

INTERNATIONAL

POLICE ASSOCIATION

22

ISSN: 2791-142X

Int'l:Police

● 國際警察

第二屆國際警察運動會圓滿閉幕
A Huge Success of the 2nd IPA Games



國際警察雜誌

Int'l Police Magazine

ISSN : 2791-142X

澳門新聞局編號 : 526

《國際警察》於 2015 年創刊的中英雙語季刊，致力向國際警界和合作夥伴透視世界安全時事，促進警務科學上的學術交流，以及搜羅最新安保裝備，以成為「國際警務資訊」的重要平台。

"Int'l Police" is a bilingual quarterly magazine published in 2015, dedicated to providing an insight into the security industry to the international police community and partners, promoting academic exchanges in police science, and updating the latest information of security equipment so as to become a platform of "International Police Information".

印刷公司：澳門飛凡廣告
Printing Company: Fei Fan Advertisement

地址：澳門和樂巷 69 號美居廣場第三期 - 嘉應花園 (第四座) 地下
Addr.: Travessa da Concordia No.69 Edf. Ka Ieng Garden, RC-U, Macau

電話 | Tel.: (853) 6388 7931

出版單位：國際警察協會澳門分會
Publisher: International Police Association (IPA) Macau Section

地址：澳門高士德大馬路 87-93 高士德商業中心 4 樓 C 座
Addr.: Rua da Horta e Costa No. 87-93, Centro Comercial Horta e Costa, 4-andar-C, Macau

電話 | Tel.: (853) 2821 7411

電郵 | E-mail: ipamacauphle@gmail.com

網站 | Website: www.ipa-macau.com

Facebook: www.facebook.com/ipamacau

Instagram: www.instagram.com/ipamacau

2022 年 7 月出版
Published in July 2022

社長
Director

李雄波
Lei Hong Po

副社長
Deputy Director

魏忠
Ngai Chung

顧問
Consultant

劉芳
Liu Fang

總編輯顧問
Editing Consultant

吳榮輝
Ng Weng Fai

財務總監
Financial Manager

周紀仲
Chao Kei Chong

市場總監
Marketing Manager

張建耀
Zhang Jianyao

執行編輯
Executive Editor

李諾謙
Marco Lei

▼第二十二期 / Volume 22

03 本會活動 IPA ACTIVITIES

言論自由與記者安全

Freedom of Expression and Safety of Journalists

06 前國際會長訃聞 / Obituary of Michael Odysseos

07 轉交捐款至波蘭助烏兒童 / Donations Handover to IPA Poland

08 歐洲警察大會 / European Police Congress

09 第二屆國際民謠舞蹈和音樂節 / 2nd International Festival of Folklore and Songs



10 第二屆國際警察運動會完滿閉幕 / A Huge Success of the 2nd IPA Games

17 國際社聞 GLOBAL NEWS

杜拜警方首推虛擬貨幣

Dubai Police released 150 NFTs

18 亞洲首間女警警察局 / Asia's first women's police station

19 專家投稿 CONTRIBUTIONS

當古樹倒下

When the Ancient Tree Falls

21 網路科技幽影之困擾 (二) / Victims in the shadowy of technologies II

30 活動預告 UPCOMING EVENTS

第六十五屆世界會員大會

65th World Congress

31 國際攝影比賽 2022 / International Photo Competition 2022

33 IPA 浪漫週 / IPA Romantic Week

34 國際五人足球聯賽 / 3rd International 5-aside-Football Tournament

35 木星盃 / Jupiter Cup

36 國際警察住宿服務 / IPA House

37 國際警察教育中心 2022 年度課程 / iBZ Gimborn 2022 Programmes



The MOOC will comprise a series of free online courses and is based on the UNESCO Training Manual on Freedom of Expression and Public Order. It is aimed at police, security forces and law enforcement agencies, including trainers of police officers, gendarmerie, emergency preparedness, security and police trainees, intelligence officers, riot police, spokespersons of police and investigators.

Both the MOOC and a global training of trainers will be designed and delivered by IBZ Castle Gimborn, the training and educational facility of the International Police Association, in North Rhine-Westphalia, Germany.

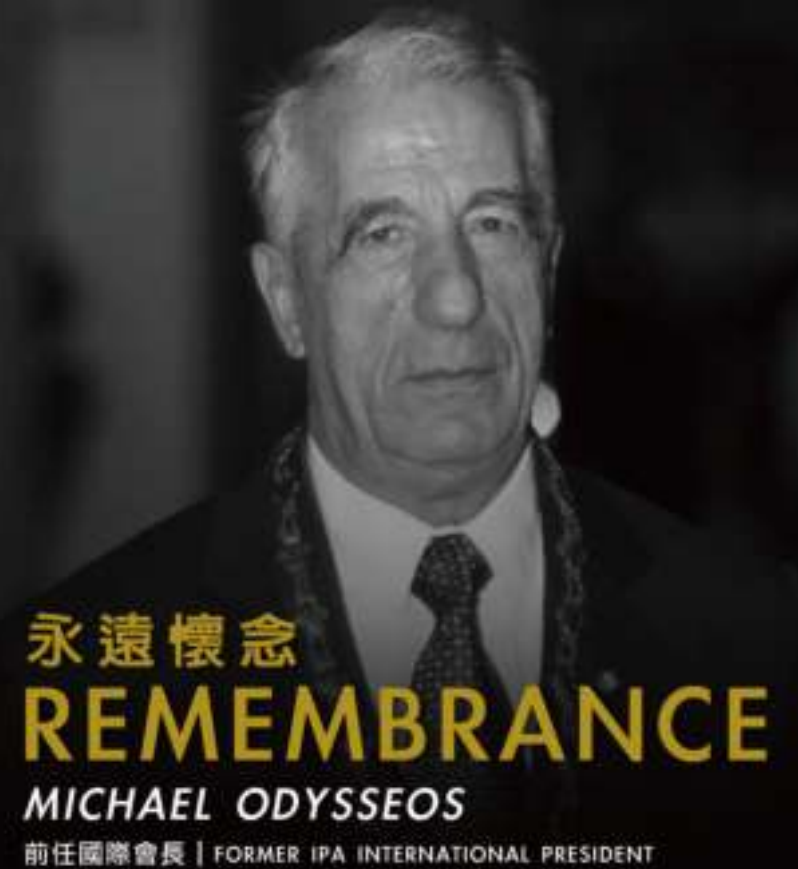
UNESCO's long experience in the training of judicial actors

According to UNESCO data, almost nine-in-ten journalist killings worldwide in recent years remain unresolved. The UNESCO and IPA training initiative will also encourage police to pursue investigations to ensure that those responsible for these crimes are identified and prosecuted.

To implement this training, UNESCO will draw from its long experience of training judges, who also play a critical role in the protection of freedom of expression, freedom of press and access to information. Since 2013, the Organization and its partners have trained 23,000 judges, judicial actors and civil society representatives from around

the world on international standards around these issues.

These activities are implemented within the framework of the UN Plan of Action on Safety of Journalists and the Issue of Impunity and will be supported with funds from the Ministry of the Foreign Affairs of the Netherlands, through the International Programme for the Development of Communication (IPDC).



我們敬愛的前任國際會長 Michael Odysseos 於 2022 年 04 月 22 日辭世。本會全體同仁表示深表哀悼，並向其家人致以摯誠慰問。

IPA 在 Michael 的生活中一直扮演著重要的角色。

Michael 在他漫長而積極的一生中貫徹本會的宗旨 - 「為友誼而服務」(Servo per Amikeco)。早於 1983 年，他協助塞浦路斯申請加入 IPA，成為正式分會之一。因此，他對 1993 年在他的祖國舉辦的第 21 屆 IPA 世界會員大會感到非常自豪。

早於 80 年代，Michael 被選為內部審計，之後從 1994 年起擔任兩屆國際副會長。此後，他更常為會務而到處奔波。對 IPA 的巨大貢獻使他先後在世界會員大會上獲得了國際警察銅獎、國際警察銀獎，以及在以色列頒發的國際警察金獎。

領導 IPA

國際警察協會是 Michael 生活的核心，而 Michael 的心亦常為 IPA 跳動。多年來，Michael 一直是我們協會在全球範圍內最偉大的大使之一。作為我們創辦人的密友和知己，他於 2000 年接任 IPA 的領導一職，同年創辦人 Arthur Troop 亦離開了大家。這是兩代偉人交接的歷史時刻，保證了我們創辦人的工作將繼續掌握在值得信賴的人手中，並保證 IPA 的價值觀和原則將繼續永存於世。而過去的十二年間，因為 Michael 以巨大的自我犧牲、奉獻精神和意志領導著我們偉大的家庭。作為會長，人們總是佩服 Michael 在工作時的認真，他對每個人的友善，他的服務意識，外交、解決問題以及政治的靈巧。

紀念 Michael

Michael 通過他的卓越承諾兌現了 IPA 的座右銘。他擁有騎士的靈魂，充滿慷慨的心和征服者的精神。我們在 IEB 和整個 IPA 世界中所有有幸與 Michael 共度寶貴時光的人都可以從他的榜樣和建議中受益，我們非常感謝他與我們分享的友誼。我們代表整個 IPA 大家庭，向 Michael 的家人以及我們在塞浦路斯分會的朋友們表示最深切的哀悼。

Mr. Michael Odysseos, former IPA International President, passed away peacefully on 22 April 2022. We express our deepest sorrow at his passing and extend condolences to his family.

The IPA always played an enormous role in Michael's life.

Michael fulfilled the IPA motto, Servo per Amikeco, throughout his long and active life, and was a driving force in ensuring his home section of IPA Cyprus always played a vital role within the association. As such, he took great pride in the organisation of the XXI IPA World Congress in 1993 in his home country.

As early as 80s, Michael was elected as Internal Auditor, before serving two terms as International Vice President from 1994 onwards. Since then, he had traveled more often for IPA affairs. His great contributions to the association have earned him the IPA Bronze Medal, the IPA Silver Medal, and the IPA Gold Medal in Israel at the World Congress in respective years.

Leading the IPA

The IPA was at the heart of Michael's life, and Michael's heart beat for the IPA. Michael was one of the greatest ambassadors of our association on a global level for many years. A close friend and confidant of our founder, he took over the leadership of the IPA in 2000, before Arthur Troop passed away in the same year. It was the handing over of the baton between two great men, a guarantee that the work of our founder would remain in trustworthy hands, with the assurance that the values and principles of the IPA would continue. This was the case, for Michael led our great family with enormous self-sacrifice, dedication and will. As President, one could always admire Michael's seriousness when conducting business, his friendliness towards everyone, his sense of service, diplomacy and his dexterity in problem solving and politics.

In memory of Michael

Michael honoured the IPA motto through the excellence of his commitment. He had the soul of a knight, a heart full of generosity and the spirit of a conqueror. All those of us on the IEB and throughout the IPA world who had the privilege of spending precious time with Michael, can count themselves lucky to have benefitted from his example and advice, and we are grateful for the friendship he shared with us. On behalf of the entire IPA family, our deepest condolences go to Michael's family, as well as to our friends in IPA Cyprus.



轉交捐款至波蘭助烏兒童

2022 年 4 月 24 日，一筆來自各地募捐集得的款項交到位於波蘭羅茲的 IPA 波蘭分會手上。在會面期間，社會事務司庫 Martin Hoffmann 先生獲當地分會會長 Piotr Wójcik 和副會長 Aneta Sobieraj 的熱情招待。

從目前募得的烏克蘭國際援助捐款中，其中的 10,000 歐元被轉交給波蘭分會。整個捐贈儀式是在羅茲的一家孤兒院裡進行，該孤兒院目前收容了 106 名來自烏克蘭的難民（93 名兒童和 13 名成人）。這家孤兒院亦將計劃收容多 150 名有需要的烏克蘭難民。而取得的款項將用於購買食品、教科書和電子學習用品，以便能夠提供烏克蘭語的遠程學習。

在捐贈儀式的過程，我們體會到協助孤兒的重要性。更有趣的是，在當地接待我們的退役警員亦是在這家孤兒院長大的，他自五歲起就在這裡生活超過十年。



DONATIONS HANDOVER TO IPA POLAND

On 24 April 2022, a donation from the international aid for Ukraine was handed over to our Polish section in Lodz/Poland. During the meeting, Mr. Martin Hoffmann, the Treasurer Social Affairs, was welcomed by the President Piotr Wójcik and Vice-President Aneta Sobieraj.

From the international donations for Ukraine Aid received so far, on this occasion 10,000 Euros were handed over to the Polish Section. The donation was handed over in an orphanage in Lodz, which currently houses 106 people from the Ukraine (93 children and 13 adults). This orphanage has made room for a further 150 people. The donations are urgently needed for the purchase of food, schoolbooks and electronic learning supplies, in order to be able to offer distance learning in Ukrainian.

The importance of helping orphanages was shown when the donation was handed over. The retired police officer, who took us from the hotel to the orphanage, had also been placed in this orphanage from the age of 5 to 19.

European Police Congress

歐洲警察大會

「變化——危機還是機遇？歐洲、社會、氣候、科技」是今年在德國柏林舉行的第 25 屆歐洲警察大會的重點主題。

歐洲警察大會是歐盟最大的內部安全會議。每年，該會議都有來自 20 多個國家的專家出席。除此之外，更有來自政界、邊境保護、特勤局以及政府、議會和行業代表與會。

德國分會作為可靠的合作夥伴，他們每年都會應邀出席這一重要的大會，並在 2022 年 5 月再次揚旗出征，主動在會上與更多潛在合作夥伴取得聯繫，提升各方合作。

德國分會柏林分支和兒童保護聯盟“Kinderschutzbund”聯同本會 IBZ Gimborn 國際教育中心一同在德國分會會長 Oliver Hoffmann 和秘書長 Jürgen Glau 的帶領下在 IPA 的展位與來賓進行了許多有趣的討論。其中一個驚喜是有遇到來自日本的會員經過展位。

大會上，德國分會會長 Oliver Hoffmann 主持了專家論壇「警用設備：堅固且安全」。而德國警察工會全國主席 Rainer Wendt 和 Panasonic 的 David Müller 則是該小組的講者。

“Change – Risk or Opportunity? Europe, Society, Climate, Technology” was the leading theme of this year's 25th European Police Congress in Berlin.

The European Police Congress is the largest conference for internal security in the European Union. Each year, the conference is a meeting place for experts from more than 20 countries. Representatives from politics, border protection, secret services as well as governments, parliaments and industries attend the conference. The German IPA Section regularly takes part in this important congress as a reliable partner and flew the flag again in May 2022 by using the many opportunities available to get in touch with network partners.

Together with Schloss Gimborn, the regional IPA group Berlin and the Child Protection Alliance “Kinderschutzbund”, President Oliver Hoffmann and Secretary General Jürgen Glau held many interesting discussions at the IPA stand. One of the highlights was when an IPA member from Japan visited the booth of IPA Germany.

Oliver Hoffmann moderated the expert forum "Police Equipment: Robust and Safe". The national chairman of the German police union, Rainer Wendt, and David Müller from Panasonic were speakers on the panel.





第二屆國際民謠舞蹈和音樂節

在 2022 年 5 月 4 至 8 日期間，塞浦路斯分會在法馬古斯塔地區的 Paralimni 和 Ayia Napa 舉辦了第二屆國際民謠舞蹈和音樂節。

開幕式在 Protaras Paralimni 進行，活動則在 Ayia Napa 舉行，三日內共有數百名人士參加。是次音樂節除了當地會員外，更有來自希臘、保加利亞、以色列、羅馬尼亞、北馬其頓和愛爾蘭的會員參與。他們把各自的文化和傳統融入到這次活動，為是次盛會增添一種特殊的風味和獨特的品味。主辦方更邀請來自克里特島干尼亞的傳統團體 Viglatores 參與和表演。東道主塞浦路斯分會則由 IPA Larnaka 分支代表出席。

在音樂節上，來自不同地區的朋友有機會體驗塞浦路斯式的熱情款待，並借此機會參觀了當地的美景和品嚐了各種傳統小食。除此之外，賓客更被安排在海盜船上進行了一次美妙的水上巡遊，最終以一個熱情如火的派對結束五天的盛會。

在此，主辦單位要感謝阿依納帕市和帕拉利姆尼市，以及普羅塔拉斯的 Kapetanios Bay 酒店，感謝他們提供寶貴的支持和款待。當然，活動得以順利舉行歸功於法馬古斯塔分支主席 George Demetriou 以及所有工作人員的辛勞。

2nd International Festival of Folklore and Songs

During the period of 4-8 May 2022, IPA Cyprus organised the 2nd International Festival of Folklore and Songs in Paralimni and Ayia Napa in the Famagusta area.

The opening ceremony was held in Protaras Paralimni, and the festival part in Ayia Napa with hundreds of spectators. The memories of the event will stay with all participants for a long time. The festival was attended by members from IPA Cyprus, Greece, Bulgaria, Israel, Romania, North Macedonia and Ireland. They all gave the event a special flavour and a unique taste from their cultures and traditions. The participation and performance of the traditional group Viglatores from Chania, Crete was a special honour. The hosts IPA Cyprus were represented by the traditional group IPA Larnaka.

During their stay on the island, our friends from different Sections had the opportunity to appreciate Cypriot hospitality, to see the beautiful sights of the area and to savour our traditional delicacies. They also enjoyed the lovely seaside and beaches, and went on a wonderful cruise on the pirate ship. The festival ended with a glamorous party where everyone had a lot of fun.

The gratitude goes to the municipalities of Ayia Napa and Paralimni, and to the Kapetanios Bay Hotel at Protaras for their valuable support and hospitality.

Last but not least, IPA Cyprus wishes to express its special thanks to the IPA region Famagusta, to its President George Demetriou, and all those members who worked hard to provide the great organisation of the event.



第二屆國際警察運動會完滿閉幕！

第二屆國際警察運動會 (IPA Games) 於 2022 年 5 月 8 至 13 日在黑山一座美麗的海濱度假勝地巴爾市 (Bar) 舉行。

來自 26 個國家的 500 多名運動員和 700 多名支持者參與是次全球警察運動和友誼慶典的盛事！本屆的運動項目包括室內足球、沙灘排球、三人籃球、射擊、乒乓球以及田徑 (5000 米) 項目。場上的運動員皆發揮出色的表現，給在場觀眾帶來了一場獨一無二的比賽和回憶！

主辦單位黑山分會更力盡完美，務求給大家留下一個美好而深刻的回憶！不論是無可挑剔的設施，完美的酒店，細至精準的統籌，在活動期間一直帶給我們眾多驚喜和難忘的時刻，特別是開幕式上，黑山國旗和奧運會會旗在兩名傘兵的帶領下從天而降，及後更有包括船上消防示範和直升機救援等表演！

我們希望提倡：對疫情說不，對戰爭說不，但對友誼和團結，我們高聲說好！

作為國際社會及文化委員會主席，Kyriakos 回顧過去三年間辛勤的準備工作，他認為一切都值得了。不論是委員會還是主辦分會，大家都竭盡所能，把最好的一切在大會上呈現出來。在此他祝賀並感謝所有運動員和教練、工作人員、義工，以及全心全意支持是次運動會的警察和地方當局。

十月份的世界會員大會上，議會委員將會決定 2024 年運動會的主辦地點。讓我們期待下屆能否突破今屆黑山分會的水準，超越自我，創造未來。

▲大會吉祥物 / Mascot of IPA Games

A HUGE SUCCESS - 2nd IPA Games

The 2nd IPA Games took place from 8-13 May 2022 in the wonderful seaside resort of Bar, in Montenegro.

The event was attended by more than 500 athletes plus over 700 visitors from 26 countries! A global celebration of Police sports and friendship! The sports competitions involved: indoor football, beach volleyball, 3x3 basketball, shooting, table tennis, as well as running (5,000 m) for both men and women, and by age categories. The performance level of the athletes was high, and they gave us all a unique spectacle!

IPA Montenegro section did its best, leaving everyone with fantastic impressions! Flawless facilities, perfect hotels, a meticulous organisation, and plenty of surprises! During the opening ceremony, the flag of Montenegro and the flag of the Games were dropped from the sky with two paratroopers, and the programme also included a demonstration of firefighting on a ship, and a rescue by helicopter!

The message shared was: no to Covid, no to war, but yes to friendship and solidarity!

As the Chairperson of the IPA Socio-Cultural Commission, Kyriakos feels completely justified. The hard work of 3 years, both of the commission and of the organising section, brought the desired result and much more! With this opportunity, he would like to congratulate and thank all athletes and coaches, the organisers, the volunteers, plus also the Police and the Local Authorities who wholeheartedly supported the IPA Games.

The Delegates will decide at the IPA World Congress in Spain in October where the next Games will be held in 2024. Montenegro raised the bar very high!

▲開幕式 / Opening Ceremony





THE FIRST DUBAI POLICE NFT AIRDROP

PARTICIPATE NOW!



杜拜警方首推虛擬貨幣

Dubai Police released 150 NFTs

杜拜警隊於今年3月31日在其官方 Twitter 上公佈正式發行首批 150 枚的 NFT (Non-fungible token)，並只要完成指定步驟，即可獲得其中一枚。活動截止前吸引超過三千人留言參與。

杜拜警察人工智能總局局長 Khalid Nasser Al Razooqi 表示，是次活動歡迎國內外人士參與，並且能有機會免費獲得杜拜警方推出的新 NFT 收藏品。

事實上，杜拜警隊不僅是阿聯酋第一個發行 NFT 的官方實體，也是世界上第一個創建自己的數字資產的警察部門。Khalid Nasser Al Razooqi 補充說，杜拜警方創建 NFT 希望傳達三個主要價值觀：創新、安全和溝通。

Dubai Police department, on 31 March, announced the release of the 150 NFTs on their Twitter account. People can get one with free of charge once finished all requirements. The post had more than 3,000 comments by deadline.

Khalid Nasser Al Razooqi, the director of the General Department of Artificial Intelligence at Dubai Police said that Members of the public, whether inside or outside the country, can own these digital assets for free by participating in the Dubai Police campaign.

In fact, according to the local media, Dubai Police is the first government entity in the UAE to create its own digital assets and the first police organisation in the world to do so. Khalid Nasser Al Razooqi informed the media that this NFT represents innovation, security, and communication.



▲來源 Source：杜拜警隊 Dubai Police

亞洲首間女警警察局

Asia's First Women's Police Station

科澤科德市女警警察局是亞洲首間供全女性警務人員使用的警察局，該局於 1973 年由當時的總理英迪拉·甘地大張旗鼓地落成，並且一直被認為賦予婦女權力的驕傲。但即使成立近 50 年，局內甚至連一張固定的餐桌都沒有。因此，近日當局呼籲增加預算，改善局內設施。

當地傳媒訪問有關人士指出，局內環境完全不能配合日常警務工作。「我們沒有獨立的調查室。由於空間不足，武器和彈藥則與文件放在一間又小又髒的房間。」她更補充：「除了長官擁有自己的辦公室外，我們一般警員（約 20 名）只可共用一間小型更衣室，局內沒有多餘作休息的地方。」

目前，市局長對該問題表示關注並盡快採取行動，務求提升當局的設施和工作環境。

The Kozhikode City Women's Police Station is the first all-women police station in Asia. It was inaugurated in 1973 with much fanfare by the then Prime Minister Indira Gandhi and the same has always been touted as a pride in terms of women empowerment. But even after close to 50 years, there is not even a permanent dining table for cops at the station. Consequently, the station calls for the raise in budget for enhancing the in-station facilities.

Local media interviewed few civil police officers and pointed out that the working environment of the station is completely incompatible with the daily police work. "We don't have an investigation room. Due to the lack of workspace, weapons and ammunition are kept in a small and dirty room with documents." Another officer added: "Other than the offices of the sub-inspector and assistant sub-inspector, what we have is a small changing room, and there is no resting place. We have around 20 officers at a time at the station and they have to use two benches to have lunch."

By now, the mayor is concerned about the issue and promised that he will take action as soon as possible to improve the facilities and working environment.

▲來源 Source：New India Express



當古樹倒下

Jared Ojuok 先生，一名警察總長兼國際警察協會肯尼亞分會秘書長，目前在肯尼亞警察局副監察長辦公室擔任新聞官。他是一位傑出的學者、精明的溝通者、變革型領導者和顧家的人。

同時，他更是一名傑出的作家。Ojuok 近日出版了他的第一部引人入勝的小說—「當古樹倒下」(When the Ancient Tree Falls)。書中以十三篇章節的形式敘述一系列的故事，從而突出了羅族人 (Luo) 的各種文化習俗和價值觀。小說以肯尼亞一個偏遠的村莊為背景，描繪了羅族傳統的政治、社會文化和經濟生活。而故事是主要關於 Ngode Aganyo 的成就，他是一個由六個相關氏族組成的聯盟 Mumbo 土地上的前殖民社區領袖。他是一位偉大的戰士和明智的領袖，他以愛和堅定的態度領導著他的家族，這使他成為所在社區良好道德和經濟成就的模範。

Jared Ojuok 寫這本書的動機是受到非洲諺語的啟發，「一個人看到一隻母雞撒糞便就應該阻止它，因為天知道誰會吃掉牠的腿？」從安全的角度來看，Ojuok 認為，向年輕一代傳授傳統價值觀和價值體系，將創造一個更有凝聚力的社會。而在這個社會中，道德將得到保存，誠實的美德、尊重長輩和親屬關係也會得到遵守。社會將尊重婦女和兒童，並共同參與培養負責任的下一代，以共同的信仰體系和價值觀為基礎，發揚文化和民族精神。

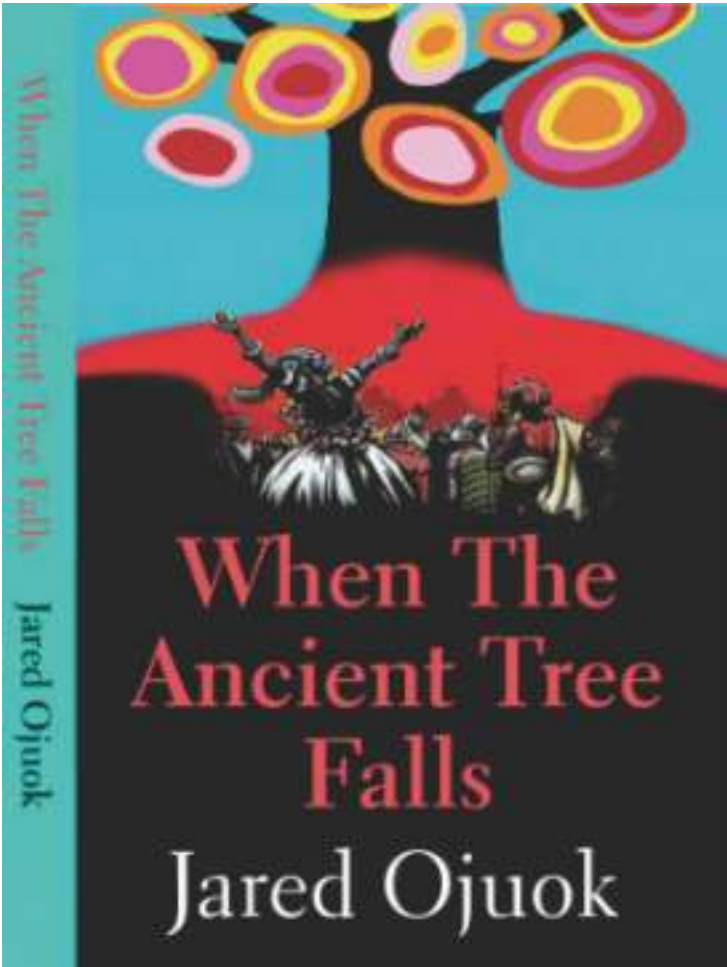
作為一名傳播愛好者，Ojuok 希望能寫出更多讓全球兒童閱讀的書籍，讓世界了解肯尼亞獨特的才能，更重要的是，將非洲文化理念重新引入全球公眾的心靈。

when the Ancient Tree Falls

Mr. Jared Ojuok, HSC, Superintendent of Police and IPA Kenya's Secretary General is currently deployed as the Public Information Officer in the Office of the Deputy Inspector General, Kenya Police Service. He is a distinguished scholar, an astute communicator, a transformative leader, and a family man.

A writer par excellence, Mr. Ojuok, wrote his inaugural fascinating novel entitled "When the Ancient Tree Falls". The series of stories narrated through the thirteen chapters in the book highlight the various cultural practices and values among the Luo people. The novel is set in a remote Kenyan village and depicts the traditional political, socio-cultural, and economic life of the Luo community. The story is about the accomplishments of Ngode Aganyo, a pre-colonial community leader in the land of Mumbo, a confederation of six related clans. He was a great warrior and a judicious leader who led his clan with love and firmness, which made him the epitome of good morals and economic attainment within his community.

Jared Ojuok's motivation to write the book was inspired



by the African proverb, "A man who sees a hen scattering excrement should stop it, for who knows who will eat the leg?" From a security perspective, Mr. Ojuok believes that teaching the young generation traditional values and value systems will create a more cohesive society where good morals will be upheld, virtues of honesty, respect for seniors, and kinship ties will also be observed. Society will respect women and children, and participate jointly in bringing up a responsible successor generation that will carry forward the culture, the spirit of a people, informed by common belief systems and values.

As a communication enthusiast, Mr. Ojuok hopes to write more books that shall be read by school children across the globe to expose the world to the unique Kenyan talent, and more importantly to re-introduce the African cultural concepts to the global public psyche.

The book is now available on Amazon for purchase.



Bulletproof Vest

- Out covering: 600D or1000D Nylon/Polyester-mixed Cotton Fabric
- Panel Material: Aramid / UHMWPE
- Model: Police、Army、Tactical
- Size: XS, S, M, L, XL, XXL, XXXL
- Weight: According to model and size
- Protection Level: NIJ0106.01 Level IIIA
- 5M shooting distance
- Bullet stop 5-6 shots
- 9mm FMJ RN; .44 Magnum SJHP
- BFS≤44mm
- Warranty: 7 years



Bulletproof Plate

- 600D oxford fabric, water resistant/ Polyurea
- Material: Alumina ceramic/ Silicon Carbide ceramic/ Boron carbide ceramic/ UHMWPE
- Normal size: 250*300mm; Other size can be customized
- Protection Level: NIJ0101.06 Level III/ Level IV
- Weight: According to size, protection Level and material
- Bullet stop: 7.62*51 M80 NATO; 7.62*39 AK47 MSC; 5.56*45 SS109 7.62*63 M2 AP; 7.62*54R API B32
- 15M shooting distance
- Level III Bullet stop: 3-6 shots; Level IV Bullet stop: 1-2 shots
- BFS≤44mm
- Warranty: 7 years



MADE IN CHINA Zhejiang Light-Tough Composite Materials Co.,Ltd.



Website: www.ltcmm.com.cn www.zjlitai.en.alibaba.com
Address: No.7, Zhenxing Road, Leidian Industrial District, Deqing County, Zhejiang
Contact person: Jimmy Liu
TEL/FAX: +86 572 8671373/ +86 572 8244505
Email: lcym@ltcm.com.cn

網路科技幽影之困擾（二）

翻譯：成振昊
會員：艾迪 · 華警教授

逐漸發展的網路犯罪和新興技術帶來的威脅

這是一個新興技術不斷湧現時代，如聯網 (IoT)、移動通信技術 (ICT)、人工智慧 (AI)、雲計算，以及人工智慧、機器人學習技術、納米技術、太空科技、生物科技、量子計算等等。這些新技術很多已經成為企業運營的常用語，如出現在準則、協議和架構中。這些新技術作為工具，會為未來全球商業帶來更高效率以及更多資源。

然而，這些突破性發展的新技術卻也成為現代犯罪手段中發展最快的，衍生最為複雜的犯罪形式。這些技術的實質性內容很容易被利用，不論距離遠近都可以造成高度的破壞性，對社會運行產生極壞影響。這些技術的應用使打擊、偵查和減少犯罪變得更加困難，也為犯罪網路提供加速成長的機會和空間，使網路犯罪更具大規模的、高利潤、極複雜等特性。尤其在去年，2020 年，新冠病毒肆虐期間，線上交流、通信和電話服務，為犯罪分子提供了新的發展土壤。

依託電腦及數位革命的進程和不斷積累，企業和工業整體推動科技現代化的發展，將敏感材料及情報分析與其重要的研究和資源相關聯，促使經濟和社會效益顯著增強，通過一系列部門運作提高了社會生產力。而這些部門目前卻面臨嚴峻的、壓倒性的、令人生畏的且耗資巨大的挑戰。保護這些資訊不被非法獲取的任務，如勞動力錯位和其他市場問題和條款，這些都加劇了不對等——尤其在世界地緣政治日趨緊張大局勢下，大多數國家認為這些高新科技對公共和國家安全帶來了風險。

實際上，現代主義科學觀遠遠超過了政府的視界。互聯網和其戲劇創造性的非凡影響往往超過了各國跟上前沿及其對未來的社會規範的影響。網路犯罪現場從受害者的地理位置延伸到全球，這也更改了刑事的司法領域，使刑事調查更為複雜——為數更多、更多行業的行動者應該發起、塑造、並實施和規範解決的方案……在某種程度上，網路犯罪是因為執法技術的缺失，這更利於犯罪，並逃避偵查。

不斷變化的犯罪環境要求負責人的對「新一代」網路罪犯進行重新評估。甚麼是最關鍵的動態框架，如何控制風險及如何找到脆弱環節。司法部門對新的犯罪環境越來越重視——另外，還需要對不斷加強的司法網路工具的理解和使用。執法人員需要裝備專業技術技能、戰略、協議、法律研究理論和程式，來應對新興網路犯罪的戰鬥。

網路安全專家及風險評估專案，2020 年度網路犯罪調查報告顯示，國家每天大約有 150 萬個潛在的網路攻擊，而全球打擊網路犯罪的成本預計每年高達到數十億甚至數萬億美元。2021 年中型企業應對重複勒索軟體攻擊的平均成本高達 6 位數。值得注意的是，被攻擊的公司的數量將翻一倍（目前全球占比 35%），即使人們的意識水



準在不斷提高，更多資源也被合理分配以降低風險——這種新型的集體犯罪被稱為「高級持續威脅」（APT），APT 具有易攻擊、傳播廣、難除根等特點。

因此，可以在一個切實可行的框架內去解決這些問題。政府可以對來自執法、情報和政策社區如知名的全球網路安全供應商、公共安全專家、法律網路犯罪專業知識和學術界資料或研究戰略機構實施開源，並做出更大範圍的承諾。形成核心結構轉型、建立相關立法並發揮其功效，這是應對國家和國際網路犯罪威脅最佳的實踐管理模式。

此外，世界首腦、專家和知名人物也公開表述網路威脅對社會和經濟的影響。政府當局通過批准法律、法規、預案，以及在刑事司法中保留有關網路安全的制度的條款，達到網路安全系統的應有的彈性和能力要求，積極、透明地將與網路相關的風險上升為國家安全問題。

關於具體的網路犯罪，目前主要集中在在敵對的民族國家支援下，有組織犯罪團夥的駭客事件。另外還有網路攻擊，如兒童

性虐待和數位兒童色情、盜版、欺詐、偽造；毒品走私、偽造、名譽傷害和經濟犯罪等。預計 2025 年將比今天增加一個數量級。在這方面，電子政務、電子商務、電子教育、電子衛生和電子環境被視為千年發展目標的推動者，它們卻為網路犯罪提供了媒介，進一步對資訊基礎設施進行新型和嚴重的攻擊。通過電子媒體發佈有害、非法或虛假資訊，這對社會造成了迫在眉睫的風險。

因此，預防網路犯罪是國家和國際網路安全針對關鍵資訊基礎設施保護戰略的一個重要組成部分；這包括通過適當的責任協調、立法預防、準備、反應和恢復框架等行動。同時，也需要採取全面的網路安全辦法，防止犯罪以及其他非法目的擴散。



威脅的本質

網路犯罪的世界現在已經成為「一個行業」，其嚴重依賴于先進的互聯網技術，被認為是侵犯隱私最高級別網路攻擊，主要以金錢為動機——執法部門和社會觀察表面，近年出現了最大膽的網路攻擊。發現網路犯罪分子通過找到薄弱環節，在進行不正當的交易時變得更加大膽、更出乎意料：移動應用程式和很多門戶入口都為其提供了更多通道——而且，提出關於資料是由誰、如何收集這些令人擔憂的問題…更糟糕的是…身份盜竊。因此，緊隨技術的演變，以「預防比治癒更好」的態度，要精通新興的網路威脅，對複雜且狡猾的惡意軟體保持警惕。通過阻止和減輕嚴重的網路犯罪攻擊可能造成的影響，採取先發制人的措施，保護關鍵資料不被截獲。

目前可以預見的最重要的網路犯罪趨勢和威脅主要包括：
（1）勒索軟體；（2）其他惡意軟體威脅（跟蹤軟體 - 加密 - 惡意程式碼 - 以手機為中心的 - 病毒）；（3）無攻擊（資料洩露和網路攻擊）；（4）阻斷服務（DoS）；（5）遠端和雲攻擊（通過雲技術或建立空間協作）；（6）快速釣魚（針對特定個人，目的是散佈複雜的惡意軟體或提取敏感資訊）和嘗試其他形式的社會控制；（7）零時差攻擊（識別軟體程式中的安全性漏洞）；（8）基於 5G 的群組攻擊（多個設備和網路同時即時攻擊）；（9）社交媒體詐騙（線上詐騙——散播虛假資訊和陰謀論——深度偽造，即「深度學習 + 偽造」）；（10）針對重要基礎設施的攻擊。

有意思的是，根據中國國家犯罪局 (CNCB) 的記錄顯示，網路對當地企業的威脅反應了網路犯罪本質的變化。網路犯罪越來越趨於擁有攻擊性和對抗性，這一點在各種形式的網路犯罪中都有體現，如高科技犯罪、資料洩露和性勒索，以及在某些情況下造成的威脅形勢，如網路間諜和網路恐怖主義。其展示了擴展攻擊和惡意行為的複雜性，另外，網路世界的持續高漲也表明其對現實世界的潛在影響。日常及工作場景目前依賴的新興技術的應用，增加了通過互聯網或資訊通信技術 (ICTs) 接觸網絡犯罪入侵的潛在因素，這可能造成許多嚴重的風險和後果，威脅公眾、國家和經濟的安全。

這些類型的網路犯罪趨勢為國內和國際都帶來了新的挑戰。比如那些不區分地域的攻擊，如今大多數勒索軟體已經滲透到世界各地的組織中（包括美國、加拿大、墨西哥、法國、德國、英國、澳大利亞、日本、印度和南非）——通過電子郵件，一種最新的傳播體系，其具大規模且有針對性的攻擊，範圍針對物聯網 / 未來城市和智慧電器、雲安全、新興技術、針對協力廠商供應商和供應鏈進行攻擊；對廣泛的工具和技術的商業利用，如「暗網」一般監視；薄弱的安全意識；恐怖主義網路犯罪聯繫，和普遍使用的匿名工具——企業仍然沒有準備好應對如今快速更新的種種威脅。

惡意軟體在的全球範圍的不斷演變，尤其是如今，資訊技術的威脅呈指數級增長，這已成為一個不可否認的事實——為了躲避商業銀行、線上供應、支付平臺等實施的安全措施，越來越複雜的變化形式不斷出現。與任何補充業務一樣，網路犯罪分子追求的最終目標，是以最大限度地提高其創新行動方式，選擇對哪些平臺進行攻擊，最能盈利。

勒索軟體（標記為「網路犯罪商業模式」，是真正意義上的「下一代」威脅。因為從技術上講，它背後是一系列攻擊工具，這些匿名技術有加密貨幣和網狀網路）這些不是直接攻擊，而是對受害者持續造成困擾，它可以一次又一次地攻擊同一個政府部門或企業。一種通用的進化模式反復鞏固這些網路威脅——這中不斷升級的屬性造就了網路罪犯成熟的戰術、技術和商業模式。

網路罪犯——因其對自己的保護，使其成為在個人和團體層面上都很難識別的駭客，比如利用代理和匿名網路改變及保護他們的身份——其展開的不間斷的多種攻擊方法，以達到目的。在單一行為中載入混合且複雜的勒索軟體，利用遠端存取的機會，感染伺服器或禁用安全軟體。全球網路犯罪網路的發展，本質上還是處於利益的驅動，形成了五花八門的網路犯罪，他們中的許多人深入暗網犯罪，這對很多目標造成了重大威脅，包括分類政府資訊、資源和關鍵的基礎設施。

儘管執法部門在應對網路威脅中日趨複雜的問題付諸了許多努力、應對了許多挑戰，但犯罪分子持續增加。利用互聯網匿名性造成了更大的風險——這幾乎滲透到每個領域、每個行業、全球範圍的每個企業，迄今為止，這一令人震驚的統計資料對整個社會產生了影響——此外，政府犯罪的駭客、非法攻擊以及威脅攻擊是最嚴重的網路恐怖主義犯罪（如網站、軍事網站、政治動機和 / 或傳播包括網路空間在內的宣傳）。

此外，犯罪分子趨於容易入門化，這是被成本效率，也就是在開發工具或技術或攻擊使用更簡單的方法所驅使的，或者由於受害者使用很差的安全防護措施，使犯罪分子甚至可以使用公開的、現成的惡意軟體進行攻擊。

另一方面，儘管網路威脅不斷的進化升級，並像資訊和通信技術 (ICTs)、及其他新興技術如人工智慧、機器學習和高性能計算 (HPC) 一樣逐漸成熟。相關風險在如此複雜的情形下呈指數級增長，這不能被完全破解，特別是在網路攻擊者使用的高科技先進方法和工具，以高效、更快、更快和更易適應的方式攻擊向當前的安全措施。此外，它呈現出一種更難追溯性，讓執法調查人員和網路安全團隊更難識別、分類和靠近。



地下網路犯罪黑市

暗網是「深度網路」的一部分，在這裡訪問是匿名的（加密、虛擬私人網路絡和其他模糊技術），在很大程度上無法追蹤，並可以訪問來自各種搜尋引擎的所有網站和資料庫，在暗網上進行非法商品和服務交易的數量是其他途徑的許多倍。這些黑市變得越來越普遍，也造成了越來越多的問題，使執法部門面臨要追蹤和起訴網路犯罪的問題。然而暗網存在的真正目的是什麼呢？它是如何運作的呢？誰是主要的運作者？在一個惡意軟體被創建後會發生什麼？資本是如何獲得、分配和 / 或洗錢的？

如今，手機、社交網路和雲計算是改變線上消費者體驗的範例，在全球範圍內，商業、商業秘密和地下經濟的迅猛發展，以及出於對資訊的預期利用，都助長了網路犯罪的傾向，在這個售賣互聯網糖果的骯髒底層，囊括了各式各樣的被竊取的帳戶憑證（如信用卡、銀行帳戶、線上支付）、工具鏈如惡意軟體（如惡意軟體）、防彈主機、商業詐騙和金融貪污，以及在數百個暗網市場繼續發展的其他服務，保守統計資料顯示每月訪問量約達到 100 萬。

這些成熟的網路犯罪組織市場有一個由買賣雙方組成的、分層次結構，每個行動都由擁有不同的專業技能的專家執行，在形成新的犯罪模式並定義明確的角色，再加上相應的商業暗語，就可以主動提供非法服務並獲得豐厚收益。通過湧現出來的合法線上技術轉換，可能導致網路威脅的根本性質改變，促使關鍵平臺實現混合盈利（如比特幣、加密貨幣和加密消息），允許無法追蹤的交易流出，就像 Tor-like 瀏覽器網路一樣進行通信以及資訊和技術的交易。

因此，越來越多的國家和使用者對數位技術互動的依賴，製造了更多接觸非法活動的機會（如網路釣魚、聊天機器人、垃圾郵件、被搜尋引擎索引的偽造的網頁等）。這些具有巨大潛能的技術盯著各行各業，對社會規範貨幣和隱私的提出了挑戰。儘管這種網路犯罪現象是新出現的，但它已經有了其可識別的排他性進化。如此高度的暴露，使它已經掌握了其他法律部門做夢都無法想像的適應和擴張強度。那麼，這些非法活動是如何發展到如此境地的呢？



開發新興人工智慧技術和網路犯罪的趨勢 -- 如何面對新的威脅

考慮到目前不同技術領域的變化速度和幅度，建立一個複雜和不確定的環境，準確預測未來的發展、場景，以及網路犯罪和造成的威脅有哪些機會和挑戰。人工智慧包括許多子學科，包括自然語言處理、機器推理、基於統計學的深度機器學習和機器人技術（超級智慧），它們可以達到或超過人類智力。

人工智慧是一個多方面的工具，並迅速滲透到現代商業運營的方方面面，以期獲得更大的經濟效益和社會效益。例如，在通信、醫療保健、疾病控制、農業、交通（自動駕駛汽車）、空間探索、科學和娛樂等領域。此外，人工智慧還可以提升驗證碼破解系統效率，包括即時識別雲計算目標，收集多個資料的使用和編譯、集和管理，以及保護記錄免受外部或潛在力量的挾持。

然而不幸的是，大多數公司都沒有意識到迅速發生的風險和面臨的挑戰，包括現有網路安全威脅的增長，已暴露到越來越重要的人工智慧系統及其結構中（如數據洩露、配置錯誤、不安全介面和應用程式介面、帳戶劫持、惡意內部威脅等），並與其他技術（例如，生物技術和核領域；演算法識別和偏差）融合。全球範圍內的網路攻擊，尤其是跨國企業的網路攻擊，已經引起了人們對人工智慧技術進一步融入日常生活和商業運營的關注。網路犯罪分子正在利用尖端的不斷發展的技術，不斷實踐，使其網路犯罪更快、更易得逞，並不斷突破現有的安全戰略管道。

目前，這些網路犯罪越來越精確、有針對性和創新性，從而增加了潛在受害者的數量。在人工智慧的輔助下，攻擊性越來越強，越來越趨向攻擊主流，系統的不斷創新使本來處於更低層次的網路犯罪也越來越複雜。在現代網路安全模型中，人工智慧與網路犯罪形成了相互依存的關係，表現為派生出各種應用程式和功能模型——這就需要更關注資料保護、隱私和其他原則和價值觀，如公平和平等、自治、透明度、問責制和應循程式等。

從好的方面看，人工智慧現在是一個開放平臺，可以討論、參與，並對建立新的管理結構、明確定義前進因素以及實現管理章程有一定影響。這些概述了人工智慧工作的基本原則、長期安全性、技術領先性、合作研究、堅持科學卓越的高標準，也包括國家和政府作出的努力、政策、社會風險領域的監管影響和原則、政策、監管影響、經濟、政策以及國防中。

在這個數字轉型和全球化的時代，作為國際警察協會 (IPA) 亞洲事務總署戰略風險情報顧問，我建議人們需要提高對網路安全的認識，基於這一出發點，政府部門、企業和貿易行業應當防範不斷出現的漏洞，還應當提防隨時發生的網路安全威脅，想要減少投入就需要主動的管理、更新風險——由於各種挑戰，如預算限制、過時的遺留系統、技術人員的流動性——專業安全和操作——實施解決方案所需的時間以及對政策解釋的不一致將使問題越來越多、越來越複雜。

VICTIMS IN THE SHADOWY OF TECHNOLOGIES II

Member : Prof. Eddie Wazen, PhD.

The Evolving Threat Of Cybercrime And The Emergent Technologies

The age of emerging technologies, such as the Internet of Things (IoT), information communications technology (ICT), artificial intelligence (AI), cloud computing, particularly in terms of machine learning and robotics; nanotechnology; space technology; biotechnology; and quantum computing to name but a few are nowadays a segment of our daily corporate idiolect -- principles, protocols and architecture, and with such tools might be a pathway to an additional outlay efficiency and resourceful future for our global commerce.

Perversely, these breakthrough development of novel technologies have quickly become one of the fastest rising forms for the entire spectrum of modern crime that raises all sorts of complications, inherently vulnerable to exploitation, a highly disruptive from both near and far, and bring about major transformative shifts in how societies function, which making it difficult to combat, detect and mitigate, and broaden an accelerative opportunities and openings for the criminality network to commit a grander, added reward and potentially further sophisticated cybercrimes, especially over the last year of 2020 online web representation, Internet-based communication and phone services as enterprising criminals have exploited fertile new ground online during the Covid-19 pandemic.

Corporations and industries as a whole that have fostered and modernized its technological advances in question relied upon computerization and digital revolution to process,



accrue; connect sensitive material and intelligence analysis on their critical research and resources for significant social and economic benefits, enhancing productivity across a host of sectors in which now pose serious challenges and face the overwhelming, daunting, and costly, task of protecting this information from those who would seek illegal access to it, including labor force dislocations and other market troubles and terms, exacerbated inequalities - especially the growing geopolitical tensions around the world and most nations view these new hi-tech risks to public safety and national security.

In effect, the scientific modernism is largely taking place beyond the purview of governments and in many cases, the extraordinary impact of the Internet and the rate of creativities is outpacing nations’ capacity to stay abreast of the cutting-edge expansions and their prospective societal norm influences, which the cybercrime scene traversed from the geographical point of the victimization to greater regions globally in which dramatically altered the criminal justice terrain and further complicating the criminal investigative efforts - a grander number and diverse actors should be involved to initiate, shape, and implement both methodological and normative solutions...and to a degree, cyber criminalities depends upon the lack of technological skills of law enforcement to advantageously commit the offenses and with assertive probabilities evade detection of crimes.

The changing criminal environment demands responsibilities reassessment of the “new breed” cyber offenders and what is the most critical dynamic framework categorizations and needs to control the risks and vulnerabilities that the

justice bureau becoming increasingly aware of the gravity of its effect to level the new playing field of crime - also, the availability and understanding of up-to-date forensic cyber tools, which become apparent that the expertise of technological skills, strategies, protocols, legal research doctrines and procedures required of law enforcers to competently battle the emerging menace of cybercrime.

Cybersecurity Experts Projects’ and Risks, 2020 annual cybercrime reviewed systematic reports with rigorous analysis that states approximately 1.5 million potential cyber attacks are attempted per day, and that the global cost of cybercrime is projected to hit almost in billions of dollars even trillions annually - and by 2021 The average cost of a repeated ransomware attacks on a mid-sized corporations and institutes is averaging high six (6) figures and above... notably, the numbers of those firms will experience double global levels of thirty five per cent (35%) despite increased levels of awareness and more resources being allocated to address risks - and this type of new class crime is referred to as an ‘Advanced Persistent Threat’ (APT), which are vulnerable to exploits for widespread impact and is here to stay.

Hence, foundation acumens in a contextual practicable framework to mitigate these issues, a broader range of commitment in developing stronger governmental open source material evidence from law enforcement, intelligence and policy communities as well as non-governmental sources such as reputable global cybersecurity vendors, public safety specialists, legal cybercrime expertise and academia data or research strategies institutes, in which forms a core structural transformation, relevant legislation and its effectiveness, and the models of best practice management for responding to the threat of cybercrime nationally and internationally.

Also, world leaders, experts and prominent figures have also openly acknowledged the cyber-threat to society and the economy, and Governmental authorities are actively and transparently elevating cyber-related risks into a national security issue, by ratifying arrangements in law, compliance, provisions and part that exists in relation to the criminal justice cyber security system resiliency and requirements on capabilities, cooperation and reporting.

With regard to specific cybercrime offences, much of the focus to date has been on cyber-enabled and intensified activities upsurge in hostile nation-state sponsored and organized crime gang hacking events, and a cyberattacks surfacing online such as child sexual abuse and digital child pornography, piracy, fraud, forgery; drug trafficking, forensic investigation, reputational harm, and economic crime, etc., which will be an order of magnitude greater in 2025 than it is today. In this regard, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for millennium development targets, and can facilitate an efficient achievement channel for criminal purposes to further new and serious threats deployment

attacks against information infrastructures, publication of harmful, illegal or false information via electronic media, which have an imminent risks by placing societies in critical ways.

Thus, Deterring cybercrime is an integral component of a national and international cybersecurity and critical information infrastructure protection strategies; this includes the adoption of appropriate responsibilities coordination’ s, legislative prevention, preparation, response and recovery framework, which requires a comprehensive approach for cybersecurity against criminal or other purposes and the proliferation activities of cybercrime.

The nature of threats

The world of cybercrime which is now become “an industry” has solidified its reliance’ s on advanced Internet technologies and the highest cyberattacks measured as an invasion of privacy with the majority of its criminality avenues are financially motivated - law enforcement and society in general observed various and most audacious cyber attacks in recent years, which showcase cybercriminals are becoming pluckier with creative streaks in executing crooked engagements and structures by finding the point of least security: mobile applications and more portal entry plugs all offer more access - also, conveying and raising alarming issues on how data been collected and by whom... and the worst yet...identity theft.

Thus, Keep up-to-date with the evolution of potential tech issues and progress spirit of “prevention is better than cure,” and conversant to the emergent of cybersecurity threats methods that equipped with belligerent and sophisticated malware in remaining vigilant regarding its status - hence, by thwarting off and mitigating the effects of serious cybercriminal possible attacks, which exhibit preemptive measures in safeguarding critical data from hostage takeover.

The most significant cybercrime trends and threats currently that can be anticipated in which includes:

- (1) Ransomware; (2) Other malware threats (stalkerware - cryptojacking -- malicious code - mobile-focused -- viruses); (3) Fileless Attacks (Data breaches and network attacks); (4) Denial of service - (DoS); (5) Remote and Cloud Attacks (implementing cloud technologies or set up collaborative spaces); (6) Spearphishing (targeting specific individuals for the purposes of distributing sophisticated malware or extracting sensitive information), and other forms of social engineering attempts; (7) Zero-Day Exploits (identifying security loopholes or vulnerabilities in software programs); (8) 5G-Enabled Swarm Attacks (multiple devices and network simultaneous attacks in real time); (9) Social Media Spoofing (online scams -- false-information and sharing conspiracy theories - deepfake ‘deep learning + fake’); and (10) Attacks against critical infrastructure.

Interestingly, according to China National Crime Bureau (CNCB) records indicate that the cyber threat to local businesses identifies a change in the nature of cybercrime, which demonstrate that cyber delinquencies are becoming more aggressive and confrontational trends that were evident across various forms of cybercrime, such as high-tech crimes, data breaches and sexual extortion, and its threat landscape in some cases - cyber-espionage and cyber-terrorism, in which exhibits the complexity of expanded attacks and sophistication of malicious activities -- also in cyberspace continuous upsurge revealing the potential for real-world impacts. The reliance on current and emerging technologies in day-to-day operations both at home and workplaces raises the prospective element for exposure to cybercrimes intrusion via the Internet or information and communications technologies (ICTs), many of which can impose serious risks and consequences that threatens the public’ s safety, national and economic security.

These types of trends present new challenges both nationally and internationally such as impacting targets indiscriminately, while most ransomware occurrences currently infiltrate organizations worldwide (Countries including the US, Canada, Mexico, France, Germany, UK, Australia, Japan, India, and South Africa) via its email -- a newest release system for both mass and targeted attacks are on the scope with the mainstream adoption of IoT /future cities and smart meters; cloud security; emerging technologies; third-party vendor risks and supplier chain attacks; wide-public and commercial availability of tools and techniques as well as the “Darknet” concerns; poor security cultures; the terrorist cybercrime nexus, and pervasive anonymization tools - and businesses are still not prepared to face today’ s fast-evolving threats.



The Evolution Of Malware

The global evolution of malware, and specifically the exponential growth of IT threats nowadays is an undeniable fact -- increasingly sophisticated variants emerge, intended to evade the security measures put in place by commercial banks, online supplies, pay platforms, etc., and as with any supplementary businesses, cybercriminals pursue active and ultimate objectives to maximize the effectiveness of their innovative operations ways achievement on which platforms to attack and the number of potential victims in the most widely-used financial profitability.

Ransomware (Labeled as a ‘cybercriminal business model’, and one of the most truly ‘NextGen’ threats since technologically it is supported by a range of attacking tools and techniques as well as anonymization measures such as

crypto-currencies and mesh networks) which is not a precipitous attack, continuously be a major issues -- it can strike again and again to the same governmental divisions and enterprises. A broad-spectrum pattern of evolution repeatedly underpins these cyber-related threats and trends - which attributed to the enhancement nature results in cybercriminals mature tactics, techniques and business models.

Cybercriminals - hackers in particular which are extremely difficult to identify on both an individual and group level due to their various security measures, such as proxies and anonymity networks that distort and protect their identity -- are deploying relentless multiple attack methodologies and objectivities to succeed, unleashing mix complex of ransomware in a single campaign, taking advantage of a remote access opportunity, infecting servers, and/

or disabling security software. The progressive of the global cyber-criminality network, which is fundamentally credited to the increased outlook for monetary incentives, has shaped numerous and diverse styles of cyber criminals, many of which dive deep into the dark web for illegal framework that poses a major threat against broad categories of targets including classified governments information, resources and critical infrastructure.

While law enforcement efforts and challenges to tackle the ever-increasing complexity issues within the threat landscape, criminals’ figures continue to grow, taking advantages of the Internet anonymity, which created larger risks - practically infiltrating every professions, every industries, every enterprises globally with shocking statistics impacted on societies as a

whole to date - also, Governmental criminality hacking, unlawful attacks and threat of attacks is the most serious cyber-terrorism offense (such as websites, military websites, politically motivated and/or distributing propaganda including Cyber Space).

in addition, criminals have tendency towards simplicity which driven by cost efficiency and by employing a simpler efforts in development of

tools or techniques and attack methods and/or using publicly available off-the-shelf malware relying on victim’ s poor security measures.

On the other hand, while the threat setting does continue to constantly evolve and mature towards ICTs as well as other emerging technologies clusters such as AI, machine learning and high-performance computing (HPC) that the associated risks are increasing exponentially in such intricacy

and complication, which cannot be completely comprehended, especially in hi-tech progressive methodologies and toolkits employed by cyber attackers to present efficient, faster and adaptable crimes to current safety measures. Furthermore, it displays harder traceability for law enforcement investigators and cyber security teams to identify and categorize evidential artifacts and the approaches.



The Cyber-Crime Underground Markets

The darknet is a part of the ‘deep web’, where access is anonymous (encryption, virtual private networks and other obfuscation techniques) and largely untraceable and reachable to a wider collection of all the websites and databases from various search engines that remarkably holds many times the volume of availability to trading in illicit goods and services online black markets, in which become increasingly commonplace and already adding to the problems in dictating the way that law enforcement facing to trace and prosecute illegal activities on cyber-space. But what is actually the black market purposefulness, and how does it function? Who are the leading operatives? What transpires after a malicious-ware is created? How is the capital acquired, allocated and/ or laundered?

Nowadays, mobile, social networks

and cloud computing are the paradigms that have changed the online consumers experience, and the global towering growth of the underground economy of business trade secrets and the desired information exploitive purposes facilitate the cybercriminal tendencies in the sordid underbelly of the Internet candy stores that encompasses a broader categories of pilfered credentials for compromised accounts (i.e., credit cards, bank accounts, online payment), toolchains such as malware (i.e., malicious software), bullet-proof hosting, kits for commercial scam and financial embezzlements, and the extras, in which continues to develop across hundreds of dark-web markets, and security statistics claims to reach an approximate of 1 million monthly visitors.

These fully-fledged Cyber-crime

organizations markets have a hierarchical structure that are made up of buyers and sellers whereby every action is performed by specialists who hold diverse technological skills and expertise in generating new criminal patterns and well-defined roles coupled with an appropriate businesslike language anonymity and presentation, which provides illegal services actively with very lucrative outcomes, and through the emergence of legitimate online tectonic shift that could trigger a fundamental variation in its threat key drivers platform schemes implementation of mixt monetization (i.e., Bitcoin, crypto-currencies and encrypted messaging) permitting untraceable outflows as well as Tor-like browser networks, communication and trade of information and technologies.

Hence, the increasing users and

national dependence on digital technologies interactions is creating an opportunity for more exposure to nefarious activities (e.g. phishing, bots, spam, fake Web pages to be indexed on search engines, etc.)...and technologies with enormous potential that target every industries and sectors, which present challenges to societal norm notions of money and privacy. Despite its relative youth, this cyber criminality phenomenon already has its identifiable exclusivity evolution, which is so lofty and exposed that it has grasped the intensities of adaptation and expansion than other legal professions and sectors in which could only dream of. So how is it possible that an illegal activity could evolve like this?

The Trend Of Exploiting Emergent Artificial Intelligence Technology And Cyber Crime -- Facing New Threats

Given the current speed and magnitude of changes in various and diverse technological areas that formulate a context of complexities and uncertainties of an exact prediction of future advances, scenarios, challenges with the metrics and opportunities for cybercrime and harm. Artificial Intelligence comprises numerous sub-disciplines including natural language processing, machine inference, statistical deep machine learning, and robotics (superintelligence) that either achieves or surpasses human intelligence.

Artificial Intelligence is a multifaceted tool and rapidly becoming the next technological movement in every aspect of daily modern business operations in which expected to bring about great economic and social benefits (e.g., communications, healthcare, disease control, education, agriculture, transportation (autonomous vehicles), space exploration, science, and entertainment, etc.)...and also, that can heighten the efficiency of improving captcha cracking systems, including real-time identification of cloud computing targets collecting several data usage and compilation, sets and management, as well as the protection of records against outside forces and/or perceiving potential threat.

Unfortunately, most corporations are unaware of the speedy risks encounters and challenges include the growth of existing cybersecurity threats and exposures into increasingly critical AI systems and its structures (e.g., Data breach, misconfiguration, insecure interfaces and APIs, account hijacking, malicious insider threats, etc.), and converge with other technologies (e.g., biotech and nuclear domains; algorithmic discrimination and biases). The highly publicized cyber attacks across the globe especially the multinational enterprises already build-up a concerning affairs about the further integrative element of AI technologies into daily-life and business operations, which cybercriminals are employing the cutting-edge evolving technological proficiencies that are constantly shifting practices in order to make their cybercrimes more efficient, swifter and adaptable to the existing security strategy channels.



Hence, these cybercrimes developed more with precision, targeted and innovative, thereby intensifying the quantity of potential victims. AI assisted and enhanced attacks are apt to an added mainstream, and the innovative of its systems is leading to a progressive complexity of even lower-level cyber criminality. Artificial intelligence and cybercrime protection have developed an interdependent relationship in contemporary cyber security models, which exhibits diverse applications and functional models derive - but also, a greater concerns over data protection, privacy, and other principles and values such as equity and equality, autonomy, transparency, accountability, and due process.

Meanwhile, Artificial Intelligence nowadays serves as an open platform for discussion, engagement and its influences of creating new governance structures and clearly defines progressive element and implementation management charter, which outlines the principles underpinning its work and overall strategy, long-term safety; technical leadership; cooperative research; upholds high standards of scientific excellence, including national Governmental efforts, policies, regulatory impacts and doctrine in the areas of societal risks, economics, politics, and national defense.

In this age of digital transformation and globalization, as the District Advisor of the Asian Affairs Bureau of the IPA, I personally recommend to increase awareness about cyber safety -- and In light of this fact, governmental divisions, corporations and trade industries should be mindful of not just the ever-growing number of vulnerabilities but also of the cybersecurity upcoming threats, in which reductive efforts required to administer proactively and govern new risks -- cause diverse challenges such as budget restrictions - outdated legacy systems - the mobility of technical staff -- balance of professional security and operations -- time involved in implementing solutions and an inconsistent interpretation of policies are becoming increasingly problematic and complex.

第六十五屆世界會員大會



西班牙濱海略雷特

眾所周知，西班牙分會原定於2020年舉辦是次大會。但COVID-19的嚴峻情勢逼使我們在2020年和2021年兩度取消舉辦。現在，我們很高興宣佈第六十五屆世界會員大會將於10月3日至9日在西班牙舉行。

為了組織這次活動，我們選擇了濱海略雷特市（赫羅納省），這個地方位於布拉瓦海岸，一個非常愉快的旅遊勝地，我們相信這裡必定能滿足您的期望，而大會的舉辦地點將是屬EVENIA奧林匹克度假村一部分的奧林匹克會議中心，這是一個由四家酒店組成的現代化酒店度假村，位於濱海略雷特住宅區。其宜人的環境和現代化的設施成功舉辦了多項大型活動。面積超過30,000平方米，設有：大花園、熱帶游泳池、溫水游泳池、水療中心、網球場和帶頂棚的停車場。它位於濱海略雷特海岸的布拉瓦海岸（距離海灘1000米。步行12分鐘）。10月的平均氣溫為22度，巴塞隆納國際機場與濱海略雷特(Costa Brava)的距離為1小時車程。赫羅納國際機場和略雷特之間的距離：25分鐘車程。

我們等待你的到來！

As you all know, IPA Spain Section has been designated to organize the 65th IPA WORLD CONGRESS OCTOBER 2020. COVID-19 forced us to cancel the organization of the WC during the years 2020 and 2021. It is our pleasure to announce that the 65th IPA World Congress is taking place from 3rd to 9th October 2022 in Spain.

To organize this event, we have chosen the city of Lloret de Mar (province of Girona), this place is in the Costa Brava, a very pleasant tourist place that will surely satisfy all your expectations and the place for the congress will be The Olympic Congress Center, part of the EVENIA Olympic Resort, a modern hotel resort composed of 4 hotels**** and located in a residential area of Lloret de Mar. Its pleasant environment and modern facilities guarantee a successful development of any kind of events. The surface area of over 30,000 m2 and feature: large gardens, tropical swimming pools, heated swimming pools, spa, tennis court and covered car parking. It is located on the Costa Brava, Lloret de Mar (1000 m. from the beach. 12 minutes walking). The average temperature in October is 22 degrees and the distance between Barcelona International Airport and Lloret de Mar (Costa Brava) is 1 hour by car. The distance between Girona International Airport (Low Cost) and Lloret: 25 minutes by car.

We are waiting for you!



國際攝影比賽 2022

International Photo Competition 2022

繼成功且非常受歡迎的 2020 年攝影比賽之後，國際警察協會社會及文化委員會（SCC）很高興宣佈舉辦「IPA 國際攝影比賽 2022」。是次獎金同樣豐富，並高達 400 歐元。入圍作品亦將於西班牙舉行的 2022 年 IPA 世界會員大會期間首次展出。會議結束後，亦會交由各分會在各各地巡迴展出。

比賽分為以下兩個類別：

公開組：任何攝影主題 / 題目

專題組：執勤中的警務人員

更多詳情可掃描二維碼。



Following on from the successful and very popular Photo Competition 2020, the IPA Socio-Cultural Commission is pleased to announce the IPA International Photo Competition 2022. The prize is up to EUR400 and please do not miss out the chance to win. A first display of the photos will take place during the IPA World Congress 2022 in Spain. A total of 50 images will be selected and will be sent to Spain for mounting and displaying at an International Exhibition. Subsequently the photographs will be offered to other sections, to encourage them to hold similar exhibitions.

There are two categories available for this year's competition. The Open Category is for Any Photographic Subject meanwhile Subject Category only accepts photos about Police At Work. Further information can be found by scanning the QR code.



MICH2000 (Tactical)

- Aramid / UHMWPE
- Black/MB Green/Coyote/Multicam
- Polyurea Spray or Painting
- Size: S, M, L, XL Weight: 1.30-1.70kg
- Side rail, NVG, Velcro, Elastic cord
- NIJ0106.01 II IAW NIJ0108.01 IIIA
- 5M Shooting Distance
- 4-5 shots
- 9mm FMJ RN; .44 Magnum SJHP
- V50 ballistic test according to STANAG 2920, 17 grain: ≥ 650 m/sec

High Cut (Tactical)

- Aramid / UHMWPE
- Black/MB Green/Coyote/Multicam
- Polyurea Spray or Painting
- Size: L, XL Weight: 1.45-1.65kg
- Side rail, NVG, Velcro, Elastic cord
- NIJ0106.01 II IAW NIJ0108.01 IIIA
- 5M Shooting Distance
- 4-5 shots
- 9mm FMJ RN; .44 Magnum SJHP
- V50 ballistic test according to STANAG 2920, 17 grain: ≥ 650 m/sec

PASGT/M88

- Aramid / UHMWPE
- Black/MB Green/Coyote/Multicam
- Polyurea Spray or Painting
- Size: S, M, L Weight: 1.30-1.65kg
- If bolt-less type, utilizing special tube suspension system
- NIJ0106.01 II IAW NIJ0108.01 IIIA
- 5M Shooting Distance
- 4-5 shots
- 9mm FMJ RN; .44 Magnum SJHP
- V50 ballistic test according to STANAG 2920, 17 grain: ≥ 650 m/sec



MADE IN CHINA

Zhejiang Light-Tough Composite Materials Co.,Ltd.



Website: www.litcm.com.cn www.zjlitai.en.alibaba.com

Address: No.7, Zhenxing Road, Leidian Industrial District, Deqing County, Zhejiang

Contact person: Jimmy Liu

TEL/FAX: +86 572 8671373/ +86 572 8244505

Email: lcyl@litcm.com.cn



IPA

INTERNATIONAL POLICE ASSOCIATION
VALLÉS OCCIDENTAL **BARCELONA**

♥ **IPA Romantic Week** ♥

St Valentine's event

February 14th/22nd 2023



BARCELONA +

VENICE CARNIVAL EXPERIENCE



**25-28
AGOSTO
2022**

Viareggio - Versilia

La 7^a Delegazione Toscana
e il Comitato Esecutivo Locale
Ipa di Pisa, organizzano

**3^o Torneo internazionale
di calcio a5**

"ipa nel cuore"



eventour
THE INTERNATIONAL SPORT

IPA REGION 12 BUCHAREST INVITES YOU TO

JUPITER CUP

BEACH SOCCER TOURNAMENT

Registration of the teams and booking the rooms will be made before the **01st July 2022** by the head of delegation directly to Region 12 IPA Bucharest!

For more details regarding the tournament, please contact **Ionel David: +40 742 101 846** or via email **ionel.david@hotmail.com**

4-10 SEPTEMBER 2022

EVENT ORGANIZED BY IPA REGION 12 BUCHAREST IN PARTNERSHIP WITH IPA ROMANIAN SECTION, COHOTELS AND THE ROMANIAN FOOTBALL FEDERATION!



cohotels



國際警察住宿服務

IPA House

國際警察協會 (IPA) 目前在 16 個分會的支持下，擁有超過 40 個物業，為會員在外遊時提供一個優惠的住宿服務。

涵蓋範圍由著名觀光城市如法國巴黎 (Paris) 以及德國柏林 (Berlin)，至寧靜淡泊的郊外如芬蘭的拉普蘭區 (Lapland)，為會員帶來一個非凡且地道的旅遊體驗。國際警察住宿服務 (IPA House) 讓會員在旅遊期間可以結交各地會員，擴展社交圈。

有興趣人士，歡迎掃描下面的二維碼參閱最新版本的 IPA Hosting Book 以瞭解更多關於住宿服務的資訊。

The IPA owns more than 40 properties in 16 IPA sections where members can stay in reasonably priced accommodation.

With locations ranging from sightseeing hotspots such as Paris and Berlin, to the beautiful winter wonderland surroundings of Lapland in Finland, to our apartment on the Australian Gold Coast, IPA Houses offer a unique opportunity to travel the world and meet local members.

Alongside these houses we have hundreds of 'other accommodation' options available, including members' holiday homes and discounts at hotels, with the number of options increasing each year.

Have a look in our IPA Hosting Book, which is regularly updated and provides an overview of each IPA House and Other Accommodation option:

2022 六月版 / June Edition





Encounter and Learning




























Follow us on
facebook.
facebook.com/IBZGimborn



Simply scan QR code
and book online.

Seminar Programme 2022

Prices incl. lodging and board | seminar prices subject to change

22 01	Aktiv in den Ruhestand	10.01. – 13.01.	480 € IPA 320 €	22 25	Tactical First Aid II 	13.06. – 14.06.	490 € IPA 360 € <small>(incl. consumables)</small>
22 02	Aktiv in den Ruhestand	24.01. – 27.01.	480 € IPA 320 €	22 26	Umweltkriminalität – Fälle organisierter und grenzüberschreitender Kriminalität im Verbrechen gegen die Umwelt 	20.06. – 24.06.	480 € IPA 320 €
22 03	Die Macht der Clans – Clankriminalität in Deutschland	31.01. – 04.02.	480 € IPA 320 €	22 26	Criminalità contro l'ambiente – Casi di criminalità organizzata e transfrontaliera nei crimini contro l'ambiente 	20.6. – 24.06.	480 € IPA 320 €
22 04	Aktiv in den Ruhestand	07.02. – 10.02.	480 € IPA 320 €	22 27	Police Street Survival Training 	04.07. – 08.07.	480 € IPA 320 €
22 05	Konflikte konstruktiv lösen	14.02. – 17.02.	480 € IPA 320 €	22 28	Unter Druck – Umgang mit belastenden Anforderungen	08.08. – 10.08.	480 € IPA 320 €
22 06	Eingriffsrecht und Europarecht – Rechtssicherheit bei der grenzüberschreitenden Zusammenarbeit	21.02. – 23.02.	350 € IPA 275 €	22 29	Polizeiliches Management von Großveranstaltungen – Kundgebungen, Demonstrationen, Sportereignisse 	15.08. – 19.08.	480 € IPA 320 €
22 07	Stress- und Konfliktsituationen – Wenn die Stressverarbeitung nicht mehr funktioniert – Hilfe durch Stressmanagement	21.02. – 24.02.	480 € IPA 320 €	22 29	Gestionarea polițienească internațională a evenimentelor majore – Mitinguri, demonstrații, evenimente sportive 	15.08. – 19.08.	480 € IPA 320 €
22 08	Taktische Einsatzmedizin 	24.02. – 25.02.	490 € IPA 360 € <small>(inkl. Verbrauchsmaterial)</small>	22 30	Social Media Master Kurs	22.08. – 26.08.	890 €
22 08	Tactical First Aid 	24.02. – 25.02.	490 € IPA 360 € <small>(incl. consumables)</small>	22 31	Environmental Crimes – Illegal Profits and Cross-Border Crime 	29.08. – 02.09.	480 € IPA 320 €
22 09	Fasten? Trau Dich! – Heilfasten im Oberbergischen Land	28.02. – 06.03.	480 € IPA 320 €	22 32	Digitalisierung und Polizeiarbeit/YouPo Seminar 	05.09. – 09.09.	480 € IPA 320 €
22 10	Social Media XL – Fit im Nutzen Sozialer Medien	07.03. – 11.03.	890 €	22 32	Digitalisation and Police Work/YouPo Seminar 	05.09. – 09.09.	480 € IPA 320 €
22 11	The Potentials of Virtual Reality in Police Training 	14.03. – 18.03.	480 € IPA 320 €	22 33	Motorradkultur und Sicherheit – Ausfahrten im Bergischen Land mit Demonstrationen und Übungen zum sicheren Motorradfahren	09.09. – 11.09.	350 € IPA 275 €
22 12	Gegen den Staat, dem sie dienen – Reichsbürger, Verschwörungstheoretiker und Rechtsextreme in staatlichen Organisationen	23.03. – 25.03.	230 € IPA 180 €	22 34	Missing! – The phenomenon of missing people in modern European societies 	12.09. – 16.09.	480 € IPA 320 €
22 13	Aktiv in den Ruhestand	28.03. – 31.03.	480 € IPA 320 €	22 34	Zaginiony! Fenomen zaginięć ludzi w społeczeństwach nowoczesnej Europy. 	12.09. – 16.09.	480 € IPA 320 €
22 14	Le maintien de l'ordre: Face aux nouvelles formes de manifestations, que faut-il faire pour adapter les techniques de maintien de l'ordre? 	04.04. – 08.04.	480 € IPA 320 €	22 35	Spanisches Seminar – Thema wird noch bekannt gegeben 	19.09. – 23.09.	480 € IPA 320 €
22 15	Aktiv in den Ruhestand	11.04. – 14.04.	480 € IPA 320 €	22 35	Seminario Español – Tema por anunciar 	19.09. – 23.09.	480 € IPA 320 €
22 16	Katastrophen- und Krisenmanagement 	25.04. – 29.04.	480 € IPA 320 €	22 36	Führungskraft sein – habe ich mir das so vorgestellt?	28.09. – 30.09.	480 € IPA 320 €
22 16	Disaster and Crisis Management 	25.04. – 29.04.	480 € IPA 320 €	22 37	ASP Instructor Course 	04.10. – 06.10.	350 € IPA 275 €
22 17	Social Media XXL – Aufbau-seminar	02.05. – 06.05.	890 €	22 38	Schreibwerkstatt – Jubiläumsworkshop	07.10. – 09.10.	290 € IPA 190 €
22 18	Handlungssicherheit bei der Bewältigung polizeilicher Einsätze mit psychisch kranken und/oder suizidalen Menschen	09.05. – 10.05.	230 € IPA 180 €	22 39	Gimborn writers	10.10. – 14.10.	480 € IPA 320 €
22 19	Feedback als Führungsaufgabe: Kritik äußern – Kritik annehmen	11.05. – 13.05.	480 € IPA 320 €	22 40	Wenn die Stressverarbeitung nicht mehr funktioniert – Hilfe durch Stressmanagement	24.10. – 27.10.	480 € IPA 320 €
22 20	Motorradkultur und Sicherheit – Training für verantwortungsbewusstes Motorradfahren	13.05. – 15.05.	350 € IPA 275 €	22 41	Im richtigen Moment (k)ein Argument?! – Professioneller Umgang mit Reichsbürgern, Populisten und Verschwörungstheoretikern	02.11. – 04.11.	350 € IPA 275 €
22 21	Führung in Aussicht oder den Rollenwechsel meistern	23.05. – 25.05.	480 € IPA 320 €	22 42	Aktiv in den Ruhestand	21.11. – 24.11.	480 € IPA 320 €
22 22	Gewalt im Spiel – Hooligans und Ultras im Umfeld von Fußballspielen 	30.05. – 03.06.	480 € IPA 320 €	22 43	Bedrohung durch Cyber Terrorismus – Wie Terroristen und Extremisten das Internet für ihre Zwecke nutzen 	05.12. – 09.12.	480 € IPA 320 €
22 22	Przemoc w grze – huligani i ultrasi wokół meczów piłkarskich 	30.05. – 03.06.	480 € IPA 320 €	22 43	The Threat of Cyber Terrorism – The use of the internet by terrorists and extremists 	05.12. – 09.12.	480 € IPA 320 €
22 23	Aktiv in den Ruhestand	07.06. – 10.06.	480 € IPA 320 €				
22 24	Unter Druck – Umgang mit belastenden Herausforderungen	13.06. – 15.06.	480 € IPA 320 €				
22 25	Taktische Einsatzmedizin II 	13.06. – 14.06.	490 € IPA 360 € <small>(inkl. Verbrauchsmaterial)</small>				