agenda, that will progressed the action plans of the co-creation labs from this event.

*INTERPOL World 2019 sought to enhance the awareness of emerging security and crime issues by looking at:*

- *Global safety today;*
- *Improving security for tomorrow;*
- *Forecasting and planning for the future.*

# II: Opening Ceremony Speeches


## Mr Kim Jong Yang, President of INTERPOL

Opening the third edition of INTERPOL World, Mr Kim Jong Yang welcomed all the guests on behalf of INTERPOL and expressed his gratitude to the Singaporean authorities for the extensive support they have provided in organizing this event. Asking a simple, yet critical question "**Are we ready for the future?**" President Kim suggested that the answer lies within ourselves as INTERPOL is engaging all stakeholders to build a bridge between the present and the future.

The opening speech focused on the cooperation of law enforcement with various stakeholders to tackle new challenges to our collective security in the face of the systemic disruptions brought about by our era's technological leaps. President Kim highlighted that in addressing technology-enabled crimes, private sector actors take center stage: either as potential targets or as partner responders. By calling attention to terrorist fundraising online and recent ransomware attack disrupting operations, INTERPOL's President addressed one more critical question: **will we be ready for the next disruption?**

Our future will see more connected objects permeating the physical space and bridging the gap to cyberspace; unmanned technology entering the civilian and criminal mainstream; and more systems being managed by ever-evolving artificial intelligence powered by machine learning. The emerging changes will accelerate the ongoing race between cyber criminals and cyber security providers. Law enforcement success in meeting the challenges that our governments and our businesses face is conditional on our capacity to communicate, and collaborate with one another. President Kim suggested that partnering with the private sector – while maintaining independence and transparency for police action – and working closely with academia and research institutions is the way forward for INTERPOL. The knowledge, skills, and creativity of the private sector, manufacturers, and research and development specialists are essential to enhancing our capacities to prevent and react to the next threat. This is what INTERPOL World brings: **by co-creating today, it prepares the law enforcement for the challenges of tomorrow.**


## Mr Jürgen Stock, Secretary General of INTERPOL

Secretary General Jürgen Stock, reflecting on the two previous editions of INTERPOL World, discussed **law enforcement's growing relationship with industry**. With INTERPOL soon entering its bicentennial anniversary, Mr Stock stated, "we are laying the foundation today for a new century of global policing, where cooperation and partnerships are of pivotal significance".

Mr Stock pointed out the fact that technology has evolved at such a rapid pace, that yearly trend predictions are largely failing to anticipate what will hit us next. With the innovation tempo soaring, the reaction time police can afford is plummeting – to the point where reaction is simply not an option. **We must foresee, anticipate, and prepare for the next breakthrough.**

He further discussed the role of industry, increasingly crucial in building new solutions and acquiring an in-depth understanding of emerging threats, and the most significant areas of partnership with the private sector, such as cybercrime. This forward-looking work, which is also at the core of INTERPOL World, provides essential insights into the outstanding challenges holding police back in effectively adapting to an ever-evolving threat landscape. Speed of responses to technological disruptions and differences in national and regional legal frameworks were recognized as among the biggest obstacles for law enforcement.

Concluding his speech, Mr Stock once again emphasized how crucial it is to keep the industry-law enforcement dialogue open - and highlighted INTERPOL World's importance in this process.

## Guest of Honour Mrs Josephine Teo, Minister for Manpower and Second Minister for Home Affairs

Minister Teo focused on **thought leadership in law enforcement**, emphasizing INTERPOL World 2019's role as an important platform to explore innovation in the global policing and security eco-system. Pointing out strategic directions for future challenges and opportunities in policing, Minister Teo discussed today's complex security environment, placing a great emphasis on the **nexus with international collaboration.**

In her speech, Minister Teo mentioned that what is bringing us together is the new challenges that could disrupt law and order across the globe, posing threats to all of our societies. With crime-fighting reaching unprecedented levels of complexity, we need new strategies to protect our people.

Minister Teo highlighted three developments which are re-shaping the security landscapes in all of our countries: increasing global connectivity, technology, and the polarization of societies. Discussing the pros and cons of the aforementioned changes, Mrs Teo emphasized the importance of information sharing in order to understand the full nature of emerging problems.

Given the importance of innovation in policing, the Singapore MHA has made it a priority to reinforce science and technology capabilities. While discussing these improvements, Minister Teo examined three particular areas that hold promise for international crime-fighting: biometrics, data analytics, and digital forensics.

In conclusion, Minister Teo reiterated that Singapore looks forward to being a part of a vibrant innovation ecosystem, which INTERPOL and IGCI in particular are also plugged into.

# III: Motivational Keynotes - Reflections

**Mr Richard van Hooijdonk**

**(The Netherlands)**

*Trendwatcher, futurist and international keynote speaker*

## Is Rapid Technological Change a Threat to Our World and What Can We Do to keep up with the Fast Pace of Change?

Taking law enforcement forward in a fast-changing world poses new challenges but also creates opportunities. Renowned futurist Mr Richard van Hooijdonk delineated how technology can outpace the capacity of the policing community if we don't adapt to the changes that new technologies bring about, as they can affect labor markets, and raise new ethical questions. Therefore, in dealing with technology we need to consider a code of ethics and standards as well as the technology capabilities that are provided.

According to Mr van Hooijdonk, change is all about the mindset – innovations fail because of the lack of an open mindset, and this is where we should concentrate our efforts. Change models for law enforcement should consider both optimization and disruptions. Senior management should also consider what Skills are needed in today's environment, and how passion, curiosity, adaptiveness, and resilience are placed on the list of priorities.

Mr van Hooijdonk highlighted that it is important to introduce a new type of law enforcement management, creating an ecosystem where law enforcers, businesses, different organizations, and diverse talents can collaborate.

Our keynote speaker emphasized that in today's fast-changing environment, resilient, adaptive, and flexible organizations and having an "only-the-paranoid-survive" mindset are vital. We should therefore be open to "reverse mentoring" where the young teach their older colleagues.

In conclusion, Mr van Hooijdonk pointed out that in the next 5 years, we will have more changes than the last 50 years. To motivate and inspire, the following transformations should occur:

- Positions become roles
- Managers become coaches
- Departments and hierarchies should turn into teams.

## Dr Ayesha Khanna

**(Singapore)**

*Co-Founder and CEO of ADDO AI, an artificial intelligence (AI) solutions firm and incubator*

# Ethics and Privacy Issues in a Digitally Enhanced Society: Do We Forego Privacy

**Innovation in new technologies like AI can be a double-edged sword** was the opening statement of Dr Ayesha Khanna, strategic advisor on artificial intelligence, smart cities and fintech to leading corporations and governments.

In order to control the problem, she highlighted the necessity of asking the right questions: **how do we govern AI so that it is not used with maleficent intent? How do we communicate with the public so that they trust us in our intent?**

The law enforcement community has to keep in mind that with great power comes great responsibility. We should be open to innovation but cautious at the same time. For example, solutions employed by the private sector, such as personalized recommendations, might not always work for the justice system.

In her speech, Dr Khanna also discussed executing AI governance in practice. From the law enforcement perspective, the change of criteria for judging AI technology products has to address data bias and sufficient privacy protection. Understanding the process flow (explain ability) of data and AI modeling is crucial for governance inspections. Among the benefits of explainable models are fairness, de-bugging models, and contesting them if needed – all of these factors are essential for building the trust between the police and societies. Governance must be accompanied by communication and accountability – trust needs to be reinforced in new circumstances like AI. Singapore for example has made AI governance a priority, declaring cybersecurity, data protection and ethics of algorithms as their priority.

Dr Khanna reminded the audience that **to make AI human-centric is not only a technical undertaking** – in order to succeed, we need multi-disciplinary teams specialized in a holistic approach to emerging crime. In line with the adage “knowledge is power,” domain expertise and experience will amplify law enforcement potential and facilitate decision-making capabilities.

**Dr Mary Aiken**

**(United Kingdom)**

*Cyberpsychologist and academic advisor*

## Future of our Communities and Our Societies: What is Likely to Occur and What Do We Need to Do to Ensure Public Safety and Maintain Security?

Recent developments in **online interactions impacted and altered our behavior**, resulting in changes to the social fabric. As a result, **new types of challenges and criminal activities arose**. Our third keynote speaker, Dr Mary Aiken, mapped out the cyberpsychology ecosystem, identifying new trends and implications for policing.

While elaborating on the impact of anonymity and online syndication, Dr Aiken discussed the online disinhibition effect, as well as the diminishing status of authority online as some of the key reasons why we observe cyber delinquent, deviant, and criminal behavior. Furthermore, due to anonymity and online disinhibition, deviant and criminal populations can find each other with ease ("online syndication"). This phenomena in turn may drive new incidence of deviant, criminal, and abnormal behavior in the general population. Dr Aiken further focused on the challenges brought about by cyberspace, such as the 450% increase in serious sexual assault and rape reports related to online dating.

In order to tackle new and emerging online crimes, law enforcement should focus on three specific constructs related to securing the future of cyber society:

- Aim of privacy
- Aim of collective security
- Aim of vitality of the tech industry

The key objective for the police community is to achieve balance – none of these aims should have primacy over the others. We should also keep in mind the potential "tsunami of criminality": we should try to move policy forward to deal with the intensity and velocity of this forthcoming escalation. **The solution lies in society's collective responsibility and collective actions.**

# IV: Co-creation labs

As INTERPOL World 2019 focuses strongly on thought leadership in law enforcement, 32 co-creation labs were organized. Every lab had speakers from three distinct yet interconnected worlds: law enforcement, industry, and academia.

In each of the labs, law enforcement officers collaborated with industry experts and academics to identify contemporary policing challenges and explore ways to face such challenges. Through co-creation, we ensured an easily accessible platform for everyone keen to contribute and share ideas, comment on them, and address future problems and opportunities.

This section presents the co-creation labs in accordance with the order they appeared under the INTERPOL World 2019 schedule of activities. Despite the shared format and structure of having a moderator, speakers from law enforcement, academia, and industry, and audience members were encouraged to actively participate in defining and driving concepts through to action. It should be noted that each lab had their own characteristics in terms of audience composition, discussion flow, and dominant themes. Thus, variation in the number of key recommendations, takeaways, highlighted information, and identified INTERPOL projects related to the lab topics should be expected.

## Co-creation labs for Day 1 (2 July 2019)

### 1. Drones

The speakers discussed the most salient issues pertaining to UAVs as threat, tool, and opportunity for law enforcement and attempted to address questions on promoting safe flying and countering drone exploitation.

Drone data use in digital forensics was also discussed:

- Data information can be used for sharing and planning
- Managing drone incident
- Other agencies able to tap into the drone data

*Key recommendations*

- Provide standard procedures and protocol countries can follow.
- Educate the public on the dos and don'ts as well as the consequences of drone use.
- Build trust and understanding between law enforcement agencies and the public in their use by law enforcement.

*Co-creation lab speakers:*

Superintendent Justin Burtenshaw,
Head of Protective Security and Firearms, Sussex Police (United Kingdom)

Ms Brooke Tapsall,
CEO DroneALERT & Agis (Australia)

Mr Ryan English,
CEO Flymotion (United States)

*moderator*

Mr Mark Bond,
Principle consultant, The institute for Drone Technology (Australia)


*Drones co-creation lab speakers*

*INTERPOL Innovation Centre*
*is actively working in the area of Unmanned Aerial Vehicles*

Digital Forensics Lab (DFL) produced a whitepaper on drones (2018) and the INTERPOL Framework for Responding to a Drone Incident – for First Responders and Digital Forensics Practitioners (2019).

Furthermore, DFL organized a number of meetings, such as Drone Meeting - Lyon, France 2017, Drone Meeting- Colorado, USA 2018 (resulted in creation of Drone Framework) and Drone Expert Group - Singapore 2019

*Co-creation lab speakers:*

Mr Christopher M. Piehota, Executive Assistant Director, Science and Technology Branch, FBI (United States)

Mr Yuri Gubanov, CEO, Belkasoft (United States)

Ms Zsuzsanna Felkai-Janssen, Head of Sector and DG Coordinator for AI, European Commission (European Union)

*moderator*

Mr Shong Ye Tan, Parnter, Cyber and Digital Trust Leader, PwC (Singapore)

## 2. Regulating Big Data

In today's data-centric society, the ability to serve and protect communities is contingent upon access to data. Law enforcement agencies and legal representatives are not keeping up with the speed of technological change, affecting their ability to use data efficiently.

Inevitable changes such as the deployment of 5G will only increase the amount of data at law enforcement's fingertips. Furthermore, changes in social attitudes have implications on how police collect and use data. New technologies have better computing capabilities and thus can perform better data gathering processes. However, there are expectations from the public on how gathered data are used.

With the current challenges in handling big data, current laws and regulations across countries do not cope with fast-paced changes in technology, and increase in data generation; Law enforcement needs to work with their governments and respective stakeholders to develop enhanced data management regulations and laws that improver access, analysis, and protection of unstructured data.

Data and technology companies are capturing and using information like never before, and have used the data to manipulate public opinion and target communications, but they at times are reluctant to share identified criminal information under the guise of privacy. Building trust collaboration and mechanisms for sharing of information is needed to ensure that community public safety and security concerns are maintained.

### *Key recommendations*

- Create common principles and standards for big data usage between private organizations and police
- Develop improved standards and mechanisms for the sharing of data across countries as required
- Build the trust in data storage and usage across all key stakeholders.

*Ms Zsuzsanna Felkai-Janssen, Head of Sector for Migration and DG Coordinator for Artificial Intelligence at European Commission Belgium: what are the privacy and protection implications to public safety and security?*

## 3. Partnerships

Borders do not exist for cybercrime, thus, partnerships and cooperation are crucial. Assistance from private partners who have access to more information are also needed. According to the speakers, law enforcement agencies certainly need to re-think the most prevalent paradigm: policing doesn't have to be exclusively executed within national jurisdictions.

Challenges such as fast paced technology, lack of clear legislative and a clear policy framework for the sharing of information, lack of trust between parties, limits placed on human resourcing and budget, all present distractions to the effective and timely sharing of information that could prevent harm and mitigate the impacts of crime across our communities.

We need to work together to make a difference focusing on proactive initiatives rather reactive responses, so that we can disrupt criminal activity and mitigate harm.

### *Key recommendations*

- Create a framework to ensure a smoother transition of information flow
- Bolster international partnerships especially in relation to tackling cybercrime
- Increase partnerships with financial institutions
- INTERPOL needs to raise cybercrime higher on its agenda
- Come up with measures to bridge the gap between public sector and the industry


Police Commissioner, Kristin Kvigne, Head of Policing Department, National Police Directorate, Norway

### *Co-creation lab speakers:*

Ms Kristin Kvigne, Police Commissioner, Head of the Policing Department, National Police Directorate (Norway)

Mr Anton Shingarev, Vice President for Public Affairs, Kaspersky Lab (Russia)

Mr Wouter Veenstra, Head Outreach and Partnerships, Global Forum on Cyber Expertise (GFCE) (The Netherlands)

*moderator*

Mr Peter Brown, Change Manager, National Criminal Intelligence System Program, Australian Criminal Intelligence Commission (Australia)

## 4. Protecting Children

*Co-creation lab speakers:*

Mr Jon Rouse, Detective Inspector, Queensland Police Service (Australia)

Ms Anna Borgstrom, CEO, NetClean Technologies (Sweden)

Dr Michael Salter, Associate Professor of Criminology, University of New South Wales (Australia)

*moderator*

Mr Paul Stanfield, Director Organised and Emerging Crime Directorate, INTERPOL

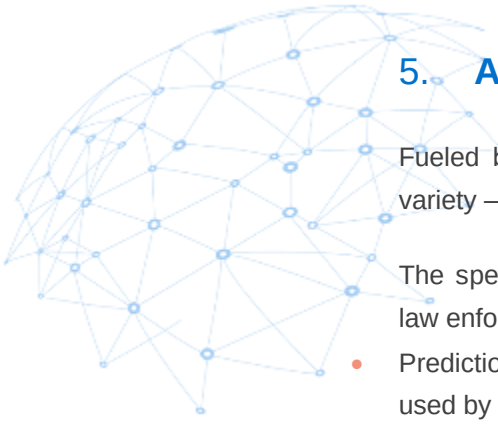
The co-creation lab participants discussed the following:

- Lack of industry regulation: Tech companies not required to abide by proactive child protection frameworks; industry aim to reduce liability and risk (rather than improve child safety) in accordance with underlying business model (companies aim to make profits, not protect children)
- Need for an integrated code of conduct, in order to facilitate introduction of legislation and strengthening of legal power
- Existing and future cooperation between the corporate world and law enforcement to deter crimes committed against children

### *Key recommendations*

- INTERPOL should promote responsible use of technology
- Encourage making use of technology (connectivity and AI) in investigation and prosecution
- Industry should take the responsibility and be more proactive in the area of child protection, introducing and promoting ethical leadership.

*INTERPOL's Child Sexual Exploitation database holds more than 1.5 million images and videos and has helped identify 19,400 victims worldwide.*



## 5. Artificial Intelligence

Fueled by the three 'V's of big data – velocity, volume, and variety – AI tools are being deployed across the security sector.

The speakers identified the following AI-based applications in law enforcement:

- Prediction and Analysis – automatic text analysis by AI (mainly used by law enforcement)
- Recognition – video and audio analysis
- Exploration - surveillance on crime trends by using drones
- Communication

Law enforcement is indisputably one of the area's most immediately affected by AI. It is an active target and an area that is getting more vulnerable due to the increasing use of AI for critical tasks. AI can help to close the information gap, as well as assist providers to better assess risk.

### *Key recommendations*

- Create an AI security compliance programme in order to reduce the risk of AI-powered systems attack and lower the impact of successful ones
- Help to bring the infrastructure, such as legal, social, governance of models, testing, transparency, and understanding, up to speed with the technical capabilities of AI
- Encourage regulators to require compliance for law enforcement's use of AI systems and pre-condition for selling or creating systems for law enforcement
- Encourage stakeholders to cooperate to employ AI for fighting crimes against children

INTERPOL

INTERPOL Innovation Centre is also supporting law enforcement efforts in ensuring effective but also ethical use of AI in policing. The Centre's Adaptive Policing Lab has the following initiative:

- 2nd INTERPOL-UNICRI AI for Law Enforcement Joint Report (2019)

*AI co-creation lab speakers and moderator*

*AI co-creation lab participants*

*Co-creation lab speakers:*

Mr Lindeberg Leite, Federal Criminal Expert, Federal Police of Brazil (Brazil)

Mr Hong-Eng Koh, Global Chief Public Safety Scientist, Huawei Technologies Co Ltd (China)

Mr Graham Ong-Webb, Vice President, Head of Future Technology Centre, ST Engineering (Formerly Research Fellow, RSIS) (Singapore)

*moderator*

Mr Irakli Beridze, Head, Centre for Artificial Intelligence and Robotics, United Nations Interregional Crime and Justice Research Institute (UNICRI)

*Co-creation lab speakers:*

Chief Superintendent Yve Driesen, Judicial Police, Belgian Federal Police (Belgium)

Ms Rosita Jupri, Cybersecurity, Principal Engineer, TUV-SUD Asia Pacific Pte Ltd (Singapore)

Mr Niels De Boer, Programme Director, CETRAN, Nanyang Technological University (Singapore)

*moderator*

Mr Peter Brown, Change Manager, National Criminal Intelligence System Program, Australian Criminal Intelligence Commission (Australia)

## 6. The Connected Car

The most significant benefits to automating cars is the ability to control the flow of traffic, extended information captured, vulnerabilities in the system that can be exploited by criminals, and to take responsibility for accidents caused by self-driving vehicles.

The speakers highlighted the following challenges for law enforcement related to autonomous cars:

- Hacking
- Reckless driving
- Accident investigations
- Terrorism

Additionally, they also elaborated on the potential consequences of cyber attacks such as:

- Driving function failure (e.g. brake systems)
- Vehicle theft (e.g. lost of vehicle)
- Vehicle system failure (e.g. dysfunctional door locks)
- Data theft (e.g. personal data, vehicle data, classified data)
- Commercial loss (e.g. brand damage, revenue loss)
- Collision (e.g. liability questions, deaths or injuries due to collision)
- Other system failures (e.g. manipulated navigation)

### Key recommendations

- Provide operational technical support
- All-round knowledge assistance
- Encourage active public-private partnerships
- Develop measures against vehicle-related cybercrime
- Support an online platform where law enforcement and private sector can share information without jurisdictional boundaries, in a secure and timely manner
- Develop Ethics and responsible guidelines for industry and law enforcement to support policing activities

**Connected car meetings organized by the INTERPOL Innovation Centre:**

- Vehicle Forensic Expert Forum – Brussels, Feb 2019
- Car Cyber Threats Expert Group – London, Sept 2019
- Car Forensics Training for Law Enforcement – London, Sept 2019

*Co-creation lab speakers:*

Mr Patrick Stevens, Director Counter-terrorism Unit, INTERPOL (Belgium)

Mr Walter Lee, Government Relationship Leader, NEC (Singapore)

Mr Donato Colucci, Senior Regional Immigration and Border Management Specialist, International Organization for Migration, Regional Office for Asia and the Pacific (Thailand)

*moderator*

Mr Ged Griffin, Senior Research Advisor, Centre for Disaster Management and Public Safety, University of Melbourne (Australia)

## 7. ISIL/DAESH 2.0

For a few years now, law enforcement has been expressing concerns about foreign fighter returnees becoming active again upon their release from prisons. Advising on this issue, security experts are emphasizing the importance of accurate biometric data collection. This co-creation lab focused on the use of biometrics in countering terrorism. The lab speakers discussed how to collect and use biometrics, and whether technological improvements alone are enough.

Main themes discussed included:

- Difficulties in data integration across different systems. Issues of legacy systems, data migration, and generational leaps must be treated as priority.
- A need for clear rules of engagement and workflow for authorization of access to data as key elements in systems that can support inter-agency collaboration.
- Effective counter-terrorism responses which require collective and coordinated actions by states – what kind of support and facilitation can relevant international and regional organizations offer.

### *Key recommendations*

- Advocate for improving border management technology
- Facilitate information sharing
- Enable interagency collaboration
- Build trust through assisting in developing national strategies

INTERPOL

INTERPOL pioneered military-to-law enforcement information exchange (Mi-Lex), starting in 2005 with **Project Vennlig** in Iraq, and later in Afghanistan through Project Hamah

**Project FIRST** (Facial, Imaging, Recognition, Searching and Tracking) will also be a key area for development at the national level across the G5 Sahel countries.

In addition**, INTERPOL's databases** currently hold details of more than 50,000 foreign terrorist fighters, 3,500 bomb-makers and some 400,000 pieces of terrorist-related information.

*Co-creation lab speakers:*

Dr Madan Mohan Oberoi, Executive Director, Technology and Innovation, INTERPOL (India)

Mr Christian Karam, Executive Director, CISO APAC, UBS AG (Singapore)

Mr Mark P. Pfeiffer, Chief Visionary Officer, SAIL LABS Technology GmbH (Austria)

*moderator*

Ms Amelia Green, Chief Digital Officer, PwC (Singapore)

## 8. Data Fusion

Perhaps the infosphere's most difficult aspect to grasp is the sheer scale of data that feeds it. Ninety percent of the data produced in the entirety of human history has been procured in the past 30 months. A data tsunami is brewing.

One of the biggest challenges law enforcement is facing is the development and implementation of effective strategies for data sharing and management. The critical role of INTERPOL is to bridge the private and public sector to create the means to build a circle of trust and initiate formal legal frameworks.

### *Key recommendations*

- INTERPOL should provide a trusted global platform for information sharing.
- Agencies should improve the ways they leverage on technology such as machine learning to filter false and unverified information.

*Data fusion co-creation lab speakers and participants*

## 9. Cybercrime

The development of technological innovations, which facilitate everyday lives, also make a significant contribution to criminality. Cybercrime, though not well defined to date, has become a serious problem globally. Possibly the greatest concern to member countries, however, is the ability of cybercriminals across the globe to use the internet for purposes of terrorism.

The experts began discussion with challenging criminal justice's responses, which are usually a case of "too little, too late". Changing definitions of policing work, legislation related to cybercrime and effective ways of collaborating with the industry were among the key points of this exchange. Speakers tackled issues of improving governance in the security and defense sectors through strengthening of institutions, cross-agency collaboration to combat transnational threats including transnational organized crime, trust-building actions, and mutual understanding on common defense and security challenges.

### *Key recommendations*

- INTERPOL - Regional desks – more cooperation and sharing between member counties and INTERPOL to support the outcomes and needs of all stakeholders
- Provide operational support but also all-round knowledge assistance
- Promote ethical and responsible behavior of industry to support law enforcement operations
- An online platform where law enforcement and private companies can share information without jurisdiction boundaries, in a secure manner knowing that the information comes from a legitimate source.

*Co-creation lab speakers:*

Mr Craig Jones,
Director, Cybercrime,
INTERPOL (United Kingdom)

Mr Naveen Bhat,
Managing Director, Ixia Solutions Group, Keysight Technologies (Singapore)

Dr Shenkuo Wu,
Law Professor, Beijing Normal University (China)

*moderator*

Mr Ged Griffin,
Senior Research Advisor, Centre for Disaster Management and Public Safety, University of Melbourne (Australia)


*Cybercrime co-creation lab speakers and moderator*

*Co-creation lab speakers:*

Mr Derek Bassler, Special Agent and Program Manager, Homeland Security Investigations, U.S. Immigration and Customs Enforcement (United States)

Mr Mark Robinson, Director, Global Security APAC, Pfizer (member of INTA) (Thailand)

Prof Kwok Yan Lam, Professor, School of Computer Science and Engineering, NTU (Singapore)

*moderator*

Mr Wayne Towson, Senior Director, Global Security, Threat Intelligence and Information Sharing, Abbott Laboratories (United States)

## 10. **Counterfeits**

Illegal online pharmacies pose a threat to the public by providing easy access to substandard, counterfeit, and falsified pharmaceuticals.

The involvement of organized crime in this type of trafficking requires close international police cooperation to identify the criminal networks engaged in this crime.

Speakers highlighted the emerging trend of using blockchain for industry sensitive assets, at the same time agreeing that while this solution can help to weed out some of the rouge traders, it will not solve the problem. Blockchain is currently deemed to become the way forward to secure the supply chain ecosystem and increase traceability and authentication of products.

Currently, several companies are already working together on developing an interoperable transparent system which can identify all parties involved in the transaction up to the pharmacy level and secure immutable audit trails.

### *Key recommendations*

- Establish working groups involving regulators, academia, and law enforcement agencies.
- Encourage and support implementation of international standards of proving authenticity.
- Consideration be given to understand why there is a need for blockchain in these circumstances and for the process to go across the entire product supply chain.

## 11. Future Capabilities and Cultures

*Co-creation lab speakers:*

Deputy Commissioner Destino Pedro, Head, National Central Bureau of Luanda, Angola, Criminal Investigation Service and INTERPOL Executive Committee Delegate for Africa (Angola)

Mr Terry Loo, Vice President of Sales, APAC, Cellebrite (Singapore)

Dr Shashi Jayakumar, Head, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (Singapore)

*moderator*

Ms Cheryl Chung, Co-Director Executive Education Department, Lee Kuan Yew School of Public Policy, National University of Singapore (Singapore)

The public safety landscape is transforming at speed and scale, requiring police forces to upgrade or change existing workforce strategies, and reconsider essential policing skills. In this co-creation lab, speakers tried to answer the following questions:

Identification – How can law enforcement use technology to identify individuals?

Intelligence – How to make use of big data to provide good intelligence?

Investigation – What can be the use of AI to aid investigation?

Operations – How to use technology to serve as road block in the cyberspace

Cooperation and collaboration – Partnership with other agencies and companies

Five challenges that the law enforcement will be still facing in the near future were identified:

1. Encryption
2. Volume of data – hampering effective analysis and obscuring the meaning behind it
3. Variety – increased variety of application and devices rendering currently used forensics tools ineffective
4. Velocity – Data are being stored in the cloud - existing regulation may prevent them to be admitted as evidence in court
5. Volatility – law enforcement have to anticipate the dynamic change of technology

### *Key recommendations*

- Law enforcement agencies need to understand how their industry partners operate in order to jointly identify effective solutions for sensitive issues.
- INTERPOL should focus on emphasizing the importance of continuous training process to update law enforcement officers' skillset and adoption of new technologies.
- Police agencies should be innovative, agile and build networks with industry to maintain a competitive edge in crime fighting

Ms Cheryl Chung, moderating the co-creation lab

## 12. Training Delivery for the Future

*Co-creation lab speakers:*

Assistant Commissioner Jevon McSkimming, New Zealand Police (New Zealand)

Mr Matt Service, CEO, Blue Lights Digital (BLD) (United Kingdom)

Mr Kee Hean Soh, Director, Home Team School of Criminal Investigation, Singapore Police Force and Senior Director Technology Development, Home Team Academy (Singapore)

*moderator*

Dr. Karene Saad, Head of Strategic and Business Planning, INTERPOL (Canada)

Can training be assisted through technology? How does mobile technologies, VR, and applications aid and improve training processes? The three speakers examined the evolution of law enforcement learning from being lecture based to leveraging pedagogy through advanced solutions such as Virtual Reality Crime Scene Training to meet current needs.

New technologies opened vast opportunities for trainers, moving the teaching process away from the classroom and changing its nature from trainer centric to learner centric (peer-to-peer learning, expert learning), with trainers becoming facilitators.

Speakers highlighted that mobile learning is also supplementary training. It allows trainees to learn at their own pace. Mobile technology enhances the speed and scope of trainings, ensuring a tight operations-training loop. Finally, data analytics allow trainers to draw insights, study trends, and seek improvements to make training better.

According to the speakers' assessment, big trends in training delivery for the future include:

- Artificial Intelligence: interview avatars able to train officers in criminal investigation
- Simulation Technology, which is configurable and recordable. Training can be recorded for after-action review, which allows for more avenues of discussion and greater areas for improvement. Simulation allows the application of realistic scenarios resulting in more impactful and effective training.
- Bespoke learning design
- Scenario-based learning – training should be delivered in the classroom using credible, current, and contextual scenarios to underpin learning
- Emulated environments, allowing users to interpret data and consider diverse ways to apply it
- Ethics training and raising awareness of potential biases

### *Key recommendations*

- INTERPOL should facilitate the accessibility of tools and methodologies for all the member countries.
- Set standards, identify and share best practices across law enforcement to improve training quality
- Ensure that training technology should encourage participants to identify and tackle inherent biases

## 13. Border Security

*Co-creation lab speakers:*

Mr Berndt Koerner, Deputy Executive Director, European Border and Coast Guard Agency, Frontex (European Union)

Mr Michael O'Connell, Vice President and Executive Advisor, NEC Corporation (United Kingdom)

Dr Urszula Mlodziejowska-Seredyn, Academic Teacher and Researcher, Radom Academy of Economics (Poland)

*moderator*

Mr Harald Arm, Director, Operational Support and Analysis, INTERPOL (Germany)

The speakers discussed how future border controls will improve the reliability of individual screening, safety of travel between countries, and help to eliminate the threats of domestic attacks.

Human training and knowledge must not be forgotten despite the abundance of technologies. Law enforcement officers should be able to step up and take control during power or machine failure. In the next five years, law enforcement need to strike a balance between developing technological capabilities and training competent officers to identify suspicious travelers.

### *Reflection from the lab*

Organizational changes are just as important as technological developments. The ability to change one's mindset when needed is crucial.

### *Key recommendations:*

- INTERPOL should continue facilitating the cooperation of law enforcement agencies regarding data sharing on profiling.
- Focus should always be on finding the balance between technology and human factors in the monitoring and management of borders, a plan for continual development in preparation of the digitalization of identification documents.

*Co-creation lab speakers:*

Dr Patrick Voss De-Haan, Head of Cybercrime Research, Bundeskriminalamt (Germany)

Mr Daniel Faggella, CEO and Founder, Emerj Artificial Intelligence Research (United States)

Mr Toufi Saliba, CEO, Toda Network (United States)

*moderator*

Dr. Karene Saad, Head of Strategic and Business Planning, INTERPOL (Canada)

## 14. **Deepfakes**

Audio and video files that have been constructed to make a person appear to say or do something that they never said or did might be the next big threat targeting the cohesion of societies. With artificial intelligence-based methods for creating deepfakes becoming increasingly sophisticated and accessible, new challenges for law enforcement, policymakers, and technology experts arise. The speakers discussed how the ability to distort reality has taken an exponential leap forward with technology and how the popularity of social media and the availability of a multitude of communications tools could allow for deepfakes to spread rapidly. The challenges are two fold, not only the reality can be manipulated and promoted for a nefarious purpose, but technology can be used and adopted to manipulate current safety and security protocols, allowing people, to purport as being people that they are not through the manipulation of AI systems linked to facial and fingerprint identification. If you cannot believe what you see or hear, what can you believe?

### *Key recommendations*

- The public needs to be informed and kept up to date about threats related to deepfakes
- Deepfakes will be harder to overcome in the future – guidelines for recognizing them and tools for examining and verifying sources are needed
- Develop a strategy through design for the identification and tagging of deepfakes as they appear and sharing this information with the information with all persons that view or listen to the content.

Mr Toufi Saliba renowned global expert in cryptography and artificial intelligence briefs the co-creation lab

*Co-creation lab speakers:*

Mr Heiko Schneider, Chief Police Officer, Management Support Unit, Bundeskriminalamt (Germany)

Mr Dongwook Kim, Networks Technical Specialist, GSM Association (Republic of Korea)

*moderator*

Mr Ged Griffin, Senior Research Advisor, Centre for Disaster Management and Public Safety, University of Melbourne (Australia)

## 15. **5G**

Due to a much higher bit rate, the ability to support a larger number of mobile devices, and a smaller cell size, the deployment of 5G networks is expected to revolutionize many of law enforcement applications. Together with the emergence of low-cost IoT devices and availability of pervasive cloud services, 5G networks are expected to enable many innovative law enforcement processes and enhance existing operations of police organizations in a cost-effective manner.

5G is really the last barrier to scale – it can scale threats but also opportunities, for example, greater integration of it with IoT technologies. Challenges ahead of law enforcement include lawful interception, identification and localization of users, availability and accessibility of information, decryption, and the ability of analyzing an expediential quantities levels of data in real time, to identify and potentially mitigate threat.

In overcoming these challenges a clearer understanding of what is relevant and irrelevant data traffic through these networks and how enhanced technology including artificial intelligence can be used by law enforcement to make sense of information quickly for pertinent investigations and policing operations.

### *Key recommendations*

- Law enforcement needs to prepare for the new wave of data challenges that will emerge with the rollout of 5G technology globally
- INTERPOL should become a key platform to discuss the threats and opportunities brought about by 5G
- INTERPOL should also work on developing best practices and guidelines and create a knowledge hub for the member countries, linking them with industry and regulators.
- Plans need to be considered by policing agencies to take advantage of 5G technology to digitally transform policing practices and activities.

A plan being developed by the co-creation lab

*Co-creation lab speakers:*

Ms Pauline Yee, Director, International Organisations and Security Directorate, International Cooperation and Partnerships Division, Ministry of Home Affairs (Singapore)

Mr Christopher Brand, Director and Country Manager, Axon Public Safety Northern Asia (China)

Assoc Prof Abhishek Singh Bhati, Campus Dean, James Cook University (Singapore)

*moderator*

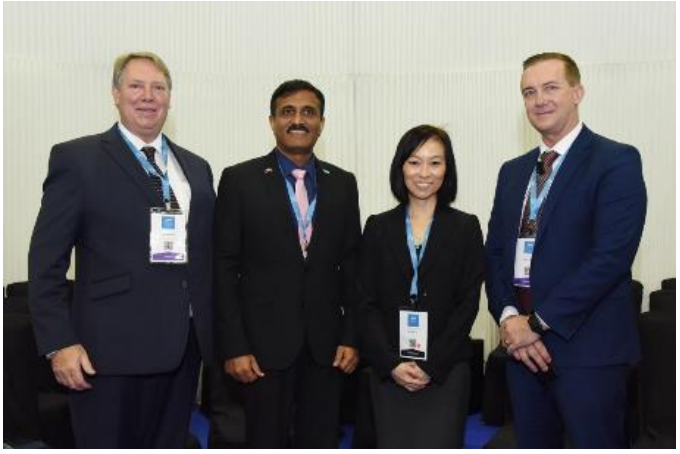
Mr. Peter Brown, Change Manager, National Criminal Intelligence System Program, Australia Criminal Intelligence Commission (ACIC) (Australia)

## 16. Community Participation

Despite the immense potential of citizen capital in fighting crime and creating safe neighborhoods, only a small fraction of citizens actively participate. The speakers, examined attitudes toward citizen participation and the relationship between different types of participation groups their behavior and needs and how best that they should be engaged and communicated with to optimize the benefit for law enforcement and the broader community. Community partnerships, the use of social media, the emergence and use of mobile application tools, are just some of the current strategies in place that have had mixed results. Capabilities such as geo fencing potentially provides additional capabilities for law enforcement agency to reach out to specific community members within a designated area and seek their support and information. It was evident during the discussion that any solution was not purely a technology one, but to ensure any strategy maximized the outcomes and opportunities a more integrated strategy was required involving broad community engagement across various diverse groups with varying needs, a clear public messaging method that provides information but also seeks help espousing the broader community needs, and innovating application of technology that links not only social media mass information collection but personalized to each member of the community.

### *Key recommendations*

- Broader community engagement aimed at developing trust in how and why information is collected and what it will be used for
- Communities should be empowered to use tools for information and evidence submission as part of a broader social conscious of going the right thing, and protecting the community and other citizens
- Establish a system that identifies the diverse needs of the community (e.g., community), so that messaging can be tailored and targeted to meet their needs.



*Community participation co-creation lab speakers and moderator*

## 17. Financial Crime

Speakers discussed how law enforcement and industry can promote robust discussions between private and government bodies while dealing with multi-jurisdiction cooperation and sharing information between various banks while protecting customers.

*Co-creation lab speakers:*

Mr Jamil Darwish, Senior Director, Automatic Data Processing (ADP) (France)

Mr Oleg Gorobets, Security Evangelist, Kaspersky Lab (Russia)

Dr John Coyne, Head of Border Security Program, Australian Strategic Policy Institute (Australia)

*moderator*

Ms. Denise Lim, Partner Risk Assurance PwC (Singapore)

### *Trends and Threats*

- Prominent actors increase global operations, emerging actors go international with purchases being made through the Darknet
- Supply chain attacks on the rise, with fin-tech startups, traders and cryptoexchangers drawing extra interest
- ATM Malware flourishes: only recently analysts described 6 new families; older families are constantly updated, infections via banks network compromise
- Attacks on cryptocurrency traders and exchange are on the rise
- Focus on cryptovaluables

### *Key recommendations*

- Financial institutions should be more proactive and transparent about information sharing with law enforcement agencies
- There should be a better framework in place to make it easier for financial institutions across regions to share data with law enforcement agencies
- Financial institutions and law enforcement agencies should keep up with and tackle different types of online financial crimes as a collective unit

*Ms Denise Lim moderating*

*Co-creation lab speaker Mr Jamil Darwish*

## 18. **Partnership with Big Data**

*Co-creation lab speakers:*

Mr Tim Morris, Executive Director Police Services, INTERPOL (Australia)

Mr Ami Braun, Vice President, Cyber Technologies and Solutions, AddOn APAC Innovative Solutions (Israel)

Dr Eleanor Hobley, Head of Research, Big Data, ZITiS (Germany)

*moderator*

Mr Matias Heilala, Director Business Innovation Lead, PwC (Singapore)

Does data-driven policing mean aggressive police presence and increased surveillance of communities?

Predictive policing and data matching solutions – this is the current picture of big data in the world of law enforcement. It is still in its infancy but there are already opportunities for data use and study. The core of policing's future is data, enabled by social media, sensors, and surveillance sources. This big data arises from the expanded ability to collect, store, sort, and analyse digital clues about crime.

The speakers discussed opportunities and obstacles for law enforcement agencies' partnerships with big data developers and solution providers.

Dr Eleanor Hobley briefing the co-creation lab

### *Key recommendations*

- Support for national agencies through the creation of standards for getting data for investigation
- Support the quality setting for data sharing framework and protocols which can be between and within countries. Second is a center of excellence for integrating technology with law enforcement. There is a fair bit of technological advancement in the private sector and INTERPOL could assess the value of new technologies for law enforcement. INTERPOL can be the center of innovation to share new technologies to various countries.
- INTERPOL could collect common problem statements from different law enforcement agencies so that they can make collective investments in solving issues.

## 19. Marine Pollution Crime

*Co-creation lab speakers:*

Mr Jerry Innocent Akubo, National Technical Officer and Drone Expert, Nigeria Police Force (Nigeria)

Dr Nadia Maaref, Director, Maritime Surveillance, Collecte Localisation Satellites (CLS) (France)

Assoc Prof Robert Beckman, Head, Ocean Law & Policy Programme, Centre for International Law (CIL), National University of Singapore (NUS) (Singapore)

*moderator*

Mr Daoming Zhang, Assistant Director, Illicit Markets, INTERPOL (China)

With 8 million items of marine litter entering the oceans every day, marine pollution crime pose significant threats to human, environmental, and economic security, negatively impacting sustainable development. Technologies such as drones, AIS and satellite imagery, side looking airborne radar (SLAR), electro-optical infrared cameras (EO/IR), infrared/ultraviolet line scanner (IR/UV), night vision cameras, Sulphur sensors play a key role in detecting offshore marine pollution offences. The speakers discussed the following items:

1) Technologies to track vessels, containers and hazardous cargo must be improved.

2) International Maritime Organisation (IMO) conventions on ship-source platform must be strengthened. There is a need for new legislation to address pollution of the marine environment from land-based activities.

4) Agencies at national, regional, and international levels must coordinate their activities and not operate in silos. Furthermore, speakers highlighted the need for better coordination between INTERPOL, UNODC, UNEP, IMO to address marine pollution crimes. Regional centers should coordinate the activities aiming at the enhancement of information sharing between states.

5) New technologies will not solve the problem if the legal issues and coordination issues are not addressed.

6) Need for more deterrent measures to prevent people from committing offences.

### *Key recommendations*

- New technologies have been useful in addressing marine pollution crime because they became a part of a robust, comprehensive deterrence system
- Countries where the use of technology against marine pollution crime have been effective are also countries with the greatest compliance to environmental goals
- New technologies will not solve the problem if legal and coordination issues are not addressed. Therefore, there is a need for law refinement, improved coordination among countries, and intelligence sharing.


Click on the photo to learn more about INTERPOL's Operation 30 Days at Sea

## 20. Virtual and Augmented Reality

*Co-creation lab speakers:*

Dr Stefan Blatter, Commander, Cantonal Police Bern (Switzerland)

Mr Sebastian De Peretti, Sales Director APAC, Obvious Technology (Singapore)

Dr Ronnie Lee, Deputy Director, GovTech Singapore (Singapore)

*moderator*

Mr. Peter Brown, Change Manager, National Criminal Intelligence System Program, Australia Criminal Intelligence Commission (ACIC) (Australia)

VR and AR used in policing are able to mimic the characteristics of police work at very diverse locations, settings, and time for the training of officers to intervene in any situation. Mixed Reality (MR) is bringing together the real world and digital elements to interact with and manipulate training, better responsiveness, information advantage, and development of new mindsets and processes. At the same time, technological complexity, dependency on technology, high costs, and risk of hacking are some of the factors deterring law enforcement from using VR and AR more often.

The speakers discussed how VR and AR are relevant for the 5 phases of the security process: alert, location, solve, track, and identify) and how it can aid the traditional shooting training (VR can be used in shooting practice where users can be supported by 3D viewers simulating sounds, lighting, spatial conditions, CBRN, and impairments). The speakers also emphasized the need for a global roadmap focused not on the technology but on the capabilities that law enforcement want to develop. They also highlighted the need for accurate data collection in order to create accurate and immersive VR/AR models, and examined future developments.

### *Key recommendation*

- Create tools with actual uses that benefit the public
- To effectively capitalize on augmented reality, law enforcement need to build trust with their Government and their communities to allow for the access of additional data that would add value to AR modelling for their local environment
- Develop closer relationships with industry that provide AR capabilities to ensure that they are aware of the needs and requirements for law enforcement
- Globally INTERPOL needs to standardize some tools for law enforcement that could be used by all member countries

## 21. Smart Cities

*Co-creation lab speakers:*

Mr Yeow Boon Ng, Senior Director, Capability Development, Science and Technology Group, Ministry of Home Affairs (Singapore)

Mr Augustine Chiew, APAC Lead, Public Safety, Huawei Technologies Co Ltd (Singapore)

Dr Vivy Suhendra, Executive Director, Singapore Cybersecurity Consortium (Singapore)

*moderator*

Mr. Wee Lee Lee, Director Cybersecurity, PwC (Singapore)

Safety and security of both the physical and cyber realms remain a key foundation in the creation and transformation of smart cities. Advanced technologies add new levels of connectivity that allow law enforcement to be more responsive and efficient.

Our speakers explored new operating models for police in smart cities – “Explore, Experiment, Experience” which was summarized in five points:

- No Change in Mission
- Race against unknown adversaries
- Re-design, re-tool, reskill, re-create
- Deepen the core of Science & Technology
- People-Technology-CONOPS (Concept of Operations)

The experts debated whether there is a privacy benchmark around the world which could hamper or enable deployment of smart city solutions: the privacy vs. security debate should be a constant discussion as it is always a pertinent issue.

### *Key recommendations*

- INTERPOL should facilitate creation of adequate tools to investigate and prosecute, and update interview and investigation procedures
- Law enforcement’s mission in smart cities generation does not change but agencies need to reinvent themselves in order to be relevant. New model and thinking may also needed to be injected into the process. INTERPOL should therefore facilitate an “evolve and adapt” principle as an organization.


Mr Yeow Boon Ng, briefing the co-creation lab on Singapore’s efforts in preparing for Smart cities

*Co-creation lab speakers:*

Ms Janey Young, Head of Team, Europol's European Cybercrime Centre (EC3) (European Union)

Mr Mikko Niemela, CEP, Cyber Intelligence House (Singapore)

Dr Seungwon Shin, Associate Professor, School of Electrical Engineering, KAIST (Republic of Korea)

*moderator*

Mr. Peter Brown, Change Manager, National Criminal Intelligence System Program, Australia Criminal Intelligence Commission (ACIC) (Australia)

## 22. **Darknet**

Network anonymization and the Darknet are used for legitimate reasons by people wishing to maintain their privacy but the Darknet is also used to camouflage illicit activities. The challenge is to uncover the intent and extent of criminal activities. The speakers discussed how law enforcement should prepare itself for the current threat and the future of cyber-enabled crimes. Darknet is an environment that will not go away now or into the future due to the demand for illicit products that can be sourced. Among the discussed issues were hiring and training technical experts on Internet, deep web and Darknet capabilities, investing in tools such as web crawling, data mining and cryptocurrency analytical tools, and transparency in the form of reporting and sharing cybercrime instances with other agencies to develop universal capabilities across law enforcement agencies.

### *Key recommendations*

- Collaboration between relevant industries is needed to share information for better research
- Balance between privacy and security rights, risk-managed building of new technologies and a legal framework
- Correlate data from multiple domains – find relationships between data as we may find hidden connections. Just inspecting the dark web is not enough, we need to monitor other domains, the surface web, and social networking sites.
- Developing technical capability investigators that analysis and assess the situation and issues quickly and link information from the open net and social media to identify targets.

Europol's Ms Janey Young, details the challenges of the Darknet for law enforcement

## 23. DNA and Biotechnology

*Co-creation lab speakers:*

Ms Anna Lim, Senior Assistant Director, Science and Technology Group, Ministry of Home Affairs (Singapore)

Mr Paul Reedy, Founder 4th Street Global (United States)

Mr Nathan Scudder, Faculty of Science and Technology, University of Canberra (Australia)

*moderator*

Dr. Karene Saad, Head of Strategic and Business Planning, INTERPOL (Canada)

DNA can be used as evidence to help convict a suspect of a crime, but also to clear an innocent individual against other profiles within a database, creating the opportunity for 'hits' – person-to-scene, scene-to-scene, or person-to-person matches – where no previous connection was known. With the advancement in technology, plus the emergency of private genealogy companies, law enforcement agencies have greater opportunities to access individuals DNA profiles and compare them against crime scene samples. Coupled with improved technology and in the use of genome sequencing has led to successful resolutions of cold cases such as 'Buck Skin Girl' and the 'Golden State Killer'. If law enforcement organization can access these private companies then they can potentially be vulnerable and exploited by criminals, and used to potentially steal DNA or create their own identify. Discussion continued and centered around a potential 'criminal gene' that predisposes an individual to criminal behavior, which presents some interesting issues around personal privacy, genetic complexity, biological determinism, and population genetics

Would another advancement in genetic analysis increase policing power or provide opportunities for criminals to exploit it for nefarious purposes?

*Created in 2002, INTERPOL's DNA database currently contains more than 180,000 profiles contributed by 84 member countries.*

### *Key recommendations*

- INTERPOL/DNA Unit to provide a governance framework for gene-editing (i.e. the use of CRISPR) for acceptance by centers using this technology
- INTERPOL should provide standards and guidance on DNA evidence
- Focus on the balance between the needs of the investigation and an individual's right to privacy – in particular, concerning open source genealogy sites.

## 24. **Predictive Capabilities**

Does predictive policing strategies lead to actual decrease in crime? Each year, increasing number of law enforcement agencies around the world is adopting software using statistical data to guide their decision-making. Even though analyzing statistical historic data to predict what areas are exposed to increased chance of criminal activity is inherently biased, it still aids police to efficiently deploy their resources to prevent criminal behavior. The speakers examined the methods of administering predictive models and the benefits and risks of predictive policing.

### *Key recommendations*

- INTERPOL should lead the discussion with member states regarding common principles, ethics across cultures, partnership with academia, industry, and other law enforcement agencies
- The importance of sharing big data and prediction algorithms

*Co-creation lab speakers:*

Mr Lebeoana Jacob Tsumane,
Deputy National Commissioner, Crime Detection, South African Police Service (South Africa)

Mr Peter Ship,
Policing SME, SAS Institute Plc (Singapore)

Dr Mary Aiken,
Cyberpsychologist and Academic Advisor, Europol's European Cyber Crime Centre (EC3) (United Kingdom)

*moderator*

Mr Ged Griffin,
Senior Research Advisor, Centre for Disaster Management and Public Safety, University of Melbourne (Australia)

*Predictive capabilities co-creation lab speakers and moderator*

*Co-creation lab speakers:*

Dr Jonathan Pan, Director of Cyber Security, Ministry of Home Affairs (MHA) (Singapore)

Mr Assaf Cohen, CEO, Anqlave (Singapore)

Dr Bernhard Haslhofer, Senior Scientist, Digital Insight Lab, Austrian Institute of Technology (Austria)

*moderator*

Mr. But Klaasen, Head of Innovation Department, Ministry of Justice and Security, The Netherlands (Netherlands)

## 25. **Blockchain**

When speaking about blockchain, we think mostly about cryptocurrency, but scarcely about the technology itself. In order to bridge that gap and finally explore the opportunities for the use of blockchain in law enforcement, the speakers began with examining the difference between public and private, permissioned and permissionless blockchain. Decentralized DNS with its unstoppable domains and online gaming were among the public blockchain use cases analysed, but the conclusion was simple: in policing, there are big promises but not enough success. Private blockchain is in fact more successful in trade finance, supply chain / food safety and insurance – nevertheless, only 1 in 10 proof-of-concept efforts move to production, because enterprises don't know what problems they want to solve. This phenomenon is also present in policing, according to the speakers.

Blockchain technology offers highly auditable solutions. The strengths of blockchain also lie on distributed architecture, consensus, encryption, and transparency. Despite the multitude of opportunities, blockchain is also posing risks, which the speakers classified in three categories: key management, smart contract logic, and IT vulnerabilities.


*Co-creation lab discussion*

## *Key recommendations*

- Encourage the discussion whether blockchain technology can be used to secure the smart devices employed by law enforcement agencies. This would enable several possible use cases: regular audit inspection checks on the integrity of these devices, detection of cyber-physical attacks on these devices, audit trail of updates, and changes made to these devices.
- Blockchain risks include key management, smart contract logic, and IT vulnerabilities, e.g., denial of service and phishing. However, the opportunities/strengths of blockchain include distributed architecture, consensus, encryption and transparency. Blockchain technology offers a highly auditable solution.
- Blockchain is a promising technology but it only enables a shift of trust – trust is about social relationships and technology alone cannot solve this problem. Indeed, false trust in blockchains can be a security risk.


*Dr Jonathan Pan*

*Co-creation lab speakers:*

Mr Paul Stanfield, Director, Organized and Emerging Crime, INTERPOL (United Kingdom)

Dr Srinivas Yanamandra, Chief, Compliance, New Development Bank (China)

Dr Salih Hakan Can, Professor of Criminology, Pennsylvania State University (Turkey)

*moderator*

Mr Ged Griffin, Senior Research Advisor, Centre for Disaster Management and Public Safety, University of Melbourne (Australia)

## 26. Transnational and Organized Crime

Transnational organized crime has been expanding aggressively due to the exploitation of legal gaps and easily accessible information sharing platforms often riding on corruption. The speakers, while considering how transnational organized crime syndicates currently use financial resources to corrupt and undermine the rule of law, were debating how to build the bridge to the future and adapt the traditional policing model of conviction, deterrence, crime control, investigation, into more proactive processes. Dialogue revolved around future-oriented ways of tackling the business model of crime, generally focused on profit, as well as data accessibility for policing.

### *Key recommendations*

- INTERPOL should assist law enforcement agencies to understand new ecosystems such as fintech and regtech
- We should continue the discussion on whether technology is mature enough for the prevention of crime: the issue of scalability/confidentiality
- Facilitate data-sharing agreements and algorithm accountability discussions
- Research: how the nature of the commodity influences the criminal venture, in order to build extensive data sets, should be examined
- Shift philosophies to a more global approach to law enforcement

*Co-creation lab speakers:*

Mr Olushola Kamar Subair, Assistant Inspector General of Police (Nigeria) and INTERPOL Executive Committee Delegate for Africa (Nigeria)

Ms Gikui Gichuhi, Senior Principal Prosecution Counsel, Office of the Director of Public Prosecution (Kenya)

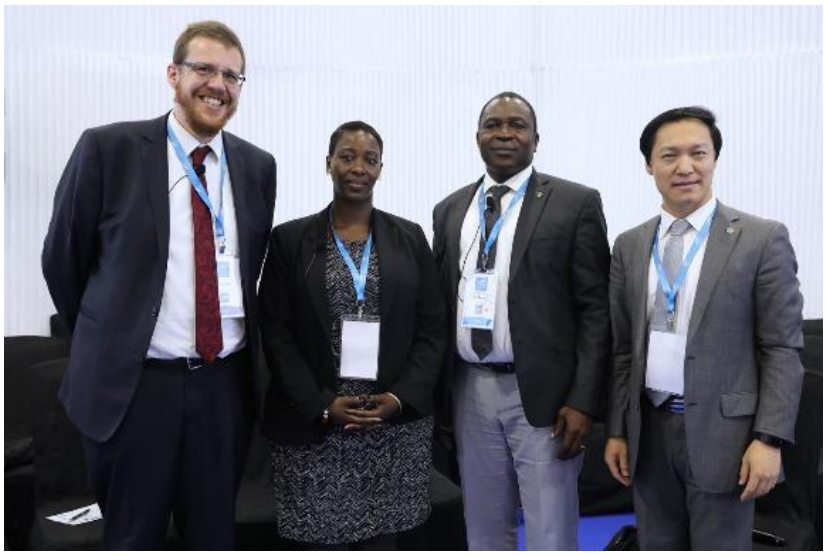
Dr David Roberts, Reader in Biodiversity Conservation, Durrell Institute of Conservation and Ecology, University of Kent (United Kingdom)

*moderator*

Mr Daoming Zhang, Assistant Director, Illicit Markets, INTERPOL (China)

## 27. Illicit Wildlife Trade

Illicit wildlife trade refers to any illegal activity – trade, smuggling, poaching, capture or colligation – perpetuated on endangered and protected species. The criminal actions are driven by strong financial interests, with a profit estimated at 7-23 billion USD per year. The advent of the Internet has expanded the market – today, wildlife products are easily available all over the web, including social network platforms such as Facebook, Instagram, Twitter, and LinkedIn. The latest statistics show that some 95% of the illicit wildlife trade is happening on the clear net.



*Co-creation lab speakers and moderator*

### *Key recommendations*

- Illicit wildlife trade struggles at being addressed as a priority in countries. It is also an area that law enforcement practitioners are not yet very familiar with.
- National authorities should dedicate a particular unit to be trained for battling cyber-related illicit wildlife trade
- The collection, storage, and presentation of digital evidence and the use of research and big data analysis such as machine learning to prosecute wildlife crime facilitated by the internet should be given importance

### Project Millennium

Project millennium assists our member countries to exchange investigative information that helps them identify the people and companies behind transnational Eurasian organized crime. The Millennium project team provides regular assessments of the Eurasian organized crime landscape based on information provided by our National Central Bureaus. Working Group Meetings have been organized in Lviv, Ukraine (May 2018), Moscow, Russia (June 2017), Tbilisi, Georgia (September 2016) and Prague, Czech Republic (February 2015).

*Co-creation lab speakers:*

Dr Peng Chen, Associate Professor and Master Supervisor, School for Information Security, People's Public Security University of China (China)

Dr Satendra Kumar, Channel Manager EM EMEA for Public Safety and Forensics, Leica Geosystems (Dubai)

Dr Pavel Gladyshev, Director, Digital Forensics Investigation Research Lab, University College Dublin (Ireland)

*moderator*

Mr. Peter Brown, Change Manager, National Criminal Intelligence System Program, Australia Criminal Intelligence Commission (ACIC) (Australia)

## 28. Geo-location of Individuals

Proliferation of geolocation data helps tracking suspects by various means, such as call data records, IP addresses, and physical surveillance. Plotting this data on a map shows a suspect's movements and location in relation to an investigated event, such as downloading contraband or unauthorized access to networks. A mobile device must be attributed to a suspect before assuming the geolocation in a particular device belongs to the suspect, but it is clear that the amount of data to analyse may be more than simply creating a map or assess whereabouts. The speakers discussed the following challenges and opportunities for using geolocation data by law enforcement:

- Technical – investigators currently use too many systems – it is important to work on coordination
- Data - law enforcement and industry must find a common ground to address communities' inquiries and build trustworthy, responsible solutions
- Breakthrough of information fusion
- Well-designed workflow and data protection protocol
- Supervision and transparency

*Co-creation lab discussion*

### *Key recommendations*

- INTERPOL should use its resources to educate the public on geo-location technology
- Academia, industry, and law enforcement should fully engage with each other to clearly recognize a process for obtaining data
- INTERPOL should facilitate work on data protection principles for law enforcement

## 29. Cyber Disruptors and Drivers of Change

This co-creation lab focused on cyberspace challenges and the ways cyber framework and new workforce competencies are adapting to the new reality. The speakers shared their perspectives on future drivers of change in cyber, such as having a clear vision and strategy, stopping "siloed" thinking and starting co-creation, thinking global and acting local, creating a network of like-minded people, building trusted consortiums, using sandbox methods, focusing on output and outcome, and being transparent about law enforcement goals.

### *Key recommendations*

- INTERPOL should consider asking member countries to identify their problems, gather feedback, and share best practices and success stories with countries facing similar problems
- Law enforcement agencies should address insufficient number of cybercrime investigators
- Nudge private sector

*Co-creation lab speakers:*

Ms Nynke Stegink, Head of International Relations, National Cyber Security Center (The Netherlands)

Dr Magda Lilia Chelly, Managing Director, Responsible Cyber Pte Ltd (Singapore)

Dr Kyung-Shick Choi, Cybercrime Investigation and Cybersecurity Program Director, Boston University (United States)

*moderator*

Mr. Shong Ye Tan, Partner, Cyber and Digital Trust Leader, PwC (Singapore)


*Dr Magda Chelly*

*Co-creation lab speakers:*

Mr William Dixon, Head, Cybercrime Futures, Centre for Cybersecurity, World Economic Forum (Switzerland)

Mr Tadahiko Ito, Research Engineer, Intelligent Systems Laboratory, SECOM Co Ltd (Japan)

Mr Soon Chia Lim, Director, Cyber Security Engineering Centre and Head Certification Body, Cyber Security Agency of Singapore (Singapore)

*moderator*

Mr. Krishna Taneja, Director National Security, TNO (The Netherlands)

## 30. Internet of Things

It is expected that the number of IoT devices including medical devices, smart cars, etc., will reach 20.4 billion by 2020. Such predictions raise inevitable concerns regarding the safety and security of the environment. With IoT powering critical devices and industrial systems, the potential damage and financial impact of locking down IoT ecosystems will rise. For instance, the Mirai malware which launched a DDoS attack via a botnet at speeds as high as 1Tb/sec, and Silex, which trashes IoT devices by overwhelming their storage capacity after gaining access using default passwords, drive individuals, organizations, and government agencies to take precautionary steps.

The speakers tackled issues concerning IoT security problem spaces such as:

- Principles, governance, and legislation (cyberspace and privacy by design, future proof legislations, IoT security standards, certification and testing)
- Ecosystem development (competitive and responsible industry, supply chain security, product lifecycle support)
- Technical references and standards (unique device identities, secure OS, cloud and applications, secure channel)

They also examined the trustworthiness of IoT data for investigations and prosecution, while assessing solutions from industry, which include Public Key Infrastructure (PKI) and firmware updates.

### *Key recommendations*

- Three steps to increase trustworthiness: liability for data, need to identify data origin, lifecycle management of data and device
- INTERPOL should encourage and facilitate collaboration for establishing a certification that will enable a safer and secure cyber environment for all

*"With the pursuit of smart cities, there is an urgent need to act on the challenges in IoT security".*

*Soon Chia Lim, Director, Cyber Security Engineering Centre & Head Certification Body, Cyber Security Agency of Singapore*

*Co-creation lab speakers:*

Mr Jeroen Van Vugt, Director, Strategy and Innovation of the Commissioner's Staff and Chief Innovation Officer, National Police (The Netherlands)

Mr Tuomo Kuosa, Content Director, Futures Platforms (Finland)

Dr John Sweeney, Director, Qazaq Research Institute for Future Studies, Narxoz University (Kazakhstan)

*moderator*

Dr. Karene Saad, Head of Strategic and Business Planning, INTERPOL (Canada)

## 31. Horizon Scanning

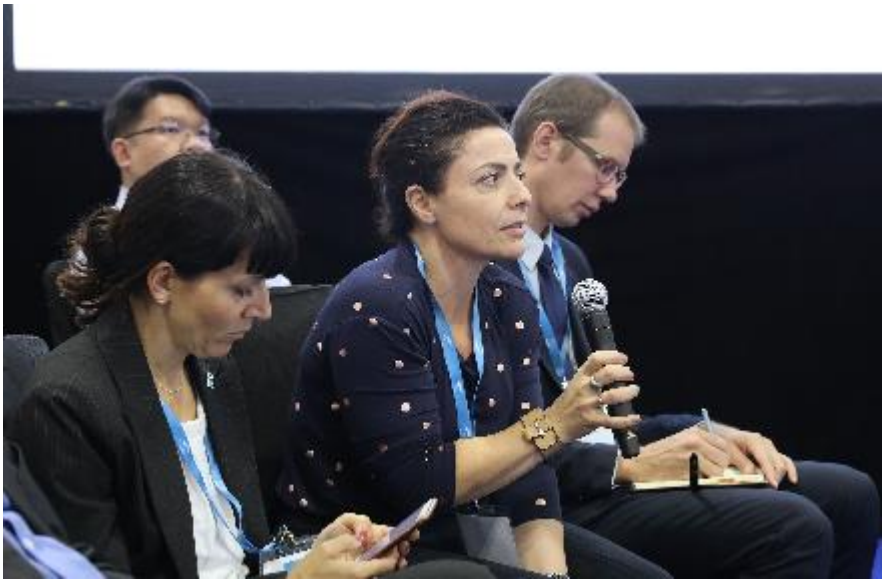
Law enforcement agencies need to be prepared to tackle future threats. The need for a dynamic, innovative international response to address emerging threats was highlighted in this co-creation lab. Speakers examined attempts of institutions and member countries to create effective horizon scanning processes. They also assessed in-house efforts to tackle these future challenges: the INTERPOL Innovation Centre has developed a continuous horizon scanning initiative. The aim of the initiative is to enhance the understanding of member countries regarding the unprecedented wave of global change including technological advances, and to advise law enforcement on the best ways to navigate these fast-developing trends.

### *Key recommendations*

- It is imperative to set up a law enforcement community that participates in a global horizon scan
- Horizon scanning needs to be a constant practice and a part of an organization's DNA

*Horizon scanning co-creation lab speakers and moderator*


*Dr John Sweeney*



*Ms. Odette Meli, Australian Federal Police*

INTERPOL

STRATalks 2019 took place in Dubai, United Arab Emirates from 5 to 6 September 2019. The theme of this year edition was “Horizon Scanning for a Safer World”. This strategic meeting was attended by 34 participants from 18 member countries across all INTERPOL regions, as well as representatives of two international organisations. The event combined workshop-style exercises focused on facilitating future-oriented skills and impact thinking, futures gaming and global shared learning in order to enhance a futures network within policing and purusue the horizon scanning process undertaken by INTERPOL.

## 32. **Privacy**

The tension between individual privacy and law enforcement predates current technological developments. Innovation, new societal contexts, and new circumstances have intensified that tension. The speakers, focusing on the use of information technology in law enforcement, discussed the pressures placed on individual privacy.

*Co-creation lab speakers:*

Ms Mailis Pukonen, Head of Operations Department and Deputy Director, CEPOL (Hungary)

Mr Andy Prakash, Co-Founder, AntiHACK.me (Singapore)

Mr Ziga Skorjanc, Teaching and Research Assistant, Department of Innovation and Digitalisation in Law, University of Vienna (Austria)

*moderator*

Dr Andreas Deppeler, Director, Data and Analytics, PwC (Singapore)

### *Key recommendations*

- The right to the protection of personal data should be observed
- Industry should indiscriminately undergo due diligence, instead of evaluation requests related to privacy breach complaints
- Ensure supervision and regulation of new tools and methods

# V: Working Groups

The following INTERPOL Working Groups are meetings that seek to empower law enforcement agencies with useful data and tools in the areas of innovation, artificial intelligence, drones and darknet cryptocurrencies.

1. **3rd INTERPOL Drone Expert Group**
   *72 participants from 25 countries met to increase law enforcement's awareness and understanding of the multidimensional nature of drones as a tool, a threat, and a piece of evidence.*

2. **3rd Darknet and Cryptocurrencies Working Group**
   *78 experts from 32 member countries and other organisations (e.g. Europol, UNODC, CEPOL and GCCPOL) joined the meeting. This WG focused on addressing the gap between de-anonymisation and attribution.*

3. **2nd INTERPOL-UNICRI Global Meeting on AI for Law Enforcement**
   *Consisting of four main sessions, this working group hosted 49 participants from 18 countries, EUCEPOL, EU Commission and OSCE.*

4. **2nd Chief Innovation Officers' Expert Exchange**
   *Focusing on three main areas (Strategic Foresight / INTERPOL Global Horizon Scan, Institutionalizing Police Innovation, INTERPOL Police Innovation and Technology Radar) this Working Group was attended by 27 participants representing 18 countries and EUROPOL.*

# 3rd INTERPOL Drone Expert Group


## Tool Thematic

Drone technology has provided new and innovative methods for assisting public safety, security, and situational awareness. Drones can significantly assist police in conducting their operations by saving time and resources, transmitting digital information instantly, increasing officer safety, and creating higher quality outputs. For example, drones can be utilised to attain situational awareness at high-risk mass events, which is typically conducted by helicopters, planes, and satellites. Further, drones can be used as an additional tool for first responders, saving time on-scene and allowing for the more efficient and effective deployment of resources.

The drone industry have developed many drone related technologies which are especially useful for law enforcement in performing their work and ensuring public safety. For example, DJI have developed drone payloads including spotlights, speakers, and beacons which can greatly assist law enforcement in search and rescue operations. Further, drone technologies have been developed to test the exhaust gas plumes of ships to help detect environmental crime, and protect the environment.

However, the use of drones in policing and public safety requires dedicated officers with appropriate education, training, and skills. Law enforcement organisations currently lack awareness of the many benefits drones can provide to law enforcement operations. More law enforcement education and training on drones as a tool is vital, and more police organisations globally should look to incorporating drones into their operations.

## Threat Thematic

Advancements to drone technology, and increased uptake by both commercial and recreational users, has produced serious unseen challenges for the drone industry, law enforcement, and public safety. Drones pose an asymmetric threat to society, and the cost of combatting drones is significant. The threat and challenges posed by drones is only going to increase - for example, with drone control over cellular networks with the introduction of 5G. In the interest of public safety, technology professionals, industry, frontline drone operators, and personnel aware of budgets and cost limitations need to work together to develop adequate drone detection and counter solutions, and prepare for the future threat.


Drone detection and mitigation requires a multi-tiered solution, and early detection is key to combatting the real time threat drones pose. There is no completely effective solution for countering drones, and more proven scenario-based testing and evaluation of countermeasures needs to be conducted, and this information shared amongst the law enforcement community, to increase the awareness and capacity of Member Countries (especially those with limited resources) to counter drones. More research is needed on the possible use of data mining, data fusion, and artificial intelligence to aid drone detection systems. Further, industry and law enforcement should collaborate to address the current lack of tools available to counter non-popular and DIY/custom drones.

Conducting a thorough drone risk assessment and planning counter drone solutions is vital to ensuring public safety and security. Prior to deploying countermeasures, it is important to perform a countermeasure risk assessment and create a countermeasure risk management plan to avoid collateral risk. More awareness and understanding is needed on how we can protect critical infrastructure from drones, and the possible collateral risks of drone countermeasures, for example, the possible collateral effects of radio frequency jammers on airport communications and operations. Counter drone operations need to be constantly reviewed and adapted, as drone technologies are constantly evolving with enhanced capabilities and functions. Additionally, legislation has not kept up with drone tech advancements, and hence legislative change is needed to allow police to deploy countermeasures to adequately mitigate nefarious drones.

Finally, identification, recording, and sharing of drone incident data is key to understanding the evolution of drone uses and technologies. However, currently there is no process nor platform to share drone incident data between Member Countries.

## Evidence Thematic

There currently exists a lack of understanding among law enforcement of the fact that drones contain valuable data, and how this data can be extracted and analysed to provide evidence to support an investigation. For example, digital forensics can be utilised to identify the drop signature and geolocation information for expelled drone cargo – a potentially vital piece of evidence that can be used by police and prosecutors. Additionally, drones can be used as a tool by police, for example, to capture pictures and video footage which can be turned into crime scene maps (including 3D maps), crime scene animations, and simulations. This allows investigators to gain a high level overview of the crime scene landscape, and more efficiently and effectively deploy resources to the right area – particularly in crimes such as illegal drug planting, illegal logging, and illegal mining.

## Conclusions

Increased sharing of information and best practice across law enforcement through expert group meetings such as this one will aid in raising the awareness, understanding, and capacity of police on drones as a tool, a threat, and a piece of evidence. We must work together, rather than independently, in order to adequately protect and serve the public.

The 4th INTERPOL Drone Expert Group will be held in approximately one year's time in Norway.

# 3rd Darknet and Cryptocurrencies Working Group


The 3rd working group thematically focused on “Addressing the gap of de-anonymisation and attribution” following the two previous editions of the working group on “altcoin tracing” and “de-anonymisation technique” discussed during the 2nd edition. During the sharing and working session, participants from various different background (LEA, Industry and Academia) identified 8 de-anonymisation methodologies.

Throughout the working group is was evident that additional requirements and information was need by all to achieve the desired and expected outcomes of the communities that we are here to protected.

Specific tasks that require urgent actions of INTERPOL for the international LE community are

1. to establish a global database of criminal cryptocurrency wallets,
2. to compile and standardise data from cryptocurrencies analytics and dark web crawler,
3. to assess activities on alternative darknets such as I2P and Freenet, and
4. to support the LE developers community.

## Key Observations

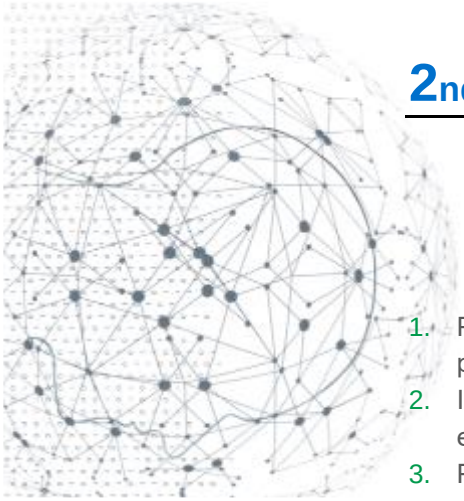
- The recent success of efforts such as Wall Street Market and the Bestmixer takedown suggest that international law enforcement agencies are learning and collaborating to deal with the challenges posed by darknet markets and cryptocurrencies.
- Dark web crime investigations, much like old-fashioned investigations, continue to rely heavily on the “follow-the-money” principle, which in the cyber context involves mapping cryptocurrency flows to gain insight into the operation of criminals and darknet markets.
- Against targeted investigations, Tor and Bitcoin are only ‘sort of’ anonymous. Human error, such as a misconfigured server or a visible email address, is often a key element in investigations.
- For cryptocurrency analytics to be effective, it is essential to compile a database of attribution tags (these are any form of context information that can be attributed to an address, such as the name of an exchange).

## Conclusions

- Law enforcement agencies should set the direction and steer nations towards a safe and secure cyberspace environment, working closely with cybersecurity experts, industry, academia and research organisations.
- Law enforcement should act as a global community when learning from incidents. This requires an open culture of sharing and mutual learning.
- The overarching objective is to empower LEAs to tackle online crime. INTERPOL Working Group on Darknet and Cryptocurrencies aims to achieve it by exploring new innovative tools and sharing investigative best practices to de-anonymise dark markets and cryptocurrencies through a global expert community.

In addition to the next working group to be held in September 2020, there has been a shared agreement on the urgency to tackle the challenges identified from this Working Group. As such a Task Force has been established to address specific needs and challenges that are detailed below. The 1st Task Force meeting was held in Singapore on 9 -11 December 2019.

- Task Force aims are
  - Establishing an international database of criminal wallets
  - Compiling Attribution ‘Tagpacks’ database for cryptocurrencies analytics for LEA
  - Mapping crawled data to standards / ontology for Dark Web crimes
  - Define the developers community, how can it work, and share that with all partner agencies
  - Assessment of activities as an alternative Darknets



# 2nd INTERPOL-UNICRI Global Meeting

This working group, organised jointly by UNICRI and INTERPOL Innovation Centre, Adaptive Policing Lab consisted of 4 main sessions:

1. Presentations from selected Law Enforcement Agencies that are working on AI projects to solve policing challenges;
2. In-depth discussion on 4 AI technologies and capabilities that provide immediate value to law enforcement;
3. Panel discussion on Ethical, Legal and Social Implications (ELSI) of AI integration in law enforcement; and
4. A Hands-On session to implement and experiment with AI. Participants were introduced to the required system infrastructure design and integration process as well as examples of AI services that can be utilized for police work

Introductory discussion explored diverse experiments of AI in law enforcement operations, as well as specific technology domains in AI useful in law enforcement. The emphasis was on the need of knowledge-sharing and collaboration between LEA and cross-stakeholders and the need of a Universal Standard / Principle to guide the use of AI in law enforcement, participants examined the four major AI applications in policing. AI technologies included:

- Audio Processing: still underexplored and underutilized, but a number of applications were demonstrated to illustrate the value of this tool, including Person Of Interest (POI) reconstruction in crimes against children, thefts, terrorism.
- Visual Processing: that use of AI and facial recognition that facilitates more automated identification for mass / crowded venues
- Resource Optimization: AI used in policing daily context, as well as mission-critical scenarios, demonstrated a quicker and more effective decision-making for personnel involved
- Natural Language Processing: a tool for information extraction from big data environment, that is relevant and timely for the investigations objectives.

The panel discussed issues of social acceptance of the practices and processes of policing initiatives, and how the future use of AI by law enforcement could be impacted if police do not have the trust and support of their communities. This extends to the application of information or outcomes deduced from the use of AI and its eventual admissibility of that information as evidence. This session was quite a positive insight into the potential pitfalls of law enforcement taking up technology without due consideration of their environment and the potential legal challenges and uses of that technology without proper and transparent engagement with relevant stakeholders.

## Way forward for AI for Law Enforcement meeting

1. The need for Universal Standard in the use of AI in Law Enforcement:

   - Based on the discussion, it is clear that LE need a clear guidance (a what-to and a how-to) to be taken into consideration when adopting AI for a specific use in law enforcement operations
   - What areas should we look into in the standard:
     Regulate the use cases, not the technology
   - Methodology:

     Appoint main focal point to liaise with local policy-makers (national legislation body) and independent auditors

     Determine the baseline – a “common language” for law enforcement-policy makers-industry-academia

     Criteria for data handling (data collection, protection and common anonymization)

     Criteria to assess bias in the machine-learning / algorithm for decision-making

     Criteria for AI initiative trial and errors

     Criteria to develop internal development capabilities

     Criteria to determine unrealistic and undesirable uses

     Translating the principles into policy

2. Adoption of national SOPs based on the Universal Standard


# 2nd Chief Innovation Expert Exchange

The 2nd CINOEE was organized during the INTERPOL World and brought together 27 representatives from 18 countries and Europol in a continuous effort to enable focused exchange between law enforcement officers around the globe tasked with innovation related work within their national agency. Following the success and feedback of the 1st CINOEE, this meeting continued to encourage the exchange of current challenges, ideas and best practices in the area of law enforcement innovation.

This year's meeting focused on three main thematic areas:

**1. Strategic Foresight / INTERPOL Global Horizon Scan**

In this working session, participants, together with the session facilitator, Futurist Dr. John Sweeney, discussed the challenge of how to effectively identify future disruptors which are defined as key phenomena and trends that have the potential to impact on law enforcement work in the future. Dr. Sweeney highlighted through numerous examples the added value of strategic foresight for law enforcement and encouraged participants to use future assessment as valuable intelligence for strategic decision making. Furthermore, the Innovations Centers work around the INTERPOL Global Horizon Scan was presented and discussed based on two exemplary phenomena: Quantum Computing and 5th Generation Telecommunication.

**2. Institutionalizing Police Innovation:**

This session was based on requests from member countries for an exchange on how to establish and maintain an innovation unit within law enforcement. The importance and urgency of this topic is rooted in the sharp recent increase of law enforcement agencies trying to drive innovation into their organisations through the establishment of innovation units. Selected participants shared their agencies very different approach and development stages, and discussed specific challenges and opportunities with the group.

**3. INTERPOL Police Innovation and Technology Radar**

For the last session, participants were invited to strategize and validate further development needs with regard to the INTERPOL Innovation Radar. This feedback was used to further customize it into its current version. The Radar is a virtual collaboration platform, aiming to

close the knowledge gap that exists between different law enforcement agencies regarding the use of new technologies and innovative approaches, limit work redundancies related to innovative projects within law enforcement agencies and facilitate a strategic and focused exchange between law enforcement agencies and external entities (including think tanks, academia, industry, subject matter experts and other international bodies) to find innovative solutions to existing challenges. Two specific examples of future INTERPOL Radar content were presented and discussed: Automated Human Voice Profiling and Modern Vehicle Forensics.

# VI: The Way Ahead

Progressing the outcomes of the INTERPOL World 2019 is critical to ensure that the INTERPOL and the 194 member countries actually maintain a ongoing benefit from INTERPOL World 2019.

The objectives of the INTERPOL Global Innovation Agenda Program are:

- Coordinate a series of projects that have stemmed from INTERPOL World 2019 co-creation labs and other research proposals;
- Coordinate potential funding and support the resourcing requirements for each of the projects;
- Building greater partnerships with academia and industry with law enforcement through the planning and delivery of projects;
- Coordinate outcomes and deliverables into other INTERPOL products including the INTERPOL Police Innovation and Technology Radar and the Technology Gyms;
- Provide guiding principles, guidelines and opportunities for INTERPOL General Secretariat and member countries on future technology application;
- Report back to INTERPOL General Secretariat, member countries and partner agencies on the outcomes that were delivered;
- Provide advice and guidance for the formation of future Co-Creation Labs at INTERPOL World; and
- enhancing Global Innovation awareness and skills across all member countries.

The INTERPOL Global Innovation Agenda Program will be coordinated and run by the INTERPOL Innovation Centre by either:

- outsourcing projects of activities to member countries to action and progress;
- outsourcing externally to academia in partnership with law enforcement agencies;
- externally to industry partners to manage and engage with law enforcement to deliver the project of activity; or
- an externally funded project undertaken within an INTERPOL Directorate, including Innovation Directorate that is managed and coordinated under this umbrella program.

# Words of Appreciation

INTERPOL would like to thank Ministry Home Affairs for dedication and unwavering commitment to INTERPOL World initiative. We are grateful for the time and effort that the INTERPOL's President, Secretary General and Executive Committee members took to attend this event.

To all the moderators, speakers, and delegates who attended and participated in this event, INTERPOL appreciate your insight and involvement. To the exhibitors and sponsors who made this event a possibility, thank you. Finally, to the organizing committee and INTERPOL Innovation Centre staff, our INTERPOL colleagues and MP International who all worked tirelessly to turn an optimistic idea into a reality.

# Contact us

Inquiries? Don't hesitate and write to INTERPOL's Innovation Centre

INTERPOL
Innovation Centre Directorate

**INTERPOL Global Complex for Innovation**
18 Napier Road
Singapore 258510

**E** EDGI-IC@INTERPOL.INT
www.interpol.int / www.interpol-world.com
Twitter @INTERPOL_HQ

# For more information

@INTERPOL_GCI

youtube.com/INTERPOLWorldChannel

INTERPOL WORLD 2019
www.interpol-world.com