

INTERNATIONAL

POLICE  
ASSOCIATION



ISSN: 2791-142X

Int'l:Police

● 國際警察

在國內推動國際警察住宿服務  
Promoting IPA House in China



國際警察協會澳門分會 International Police Association Macau Section

# 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，以及搜羅最新安保護備，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 10 月出版  
Published in October 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

▼第二十三期 / Volume 23

## 03 本會活動 IPA ACTIVITIES

首間 IPA 國際管理學院  
The First IPA International Management Academy

05 第 27 屆 IPA 地中海地區會議 / 27th Meeting of Mediterranean IPA Sections in Ohrid

06 動起來！推廣高爾夫球運動 / Let's Golf! Promoting the Sports of Golf in Popularity

 07 在國內推動發展國際警察住宿服務 / Promoting IPA House in China

## 09 國際社聞 GLOBAL NEWS

身高不等於一切！未足 160 公分都可以投考西班牙警察  
Now you can be a police even shorter than 160cm

10 日本引入視像報警 / 110 Video Reporting System in Japan

12 局長家 500 米外的假警局 / Bogus Station 500m Away From the Chief's Home

## 13 專家投稿 CONTRIBUTIONS

六個你不知道的德國法律  
Six German Laws You Should Know Before Arrival

15 言論自由和記者安全課程內容概論 I / MOOC on Freedom of Expression and Safety of Journalists (I)

17 網路科技幽影之困擾 (三) / Victims in the shadowy of technologies III

## 27 活動預告 UPCOMING EVENTS

第十二屆國際展覽會  
Barcelona International Trader Show

29 IPA 超級之旅 / IPA Super Tour

30 第 3 屆岡比亞之行 / 3<sup>rd</sup> Tour of Gambia

31 IPA 浪漫週 / IPA Romantic Week

32 國際警察住宿服務 / IPA House

33 國際警察教育中心 2022 年度課程 / iBZ Gimborn 2022 Programs



自 2022 年 9 月 25 至 29 日起，IPA 羅馬尼亞分會開辦歷史上第一所 IPA 國際管理學院。

是次倡議自 IPA 羅馬尼亞分會和以色列分會發起。開辦這樣的學院主因是目前缺乏一個專業平台可以研究和交流有關 IPA 管理專業的議題。在世界會員大會上，由於時間緊張，導致沒有深入討論的空間。每年會內都有開辦各類專業講座，唯獨是欠缺討論會務管理的專題講座。人們認為即使在本會的國際教育中心（IBZ Gimborn）亦沒有一個單獨的國際研討會專門討論 IPA。

該項目的目的是每年舉辦一次由分會會長和主席參加的專題研討會。第一階段的目的以有限的方式舉辦第一次這種類型的研討會，主要的想法是它可以以一種簡單的方式進行，同時讓所有參與者都能積極參與其中。在得到首次研討會的意見回饋後，我們相信不久的將來會邀請更多的分會加入這個項目。

是次研討會由專業委員會主席 Demetris Demetriou 協調，這表示 IEB 不僅了解這一舉措的目的，而且了解並認同這個項目為整個協會帶來的未來得益。

在錫比烏舉行的研討會上，來自羅馬尼亞、以色列、北馬其頓、塞浦路斯、德國 6 個地區的 45 名代表，以及保加利亞的一名觀察員參加了是次研討會。

第一部分是各分會的介紹，大家就自己所在分會或地區的情況、問題、成就、會員和當地 IPA 理事會的需求等進行了簡單介紹。第二部分是 IPA 戰略規劃的專業講座，

然後將代表們分組，每個組別皆就一個議題進行討論。確定了組長後，並在第三部分上向與會者發表總結，以及進行一般性的討論。

四個主題分別是：

- 如何招募年輕警務人員，如何鼓勵年輕警務人員對本會活動產生興趣；
- 如何維持資深 IPA 會員，如何與他們保持聯繫並將他們融入本會活動；
- 如何與各級警察部門以及相關政府部門和同類組織建立聯繫；
- 與世界各地的分會作出聯繫、合作和國際倡議的想法。

分會主席、主席團成員和參與 IPA 管理的成員在會上可以相互學習，深入了解問題。除了相互學習之外，結識來自不同分會的會員也是活動目的之一。

與會者在總結皆提出，雖然他們本身對本會有深厚的了解，但經過一連串的交流後，他們皆同意自身對 IPA 的認識有更上一層樓的提升，並且通過長時間深入的研討環節，與各分會成員建立更緊密的連繫，對未來舉辦活動有不少幫助。

總而言之，繼續開展與警察工作相關的專業項目是非常重要的，與關注協會內部問題同樣重要。對 IPA 系統進行深入分析，確定 IPA 想要達到的目標在哪裡、IPA 存在的問題以及實現 IPA 目標的最佳方法是什麼。

From 25-29 September 2022, IPA Romania hosted the first and historic IPA international management academy.

The initiative for this academy came from the IPA sections of Romania and Israel. The reason to start such an academy was due to a lack of a professional platform that allows for the study and exchange of information on professional issues of IPA management. During the World Congress, time is short, and so far, no room for in-depth professional discussions has been found. Every year there are instructive professional lectures on fascinating topics, but without any connection to the IPA. They consider that even at IBZ Gimborn, the education centre and IPA flagship, there is not a single international seminar dealing solely with the IPA.

The purpose of this project is to hold a professional seminar once a year with the participation of members of the presidency and chairpersons of branches. In the first phase, the intention was to hold the first seminar of its kind in a limited way, because the main idea was that it

could be carried out in an easy way and allow at the same time for all participants to be actively involved. Now, after the seminar has taken place, and after seeing the feedback of this project, more national sections will be invited to join this project in the soon future.

The seminar is coordinated by the chairperson of the Professional Commission Demetris Demetriou, which shows the IEB not just understands the purpose of this initiative, but also the future benefits for the Association as a whole.

With regard to the seminar held in Sibiu, there were 45 participants from 6 sections which were Romania, Israel, North Macedonia, Cyprus, and Germany, plus an observer from Bulgaria.

The first part was devoted to the presentation of each section, and everybody spoke about the situation in their own section or region, about the problems, the achievements, the needs for members and local IPA boards.



In the second part, a professional lecture on strategic planning in the IPA was given, and then the representatives were divided into discussion groups, with each group receiving a topic for discussion. Group leaders were determined, and the summaries were presented in the third plenum to all participants, and a general discussion was held with all participants.

The 4 topics were:

- how to recruit young police officers, and how to encourage young police officers to become interested in activities;
- how to keep veteran IPA members, how to keep in touch and integrate them into activities;
- how to develop contacts with the Police Command at all levels, as well as relevant government ministries and similar organisations;
- Ideas for contacting IPA sections around the world, collaborations, and international initiatives.

A meeting of branch chairpersons, members of the presidency

and members engaged in IPA management allows mutual study, understanding issues in depth, without pressure and without pursuing a stressful schedule. Beyond the mutual study, it is very important to meet members from different sections.

All participants testified in their summary that although they had knowledge in everything related to IPA, now they knew much more, their motivation had increased, and connections had been formed that will contribute to tightening the ties and expanding the activities.

In conclusion, it is very important to continue the professional projects related to police work, but it is at least as important to focus on the internal problems as an association, to make an in-depth analysis of the IPA system, to establish exactly where the IPA wants to reach, what problems IPA has and what the best ways are to achieve the goals of the IPA.



## 第 27 屆 IPA 地中海地區會議 27th Meeting of Mediterranean IPA Sections in Ohrid

▲文 Author/ Kyriakos Karkalis

第 27 屆地中海地區會議於 2022 年 6 月 16 日至 19 日在北馬其頓田園詩般的奧赫里德湖舉行，並且取得了巨大成功。會有來自阿爾巴尼亞、波斯尼亞和黑塞哥維那、保加利亞、克羅地亞、塞浦路斯、希臘、以色列、馬耳他、黑山、北馬其頓、葡萄牙、羅馬尼亞、塞爾維亞、斯洛文尼亞、西班牙等 16 個國家的代表以及應邀的奧地利代表與會。除此之外，是次會議更邀請到保護人權組織（OADO）的創辦人兼主席弗洛倫丁·斯卡萊奇（Florentin Scaletchi）作為特邀嘉賓。

Kyriakos Karkaiis 先生和 Martin Hoffman 先生代表 IEB 向與會人員轉達了國際理事會的問候和祝願。是次會議在友好的氣氛下舉行，符合我們協會的原則和價值觀。

在會議期間，IPA 會員和同僚們發表了數個有趣的專題演講，內容對與會的每一個人就協會的未來發展和計劃都有很大的啟發。

最後，會議主席 Karkaiis 先生特別感謝是次主辦單位 IPA 北馬其頓分會的安排。伴隨著遊覽本地各類特色景點和美景，夜晚伴隨著音樂和來自各方無懈可擊的款待，使是次旅程變成各位人生其中一段難忘的回憶。

The 27<sup>th</sup> Meeting of Mediterranean Sections was held with great success from 16-19 June 2022 in the idyllic setting of Lake Ohrid in Northern Macedonia. Delegations from 16 countries participated including Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Greece, Israel, Malta, Montenegro, Northern Macedonia, Portugal, Romania, Serbia, Slovenia, Spain, plus the invited section, Austria. Beyond that, the founder and President of the Organisation for Human Rights Defence - OADO, Florentin Scaletchi, was invited as a special guest.

Mr. Kyriakos Karkaiis and Mr. Martin Hoffman represented the IEB and conveyed the greetings and wishes of the International Board to the meeting's participants. The Mediterranean Sections' meeting was held in a friendly atmosphere, in accordance with the principles and values of our Association.

Fellow Officers and members of the IPA, during the meeting, made several interesting presentations of professional interest. It was inspiring to everyone in the meeting for the future plan and the development of the association.

Last, but not least, Mr. Karkaiis, the chairperson of this meeting, particularly highlighted that the organising section IPA North Macedonia took great care to ensure that the Mediterranean Sections' meeting was an unforgettable occasion, with wonderful excursions to the uniquely beautiful landscape, nights with music and impeccable hospitality from all sides.

## 動起來！推廣高爾夫球運動

## Let's Golf! Promoting the Sports of Golf in Popularity

▲文 Author/ Marco Lei

由今年九月份起，會員憑有效會員證於珠海名人高爾夫球竹仙洞俱樂部可享有入會優惠，以及場內餐廳優惠。

位於珠海市灣仔的竹仙洞俱樂部佔地面積有 25 萬平方米，擁有超過百個高爾夫打位。除此以外，俱樂部內更設有多種娛樂設施，包括酒廊、水吧、特色餐廳、健身中心等。

是次合作由本會新晉名譽顧問羅利女士發起，以「高爾夫離你不再遙遠」的企業理念，與本會一拍即合。透過是次合作，除了豐富會員和紀律部隊人員在工餘時的生活外，本會希望能夠積極推動社會上多元化的運動類型，讓更多人能認識和接觸高爾夫球這項運動。

讓我們為友誼而服務，以球會友。

Starting with September of this year, members with the effective membership ID can enjoy the discounts on enrolment as well as the in-club restaurant service at Master Golf Zhuxiandong Club.

Situated at Wanzai, Zhuhai, Zhuxiandong Club covers an area of 250,000 sq.meter and has more than 100 of driving ranges in site. Moreover, the club has a variety of entertainment facilities such as lounges, bars, restaurants, fitness centers, and so on.

This cooperation was initiated by Ms. Rowley, the new Honorary Advisor of the Macau Section. With the "Golf is never far away from you", the corporate philosophy does match with the Association. Through this cooperation, we, the IPA, would like not just to enrich the lifestyle of members and law enforcement personnels beyond their working days, but also actively promote the diversity of sports in the society and let more people know about the sports of golf.

Let's servo per amikeco and make friends through golf!



在國內推動發展國際警察住宿服務  
Promoting IPA House in China

▲文 Author/ Marco Lei



日前，會長李雄波爵士率領代表團到訪位於中國浙江省湖州市德清縣的莫干山。有「江南第一山」的美譽的莫干山，於1994年被列為中國國家重點風景名勝區，每年遊客量達至過百萬之多，這不難想象它在世界上的知名度。

除了作為江南地區的第一山峰外，莫干山亦以「清涼世界」著名，四季各有其獨特的景色，而且鄰近景點眾多，十分適合作為本會國際警察住宿服務的先鋒地段。

此行，本會代表團拜訪相關單位和人士瞭解當地文情，與此同時亦向各位介紹本會的國際警察住宿服務。我們希望借助本會平台能夠推廣更多國家重點風景名勝給國外的同僚們。透過到訪莫干山等名勝以感受和體驗中華文化的精粹和我國引人入勝的風景。

同行出席的有常務副會長魏忠爵士、亞洲事務總署首席監督朱美興先生、區域顧問盛志明先生、公關部部長陳伯聯先生、副部長陳繼隆先生以及榮譽會員楊體春先生。

In September, President Po led a delegation to visit Mount Mogan which is located in Deqing County, Huzhou City, Zhejiang Province, China. Mount Mogan, known as "the Top Mount in Jiangnan", has been listed as a National Park of China since 1994. There are over millions tourists visiting here annually and it is not difficult to imagine how popular it is on the globe.

Other than being the top mount in Jiangnan, Mount Mogan has another name of the "Cool World". There are different scenes in each season and various attractions are surrounding the Mount Mogan. With all these conditions, this is, for sure, one of the best spots for pinoeering the service of IPA House of the Association in China.

During the trip, the delegation met relevant units and personnels for studying more about the local culture. In the meantime, they also gave a brief presentation of the IPA House. With the platform of IPA, we would like to promote as many National Park of China as possible to the law enforcement personnels around the world. By visiting National Parks such as Mount Mogan, we want to show them the essence of Chinese culture and the fascinating scenery of our country.

The delegation is made up with members as follow: Chevalier Ngai Chung, the Executive Vice-President; Mr. Zhu Mei Xing, Chief Supervisor of the Asian Affairs Bureau; Mr. Bill Sheng, District Advisor; Mr. Simon Chan, the Chief of Public Relations; Mr. Chen Ji Long, Deputy Chief of Public Relations; and Mr. Yang Ti Chun, Honorary Member.



## 身高不等於一切！未足 160 公分都可以投考西班牙警察

西班牙最高法院於七月份時就當地對女警的最低身高限制表示遣責，主審法官認為該規則對部分人士帶有「歧視」意味。

事源一名年輕的女警候選人在 2017 年因身高僅差四公分而遭拒參加警察考試後，向西班牙最高法院投訴。

根據西班牙警隊要求，想要加入國家警察部隊的女性必須達到 1.60 米（5.2 英尺）的最低身高要求。與此同時，男性必須至少有 1.65 米（5.4 英尺）高。而法院指出，這項身高限制「構成對女性的間接歧視，因為相較於女性，對男性的最低身高限制（165 公分）更加寬鬆。在西班牙，女性未達門檻（160 公分）的百分比（25%）遠高於男性未達門檻（165 公分）的百分比（3%）」。

因此，法院命令若原告通過考試，警方應雇用她，並比照 2017 年考取的女警給予同等薪級待遇。

## NOW YOU CAN BE A POLICE EVEN SHORTER THAN 160CM

Spain's Supreme Court in July has condemned the local minimum height requirement for female police officers, which the judge said was "discriminatory" for some people.

A young female police candidate filed a complaint with Spain's Supreme Court in 2017 after she was rejected from the force in the same year because she was only 4cm shorter of her height.

According to the requirements of Spanish police force, women who want to join the national police force must meet a minimum height requirement of 1.60 meters (5.2 feet). Meanwhile, males must be at least 1.65 meters (5.4 feet) tall. The court noted that the height requirement "constitutes indirect discrimination against women because the minimum height requirement (165 cm) is more loosen for men than for women. In Spain, the percentage of women who do not meet the threshold (160 cm) (25 %) is much higher than the percentage of men (3%) who do not meet the threshold (165 cm)." Therefore, the court ordered that if the plaintiff passed the exam, the police should employ her and pay her the same as other women who joined in 2017.

Spain's police force has now followed up and ordered to accept her application to exam.



## 日本引入視像報警

日本警察廳於九月公佈，將試行「影像通報 110 系統」。市民可以透過手機或平板，在報案時將現場的視像情況同步傳送到警局，讓警方到達現場前能夠對事件有更多的情報。

當 110 報案中心接獲報案後，接線警員會詢問報案人使用視像的意願。一經報案人同意，中心會透過通訊軟件傳送一次性的連結。報案人只需登錄並輸入接線警員傳遞的登錄密碼，即可登入該視像系統。

系統會將上傳的影像發送到正在趕往現場的警員，讓他們能夠事前掌握更多情報，有助於更迅速正確地對應案件。

是次計劃預計由 10 月 1 日起開始，試行六個月後在 2023 年 4 月 1 日正式公開運作。

## 110 VIDEO REPORTING SYSTEM IN JAPAN

Japan's National Police Agency announced in September that they will try out the "110 Video Reporting System". Citizens can simultaneously convey the video of the scene to the police station through their mobile phones or tablets when reporting a crime, so that the police can have more information on the incident before they arrive at the scene.

When the 110 report center receives a report, the operator will ask the reporter's willingness to use video reporting system. With the approval of the reporter, the operator will send a one-time link through the communication software. The reporter only needs to log in and enter the login password sent by the operator to log in to the video system.

The system will send the uploaded video to the police officers who are rushing to the scene, so that they can have more information in advance and help them deal with cases more quickly and correctly.

The project is expected to start on October 1, and will be officially launched on April 1, 2023 after a six-month trial.

## 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.ltcn.com.cn](http://www.ltcn.com.cn) [www.zjlitai.en.alibaba.com](http://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@ltcn.com.cn](mailto:lcyl@ltcn.com.cn)



## 局長家 500 米外的假警局

印度警方在比哈爾邦 (Bihar) 搗破一間由犯罪集團經營的假警局，拘捕 4 男 2 女，合共 6 人。涉案團伙在當地一家酒店裡經營一間「警局」長達八個月，而更令人震驚是該酒店距離真 · 警察局長的住所僅僅 500 米。

據媒體報導，犯罪集團在酒店內設立警察辦公室，並且設假投訴站向報案人收取費用，同時亦會收取費用並謊稱能夠協助他們獲取社會房屋或警察工作。與此同時，他們更向鄰近農村地區的市民支付約 500 盧比的日資以假裝是在站內工作的警察。

事實上，冒充警察或士兵的行騙事件在印度卻是十分常見的，人們普遍對穿制服的人感到恐懼和尊重，但設立假警察局會使騙局更上一層樓。一名真 · 警員甚至受訪稱「我們都曾聽過國內有假警察或假調查人員，但第一次聽見有假警局。」

而揭發今次騙案是源於有名真 · 警員在巡邏時發現兩名一男一女的可疑「警察」。他們身上所配戴的槍枝與隊內不同，因此騙案才得以瓦解。警方相信主腦仍然在逃，而被捕的六人中則稱自己是受害人，事件有待調查。

## BOGUS STATION 500M AWAY FROM THE CHIEF'S HOME

Indian police smashed a fake police station run by a gang in Bihar state, arresting four men and two women, a total of six people. The gang operated a "police station" in a local hotel for up to eight months, and what is even more shocking is that the hotel is only 500 meters away from the residence of the actual local police chief.

According to media reports, the gang had set up police offices in hotels and set up fake complaint stations to charge people who report, while also charging fees and falsely claiming to be able to assist them with social housing or jobs in the force. At the same time, they paid about 500 rupees to citizens in neighboring rural areas to pretend to be police officers working at the station.

In fact, incidents of fraud to be police officers or soldiers are very common in India, where there is widespread fear of and respect for those in uniform, but setting up a bogus police stations will take the scam up a level. A real police officer even said in an interview, "We've all heard of fake police officers or fake investigators in the country, but this is the first time we've heard of a fake police station."

The deception was revealed when a real police officer spotted two suspicious "police", a man and a woman, while on patrol. The guns they were wearing were different from those in the force, so the deception was broken down. Police believed the ringleader is still at large, while the six arrested said they were victims and the investigation is under way in the case.



▲文 / 樹大招風

## 六個你不知道的德國法律

▲插圖 Illustrations/ macrovector



旅遊，是現代人在生活上不可或缺的一環，更是辛勤工作、學習的重大推力之一。為了玩得盡興，人們一般都會預先「學習」任何關於當地住宿、美食、行程等資訊，務求規劃一個完美假期。未知國度的法律法規則是人們較少留意，而往往卻容易成為旅途上破壞回憶的邪惡種子。

德國，擁有豐富的山水美景、濃厚的歷史遺跡，以及聞名世界的啤酒之外，其背後更藏有鮮為外地人所知的法律法規。想福祿如意地踏上旅途，就讓我們細看其中的幾條，為下次的德國之旅做足功課！

提起德國這個國家，啤酒必然是大多數人第一時間聯想到的東西。然而，與大多數國家規定的合法飲酒年齡不同，在這個啤酒大國，低至十四歲的小孩，在監護人的陪同下，皆可飲用啤酒或葡萄酒；滿十六歲的小孩，即使沒有合法監護人的陪同下，仍然可以自行購買或飲用低於酒精濃度百分之一點二的啤酒或葡萄酒；而年滿十八歲則可購買或飲用任何類型的酒精飲品。

雖然合法飲酒年齡比起大多數國家較為放鬆，但對於醉駕的處罰仍然是非常嚴肅，甚至更為嚴謹。在德國，當你處於醉酒的狀態下使用單車，警務人員有權當場截停，並可處以禁止騎行單車、滑板等交通工具最高十五年之長。而該「醉駕」記錄亦會影響未來考取駕照，或當場註銷已有的駕駛執照。

有人會話：「飲酒時 uber，飲水時開車。」但謹記你飲水時，亦要照顧好自己的車輛有足夠汽油 / 電方可進入高速公路。否則，任何無正當原因（不包括無汽油）而在高速公路上停車是違反當地法律。當然，除了違規之外，在德國的高速公路停擺本身都是一件極度高危的行為，因為當地的高速公路是沒有限速的！

歐洲大部分的主要城市，包括德國的柏林、漢堡等，景點之間都是可步行的距離。因此，與其自駕遊，大多數旅客則會選擇以步行為主、公車為輔。而這個出行方式卻暗藏另一個容易觸法的種子，特別是外地人。在澳門，市民在橫過馬路時大多以路面實際情況去作判斷，而忽略交通指示燈的作用。而這個邏輯思維會導致你在德國面臨至少五歐元的罰款，甚至遭受當地人當場責罵的風險。在德國，任何人橫過馬路時應該按照交通指示燈的訊號行動。

作為旅客，入鄉要隨俗，入境要守法。自第二次世界大戰，德國當局禁止任何納粹式敬禮和其他與納粹有關的符號和信號。一經定罪最高可判處三年徒刑，但法院通常會處以罰款。2017年，兩名中國旅客在柏林帝國國會大廈大會場（Berlin's Reichstag）外以納粹式敬禮遭當局拘留，最後每人處以罰款 580 歐元。而另一名加拿大旅客亦同樣因拍照時觸法被拘留，最後以罰款告終。但幸運女神亦有休息的一刻。一名美國旅客在 2017 年在餐廳以納粹式敬禮後則遭路人毒打，當場被德國人「正法」。

出外旅遊除了擔心「食唔慣」，亦有一派人士擔心「訓唔慣」而自備枕頭被單。如果德國是你的其中一個目的地，我勸你「放下枕頭，立地就訓」。根據德國法律，枕頭被視為被動武器（passive weapon），這意味著它可能被用來對個人造成傷害，從而導致被控襲擊等違法行為。

其實，為自己提前規劃住宿行程只是務求玩得盡興，玩得安心。人生路不熟的情況下往往會增加不如意事情的發生，甚至會出現危及性命的時刻。趁機會多瞭解別人家的文情、法規，相信可以大大提升你的旅遊體驗，減低你的外遊風險，讓我們都能夠安心出行吧！



專家投稿 Contributions

## SIX GERMAN LAWS YOU SHOULD KNOW BEFORE ARRIVAL

▲ Author/ 樹大招風

Travel is an indispensable part of modern people's life, and it is also one of the major thrusts of hard work and study. In order to have a perfect vacation, people in general "study" information about local accommodation, food and itinerary in advance. The laws and regulations of foreign countries, however, are that people pay less attention to, and it is often easy to become the evil seed that destroys memories on the journey.

Germany, is well known with its rich landscapes, spectacular historical sites, and world-famous beer. Yet, its laws and regulations are rarely known to foreigners and tourists. If you want to enjoy your trip to Germany, let us take a closer look at a few of them for your next journey to there!

When it comes to Germany, beer must be the first thing comes to people's mind. However, unlike the legal drinking age set by most countries, in this beer country, children as young as fourteen can drink beer or wine when accompanied by a guardian; children over sixteen, even without a legal guardian accompanied, they still can buy or drink beer or wine with an alcohol concentration of less than 1.2%; at the age of 18, they can buy or drink any type of alcoholic beverages on their own.

While the legal drinking age is looser than in most countries, the penalties for drunk driving are very serious, or even stricter. In Germany, when you use a bicycle while intoxicated, police officers have the right to stop on the spot, and can impose a ban on bicycles, skateboards and other vehicles for up to 15 years. The "drunk driving" record will also affect the future driver's license, or cancel the existing driver's license on the spot.

Some people say: "Take Uber when you drink alcohol, drive when you drink water." While making sure yourself hydrated, you should also take care that your vehicle has enough gasoline/electricity before entering highway. Otherwise, it is a violation of local law to park on the highway for any reason (excluding running out of gas). Of course, in addition to violations, it is an extremely high-risk behavior to stop your car in highway because, in Germany, there is no speed limit on highways!

Most attractions in major cities in Europe, including Berlin and Hamburg, are within walking distance. Therefore, instead of traveling by car, travelers will either walk or take public transports. However, this may be another trap, especially for foreigners. In Macau, some people do not follow the traffic signal for their convenience while crossing the road, which can lead you to face a fine of at least five euros in Germany, and even the risk of being scolded by the locals on the spot. In Germany, anyone crossing the road should follow the signals of the traffic lights.

As a tourist, you must follow the customs, and obey the law in other country. Since World War II, German government has banned any Nazi salute and other Nazi-related symbols and signals. If convicted, the sentence can be up to three years in prison, but the court usually imposes a fine. In 2017, two Chinese tourists were detained by authorities for giving a Nazi salute outside Berlin's Reichstag, and were eventually fined 580 euros each. Another Canadian traveller was also detained for violation while taking photos, and ended up with a fine. Parcae also has her own day off. An American tourist was beaten by passers-by after giving a Nazi salute at a restaurant in 2017, which was "justified" by the local Germans on the spot.

Besides the food cultural shock, some people do not sleep well without their own pillow while traveling so they may bring their own pillows and sheets. If Germany is one of your destinations, I urge you to put the pillow back to your bed. Under German law, the pillow is considered as a passive weapon, which means it could be used to cause harm to an individual, leading to charges of assault and other offenses.

Planning for your trip in advance is to ensure your journey with ease in other country. Nobody wants to happen something accident which may destroy the mood mentally, or even harm the body and life physically upon the trip. I do hope that this article can inspire you to know the essence of studying law and regulation before arrival and I wish you have a nice trip!

Contributions 專家投稿



▲插圖 Illustrations/ pikisuperstar

## 言論自由和記者安全課程內容概論 I

根據聯合國於 1948 年通過的《世界人權宣言》第十九條，「人人有權享有主張和發表意見的自由；此項權利包括持有主張而不受干涉的自由，和通過任何媒介和不論國界尋求、接受和傳遞消息和思想的自由。」確立了言論自由在國際層面上的基礎定義。然而，這些國際文件並沒有任何法律約束力。因此，在某些地區和國家則會另設如憲章或公約含法律約束力的文件，以更進一步加強保障人民的言論自由。

每個人的言論自由權，包括記者，不僅只是接收，甚至有傳播訊息和意見的權利。因此，新聞和媒體自由亦是值得關注和保護的，並經常成為國家法律中的一項規範，如《德國憲法》第五條，「出版自由及廣播與電影之報導自由應得以保障。」以及《美國憲法》在第一修正案亦明顯規定，「國會不得制定關於剝奪言論自由或出版自由的法律。」等內容。然而，根據聯合國教科文組織的研究報告顯示，自 2016 年到 2021 年間，有超過四百名記者因工作關係或在執勤時慘遭殺害。而至今仍有九成的案件是並未結案，這亦表示世界上仍有數百名疑兇逍遙法外。

在這些悲劇下，國家必須積極支持包括新聞工作者在內的公民，確保他們能夠合法行使言論自由的權利，以及支持記者以安全的環境下展開工作，特別在示威或罷工期間。而作為執法工作者的警務人員，為了能確保新聞工作者和自身任務得到相互協調，首先我們要先瞭解記者的身份和合法權益。聯合國人權委員會會員 **Hélène Tigroudja** 在課上分享，該委員會對於新聞工作者是沒有任何定義，不過他們卻對於新聞工作提供一個更精準的定義，「新聞是廣泛的參與者共享的職務，包括專業的全職記者和分析師，以及網誌作者和作家，他們在互聯網或其他地方以印刷形式進行自我出版。」這意味著人權委員會確實採用了一種功能性定義和功能性方法來定義誰是記者以及新聞工作的定義。執行記者工作的人便擁有《公民權利和政治權利國際公約》第十九條的廣泛保護範圍。而更重要的是，當我們談論想要報導抗議活動或任何一個議題時，國家可能需要向記者提供「認證」（Accreditation），如參加活動、示威、遊行等的資格，但這一行為並不属于「授權」（Authorization）。換言之，對於人權事務委員會而言，國家強制實施這種認證程序是完全合法的，而不是授權程序來行使記者職能。

當一個被人權委員會理解為「記者」的人在活動中進行報導時，這個人當然需要獲得充分的保護。作為執法者的你對當事人的身份存有疑問時，如身上沒有配戴記者證件或服飾時，委員會則建議一種推定，即該人確實是博主或記者等新聞工作者。因此，在如此推定下，執法人員並不能把當事人與抗議者混淆，視為驅散等執法行動的目標。

▲內容節錄於 MOOC 第一章節。

## MOOC ON FREEDOM OF EXPRESSION AND SAFETY OF JOURNALISTS (I)

According to Article 19 of the Universal Declaration of Human Rights adopted by the United Nations in 1948, "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." established the fundamental definition of freedom of expression at the international level. However, these international documents are not legally binding. Therefore, in some regions and countries, legally binding documents such as charters or conventions will be set up to further strengthen the protection of people's freedom of speech.

Everyone's right to freedom of speech, including journalists, not only to receive, but even to disseminate information and opinions. Therefore, freedom of the press and the media is also worthy of attention and protection, and is often a norm in national law, as in Article 5 of the German Constitution, "Freedom of the press and freedom of reporting on broadcasting and film shall be guaranteed." and The U.S. Constitution also clearly states in the First Amendment that "Congress shall not make laws depriving freedom of speech or freedom of the press." However, according to a UNESCO study, more than 400 journalists have been killed between 2016 and 2021 due to their professions or while on duty. Ninety percent of the cases are still open, which means that hundreds of suspects are still at large around the world.

In the midst of these tragedies, states must actively support citizens, including journalists, to ensure that they can legally exercise their right to freedom of expression, and to support journalists working in a safe environment, especially during demonstrations or strikes. As law enforcement officers, in order to ensure that journalists



▲ Source/ MOOC

and their own tasks are coordinated with each other, we must first understand the identity and legitimate rights and interests of journalists. **Hélène Tigroudja**, a member of the United Nations Human Rights Council (UNHRC), shared in the class that the Council does not have any definition of journalists, but they provide a more precise definition of journalism, "Journalism is a job shared by a wide range of participants, including professional full-time Journalists and analysts, as well as bloggers and writers, who self-publish in print on the Internet or elsewhere." This means that the Human Rights Council has indeed adopted a functional definition and a functional approach to defining who is a journalist and who does journalism. Those who work as journalists enjoy the broad protection of article 19 of the International Covenant on Civil and Political Rights. And more importantly, when we talk about wanting to report on protests or any issue, the state may need to provide journalists with "accreditation", such as qualifications to participate in events, demonstrations, marches, etc., but this behavior does not belongs to "authorization". In other words, for the Human Rights Council, it is perfectly legal for the state to impose such a certification process, rather than a mandated process to exercise journalistic functions.

When a person, understood by the Human Rights Council as a "journalist", reports at an event, that person certainly needs to be adequately protected. When you, as a law enforcement officer, have doubts about the identity of the person concerned, such as not wearing a reporter's ID or uniform, the Council recommends a presumption that the person is indeed a journalist such as a blogger or reporter. Therefore, under such a presumption, law enforcement officers cannot mixed up the parties with the protesters as the target of law enforcement actions such as dispersal.

# 網路科技幽影之困擾（三）

▲文 / 艾迪 · 華警教授

▲譯 / 成振昊

▲插圖 / macrovector

## 人工智慧 (AI) 和機器學習 (ML) 中初顯的安全威脅

近年來，人工智慧（如圖像和語音辨識、智慧型機器人、語言任務和博弈等）取得了巨大的進步，人工智慧技術在不斷的發展和突破，朝著安全有益的方向探索。具有共同的全球利益、客觀目標、時刻關注並勇於挑戰的學者和決策者，通過研究和不斷合作處理短期和長期的技術安全帶來的影響，包括環境治理（如應對氣候變化，以及流行病應對）和生物風險。

人工智慧會發酵短期事件，如隱私、偏見、不平等、安全和保障等，從而影響了全球網路安全、數位化和核武器系統的威脅及發展趨勢。儘管人工智慧和機器人學習從方法策略角度影響了資料驅動型企業，然而安全問題始終是這些公司至關重要的環節。況且，在制定網路安全計畫時，常常需要做出及時調整，且花費巨大。但到了使用人工智慧和機器人學習的系統時，受威脅的規則有所更改。在即將到來的人工智慧時代，政府和行業仍沒有充分準備好控制和標準進行應對。

人工智慧 / 機器人學習的應用和結構變得更強大、更通用，和其他技術一樣有著類似的應用前景和阻礙。它們可能在許多領域已經優於人類本身 - 如果人工智慧 / 機器人學習替代了人類，它可能會在經濟、社會等方面帶來積極的轉變。但如同工業革命一樣，改革也有可能對現有網路行為造成威脅，可能為漏洞威脅、挑戰方面帶來新的場景及災難性

的威脅。在直接的軍事對抗下（如間諜活動、心理戰和政治戰爭以及金融工具），國家和非國家對手的遭遇戰進一步加劇，這些對抗利用了我們開放經濟社會的伴隨而來的脆弱點（如基礎設施和社會凝聚力）。

儘管，現有系統經常出現無法預料的錯誤，遇到大量的技術困難和問題，這與反復的設計以及不斷出現的錯誤有關，這會將敵對挑戰（被貼上破壞威脅的標籤）在全球範圍內擴大……進而擾亂勞動力市場、改變長期形成的角色，甚至影響政治主張——先進的人工智慧架構將會成為經濟的關鍵，也是政府資產，它將具有適應性，既能在微觀上更精準，宏觀上更快速……人工智慧也使得網路攻擊和數位假情報更多的被犯罪分子利用，以集中在個人的新模式極大地改變了數位安全的威脅——和 / 或創造轉基因生物製劑。

隨著人工智慧系統進一步融入現代社會，並成為不可或缺的部分，其受到的攻擊將更具有突發性和系統易感性，進而對國家安全產生重大隱患。在人工智慧和機器學習系統中，有一些關鍵部分需要的複雜資料量更高，在這些資料中，人工智慧可以學習 / 訓練和推斷加上其模型本身的後續演算法和程式，生成預測、結果和見解——因此，它的技術結構也將提高敵方資訊處理的規模、精度和持久性，這將以三種途徑加劇其破壞性：



### 信息

人工智慧可以生成基於文本的內容，並操縱圖像、音訊和視頻，包括通過生成對抗網路 (generative adversarial network, GAN) 及強化學習 (reinforcement learning, RL) 進行深度偽造，這對區分真實、合法的資訊造成極大阻礙。

### 受眾

人工智慧可以創造出有著個體特徵、輪廓和大體形象的個人（即生成假角色），假角色具有偏好、行為和信念等，與鑑定的特定受眾交互資訊。

### 媒介

人工智慧可以嵌入到平臺中，如通過位置演算法分類，以擴散破壞性資訊（控制和操縱數位資訊）。

在人工智慧 / 機器人學習系統擴展的進程中存在很大的模糊性、不適應性和分歧，與傳統網路攻擊中的“漏洞”或代碼中的人為錯誤不同，人工智慧攻擊是由底層演算法的固有限制導致的，目前還無法修復。社會趨向於人工智慧的安全性和建設性發展，以此為目標培養有領導力的研究人員、行業顧問，並從高校實驗室和科技公司中得到更多支持，包括推進先進的研究專案、基金，在機器人學習實驗室裡就國內和國際的戰略風險問題開展會議和討論。

### 網路攻擊及風險的加速出現

儘管以上只是人工智慧 / 機器人學習模型場景的一些演示範例，但在實際執行中，駭客可以在不同的單元上複製導致崩潰的程式，精準攻擊系統——大量的曲線和攻擊通過擴增成為可以進行網路攻擊的實體集合，再疊加每一步的機會軌跡，導致人工智慧 / 機器人學習在開發過程中，從錯誤的活動、有毒演算法和創建保密訓練資料集中學習如何干擾輸入，導致不可預見的損失。

惡意軟體在人工智慧時代能夠轉衍生成成千上萬的不同格式和方法，這些程式一旦載入到電腦系統上，比如多變的惡意軟體，超過 90% 的惡意可執行檔都是由此產生……深度強化學習演算法已經可以找到漏洞和隱藏的惡意軟體，並進行有針對性的攻擊。因此，人工智慧系統成為了一類新的攻擊目標，而在應對這類情況的前沿機構，如政府、商業公司和研究人員已經受到了如逃避、資料中毒、模型複製和利用傳統軟體缺陷開展的欺騙、操縱、損害等攻擊，並使人工智慧系統失效。

相比與傳統網路活動，與之相關但又不同的威脅是由於人工智慧系統的部署將很容易受到來自人工智慧強化領域的對抗性攻擊。公民社會、執法和 / 或軍事中的傳統的人工是否可以被人工智慧替代……另外，生物技術在科學創新的推動下，目前已經實現可程式設計，如基因編輯工具，它會引領一個新的時代，一個人類可以編輯 DNA、合併龐大的計算能力和人工智慧的時代。生物技術的創新可能會給最令人類文明困惑和無力解決的挑戰提供全新的解決方案，包括健康、食品生產和環境可持續性等，但與此同時，也會帶來極大的負面隱患。

## 人工智慧對公共安全和智慧社會的影響

目前，科學家和相關從業人員在監管、電腦犯罪、網路技術安全領域的合作已成為共識，為執法和數位社會中出現的突發事件和挑戰提供了全面的視角。人工智慧 (AI) 的出現，以及物聯網 (IoT) 設備的廣泛應用，通過推動文化變革形成多樣化產業，創造了相互關聯的智慧社會。隨著大資料應用的在複雜技術、個人監管的創新擴展成為一個全新的大資料應用流、容量中繼資料和平臺。這些都可以助力風險的防範，締造更安全的社區，但在公共安全和安保方面仍在惡意濫用的可能以及潛在的風險。

因此，網路罪犯（駭客）試圖成為電子人，人工智慧也不例外，他們的目標是在最短的時間內獲得更暴力的利潤，利用更多的受害者，創造多樣化的、創新的犯罪商業模式，加快和提高攻擊的成功，同時減少被逮捕的可能。因此，人工智慧維度具有更大的熟練度和自主性，充分展現了人性和技術的融合。政府對各種高科技工具的利用，可以通過已經部署和積極研究的自動化和增強來提高作戰效率，如目前的全息通訊、智慧城市 / 智慧社會、面部識別系統、影片監控和搜索技術支援影片和圖像分析調查，偵查罪犯臉部照片的特徵等，阻止進一步犯罪，逮捕網路罪犯等。

所以，科學應用同時帶來複雜的挑戰，用非常有限的人力資源對幾乎無限的內容進行分析過濾，尤其是新一代的人工智慧，可以實現工具和技術的更廣泛配合，提供有效的監管、預防犯罪，更早地發現重大犯罪的信號，在犯罪行為發生的早期快速逮捕罪犯，取得更好的結果。

隨著人工智慧在現代化進程中的廣泛應用，尤其在個人（模式識別）和軟體（演算法和電腦硬體）中，人工智慧將持續應用於刑事司法系統。這會導致其成為犯罪分子的攻擊目標。不像傳統的網路安全可被人工糾正並處理「漏洞」，以此阻止犯罪分子控制或操縱系統…相比之下，人工智慧的問題是由內部引起的，由此產生的人工智慧的攻擊，無法被「修復」或「修補」，它需要不同的工具和策略來保護核心演算法不被病毒感染。

研究暴露了各種各樣的問題，比如佩戴一副彩色眼鏡可以極大降低了人工智慧識別的準確性，或者通過染髮、語音、手語躲過執法檢測，總之，對目標的攻擊在持續升級。加密貨幣、帳戶劫持、資料盜竊或網路間諜以及恐怖主義等犯罪活動似乎都在持續增長，網路罪犯一直是對政府系統發起複雜攻擊的最新技術的早期採用者，人工智慧也不例外。他們利用其進行內外攻擊，「深度偽造」是目前作為人工智慧對內攻擊最出名的例子。

因此，政府希望通過人工智慧來擴展服務，比如在地方和國家政府網站上使用智慧「聊天機器人」來幫助民眾實現各種功能。執法機構仍然希望利用現有的資料來源輕鬆獲得資料，如利用手機、平板電腦、全球定位系統、無線通訊網路和其他如包含豐富資訊的接入點。從這些連接中產生的所有記錄都通過數位方式收集，執法機構可以更行之有效的進行分析並得出情報，推進複雜的調查工作。

我認為創新技術檢測將降低虛假資訊活動和敲詐勒索的風險，也同樣降低針對人工智慧資料集的嚴重威脅。分析就如何利用人工智慧來提供支持、降低這些威脅提出了建議，具體例子如下：

抓取文檔的惡意軟體可以更有效的開展攻擊。

勒索軟體攻擊，可以通過智慧目標進行逃避。

令人信任的社交軟體受大規模攻擊。

資料污染，在檢測規則中識別盲點。

逃避圖像識別和語音生物識別。



此外，針對安全的數位未來發展的更多的預測和參考如下：

利用人工智慧技術方面的前景作為打擊犯罪的工具，以抵禦未來的網路安全和治安監管。

全方位保護基礎設施，包括網路加密 [ 協定資訊圖 ]、代理、防火牆和網路責任保險等，預防和保護未來的網路安全攻擊。

通過不斷的研究、評估、訓練和實戰，促進防禦技術的改進和發展。

通過雲端、終端、電子郵件、物聯網和網路等途徑，增強的互聯、分享威脅的智慧解決方案，實現政府對企業和消費者的彈性管理，以獲得更好、更快的保護。

收集、交換和傳遞情報，以制定和實施精細化的流程，並深入瞭解人工智慧、機器人和相關技術，如預防犯罪、刑事司法、法治和新出現的安全威脅領域的綜合政策。

培育和發展安全的人工智慧設計和戰略架構。

立法上減少對使用人工智慧解決網路安全問題的過多限制。

撬動公私合作，建立真正的夥伴關係，成立多學科專家小組。

## 總結



毫無阻礙和不計後果的熱情讓世界吸取了許多痛苦的教訓，科學技術暴露出了被煽動和執行的嚴重漏洞。人工智慧在社會的這些關鍵方面所發揮的不受約束的創造力，將為今後帶來許多亟待解決的威脅。在這些威脅中，政策制定者、當局和關鍵行業必須出臺強制性的安全合規問題，並由適當的監管機構在最佳時間時強制執行，既要避免扼殺創新，又要在這個快速變化的領域中防範這些風險。

然而，在這一挑戰中，公眾面臨著關鍵基礎設施安全、實體及公共部門網路安全的雙重挑戰。缺乏對網路問題的預見性、無法持續追溯過去，都是最突出的問題。“威脅的停留時間”也在悄無聲息的對監管機構、政府機構和安全公司造成困擾。所以最終的問題是，他們做得是不是還不夠？

據網路專家統計，每天約有 100 萬次潛在的網路攻擊，隨著移動和雲技術的發展，這個數字還會增加。為了降低增長，政府、執法部門、行業和企業一直在努力拓展其網路安全團隊。然而，為了準確地識別潛在的駭客和 / 或攻擊，網路安全團隊應該明確誰是網路罪犯、他們使用什麼技術以及將可以採取哪些措施保護和預防未來出現的網路犯罪。

政府和社交媒體公司之間的配合仍然是臨時的。此外，政府需要投入更多的注意力和資源來應對檢測、歸因和媒體的身份驗證等方面。因此，由於犯罪模式、政策和技術正在隨著智慧社會不斷變化，各國和國際執法機構都需要制定面向未來的立法框架；(a) 重新審視預防犯罪；(b) 調查、決策做出預防性監管；(c) 防止或降低具有破壞性的網路攻擊，以及 (d) 確保安全執行，即：指揮、控制、通信和情報。

隨著這些人工智慧和機器學習科學工具的進化，人類文明的前沿技術可以實現對話交流。網路犯罪分子已經繞過了層層的網路安全控制和防禦，他們的成功之處在於採用各種不同程度的複雜方法或創新，從而在系統使用方面獲得優勢，而這些系統是可以模仿人類行為來執行特定的任務。因此，考慮到潛在的用途，網路犯罪分子會追求高投資及高回報，從而加速攻擊的數量，加強惡意服務，以保護匿名性，躲避執法機構，在這些地方，歸因和調查犯罪已經成為一大挑戰。

在世界範圍內，致力於確保安全和權益的超級智慧的社區正在蓬勃發展，但在先進的網路安全人工智慧系統的發展過程中，存在很大的不確定性和分歧。這種系統可能帶來好的結果，尤其在降低風險和威脅方面，也可能帶來更為複雜的負面影響——通過貫徹嚴格的安全意識，最終在安全問題、挑戰和解決方案上形成特有的管理流程，這需要全面、普遍的合作和以及對網路安全態勢的戰略的重視，以及持續的執行下去。

在國際警察協會亞洲事務總署中，我們延續了以價值觀教育這一傳統，在這裡通過有組織、有紀律及嚴謹的分析，創造有挑戰性、有意義的經驗。

## VICTIMS IN THE SHADOWY OF TECHNOLOGIES III

▲ Author/ Prof. Eddie Wazen, PhD.

▲ Illustrations/ macrovector



### THE EMERGENT SECURITY THREATS IN ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)



In recent years have seen dramatic progress, enhancements and breakthrough in artificial intelligence evolvement (e.g., image and speech recognition, autonomous robotics, language tasks, and game playing), and towards discoveries' for its safety and beneficial direction, research and collaborations, which as part of societal norm of technologists, academics and policy-makers with a shared global interest objectivities, attentions and challenges in shaping productive process, fostering scientific virtuosity and dimensions by addressing the near-term and long-term technical security implications and governance, including the environmental mitigation (such as, combating climate change, and pandemic response) and biological risks.

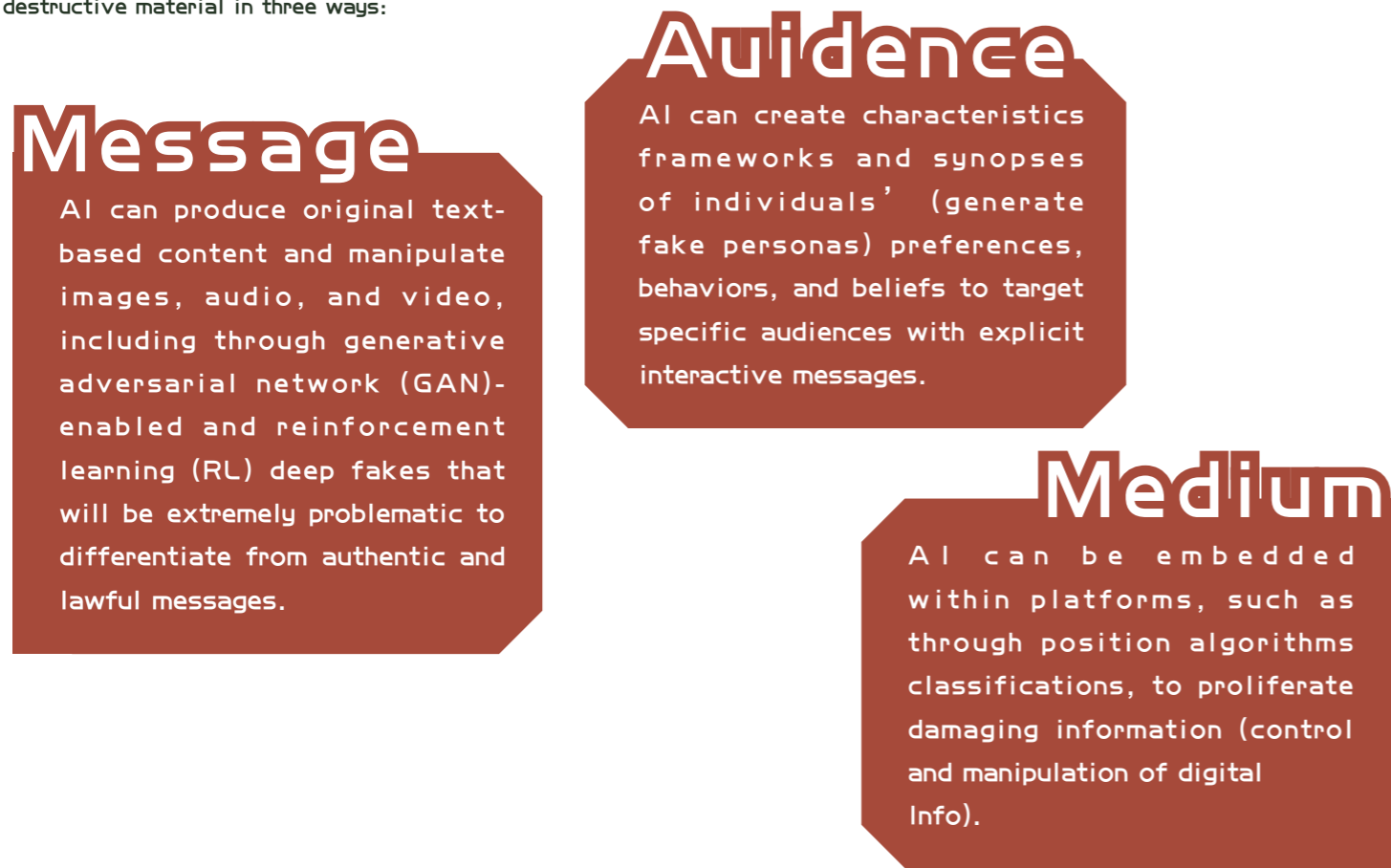
and misconfigurations as any other technologies, they may become superior to human performance in many domains - if this occurs, it could lead to extremely positive transition as transformative economically, socially, and politically as the Industrial Revolution, but could also altering existing cyber acts threats, potentially creating new liability scenarios classes of vulnerabilities threats challenges posing catastrophic dangers, and further emboldening state and non-state adversaries encounters underneath the edge of direct military confrontation (e.g. espionage, psychological and political warfare, and financial instruments), which exploit additional vulnerabilities in our open economical society (such as, critical infrastructure, and societal cohesion).

Hence, Artificial Intelligence elevates near-term apprehensive affairs illustrating as privacy affect, bias, inequality, safety and security, including emerging threats and trends in global cybersecurity encounters, digitization and nuclear weapons systems. Thus, Artificial Intelligence and Machine Learning (AI/ML) are methodically strategic technologies for all data driven businesses -- therefore securing it is essential to the corporate sectors involved and alike, and in developing a cybersecurity plan resiliency can often be timely and equally expensive...but when it comes to artificial intelligence and machine learning (AI/ML) systems, the threatening game changes, in which the governments and commercial segmentation still not fully prepared to defend its controlling adequacy and standards in the coming (AI) phase.

Hence, our existing systems often go wrong in unpredictable methods, numerous technical difficulties and problems, related designs setbacks, and multitudinous accident negative functioning outcomes, in which will extend a wider-range and reach of antagonistic challenges (labeled as sabotage threats) globally... It will disrupt the labor market, changing the nature of long-established roles, and could be used to influence political thinking and opinion - an advanced AI structure could be key economic and governmental assets that will be adaptable suitability to act with micro-precision, but at macro-scale with a grander rapidity...also, the AI enhancements of cyber attacks and digital disinformation campaigns in the hands of malicious actors utilization in harmful criminalities will dramatically alter the digital security threat landscape that target and centered upon individuals in new modes - and/or the creation of engineered biological agents.

AI/ML applications and structures become more powerful and more general that grips similar prospects for utilization

As artificial intelligence systems are further integrated into critical components of society, these AI attacks characterize an emergent and methodical susceptibility with the probabilities to have significant consequences and impact on the security of the nation. There are critical assets in artificial intelligence and machine learning systems that require higher volumes of complex data, in which can learn/train and extrapolate its predictions, results and insights, including its model itself follow-on algorithm arrangement and formulation - therefore, its technological structure will escalate the magnitude level, precision, and persistence of adversarial information processes that exacerbates critical challenges of destructive material in three ways:



There is great ambiguity, inaptness and divergence over timelines for the expansion of advanced AI/ML systems, and unlike traditional cyberattacks that are caused by “bugs” or human mistakes in code, AI attacks are enabled by inherent limitations in the underlying AI algorithms that currently cannot be fixed, and the community working towards its safety and constructive superintelligence, in which has cultivated leadership from researchers, high-profile support from industries advisors, universities labs and in tech companies, including advanced research projects, funds, extensive discussions and conferences in machine learning labs about strategic risks issues nationally and internationally.

**Accelerated Cyber Attacks and Risks**  
While these are just a few illustrative paradigms on what actually an emerging space with AI/ML model scenario, but in numerous methods and conducts hackers could replicate crash programming on various units, which can target the systems - there are plentiful curve and multitude of fundamental attack in expanding the set of entities that can be used to execute cyberattacks, plus

the opportunities trajectories for at every step, which can lead to the exploitation of AI/ML process from erroneous activities, poisoning algorithm and creating inferences about confidential training dataset to learning model how to perturb an input, in which leads to an unforeseen accumulation of losses.

Malware in the AI era will be able to transmute into thousands of dissimilar format and methods once it is lodged on a computer system, such mutating polymorphic malware, in which accountable for more than ninety percent (90%) of malicious executable files... Deep RL tools can already find vulnerabilities, conceal malware, and attack selectively - thus, the AI systems represent a new target for attack, and while on this phenomenon edge frontage, governmental agencies, commercial firms and researchers have already documented attacks that involve evasion, data poisoning, model replication, and exploiting traditional software flaws to deceive, manipulate, compromise, and render AI systems ineffective.

However, the comparative threats related to, but distinctive

from, conventional cyber activities, because AI systems arrangements will be vulnerable to adversarial attacks from whichever domain where AI intensified augmentation action — whether traditionally human-based tasks being replaced by AI, civil society, law enforcement and/or military... also, Biotechnology in which is now programmable with scientific innovations, such as the gene editing tool that ushered in an era where humans are able to edit DNA, coalesced with immense and gigantic computing power and AI. The Biotechnology creativities might offer and provide novel solutions for civilizations most puzzling and ineptitude challenges, including in health, food production, and environmental sustainability, but at the same token, can enhance a dark side excessively.

**The Impact of Artificial Intelligence on Public Safety, Security and Smart Societies**

It is current understandable that collaborative between scientists and practitioners in the fields of policing and cyber criminology, IT law and security, providing a comprehensive insights on the existing emergent encounters and challenges in law enforcement and digital society, in which the advent of Artificial Intelligence (AI) jointly with the wider-spread of Internet of Things (IoT) devices creating interrelated smart societies’ by driving the cultural change toward diverse Industries. The scope of connectivities, immense upsurge in the capacity of nifty devices and rising interfaces amid the increased sophisticated technologies, individuals and policing with the innovative expansion of an entirely new streams Big Data applications, volumetric metadata and platforms that could support preventive measures to bring about a safer community, but there are possibilities as well as potential risks for malicious abuse in the context of public safety and security too.

Therefore, cyber-offenders (hackers) try to become cyborgs, and AI is no exception, in which expedite and improve the success of their attacks by extending opportunities for revenue within a shorter period, exploiting more victims and creating diverse, innovative criminal business models - whilst lessening probabilities of being caught. Hence, AI dimensions promises greater adeptness and autonomy that exhibits augmented humanity and technology fusions, and governments’ utilization of the various sets of high-tech tools, which can enhance operational effectiveness through automation and augmentation in which already been deployed and actively researched with current holographic communications, smart cities / smart societies, facial recognition system, video surveillance and search technologies that supports investigation in video and image analysis, detecting characteristics of criminal mug-shots, deterring further delinquencies and apprehending cybercriminals, etc.

Thus, the scientific applications posing complex challenges of analyzing a virtually infinite amount of content filtering with a very finite amount of human resources, especially the new generation of AI-enabled tools as necessary to keep pace with the expansion of the technological purview in providing an efficient policing and preventative crimes by uncovering felonious warning signs, illegality earlier and apprehending offenders faster and obtain better results.

The modernistic of Artificial intelligence become more widespread and will be a permanent part of the criminal justice system through its usage, in particular individuals (pattern recognition) and capability in software (algorithms and computer hardware), which eventually and naturally becomes an attack targets for criminals -- unlike traditional cybersecurity vulnerabilities deals with errors “bugs” can be identified and rectified and by educating users in order to stop adversaries from gaining control or manipulating systems...in contrast, the problems is more intrinsic that creates an AI attacks, which cannot be “fixed” or “patched,” it requires different set of tools and strategies to protect against core algorithmic susceptibilities.

Research statistics exposed diverse cases (such as, sporting a multi-colored pair of glasses), in which has the capacity to attack AI-based facial recognition systems, critically degrading its accurateness...and/or inspired strategies of individuals dyeing one’ s hair to avoid law enforcement detection, and or speech and language translation -- also, advance attack targets continues to intensify. Crypto-currency, account hijacking, data theft, or cyber espionage and terrorism are all areas where criminal activity appears to be on the rise, and cybercriminals have always been early adopters of the latest technology at launching sophisticated attacks on government systems, and AI is no different... in which will leverage on AI both as an attack vector and an attack surface... ‘deep fakes’ are currently the best-known use of AI as attack vector.

Hence, the government looking to AI to expand its service industries - such as using intelligent “chat bots” on local and national government websites to assist citizens with various functions. Law enforcement agencies are still able to obtain advantages of the several sources of data available on hand, such as cell phones, tablets, GPS, wireless communication networks and other access points that contain a wealth of information, and all the fact records emanating from these connections can be digitally collected, forensically analyzed and turned into identifiable patterns for an actionable intelligence faster than ever before that can profoundly impact on very complex investigations.

I advised that innovative technology inspections will be compulsory vital outlook to mitigate the risk of disinformation campaigns and extortion, as well as felonious threats that target AI datasets – the evaluations exhibits recommendation on how AI could be used to support and diminish these probabilities, per example:

Documenting-scraping malware in creating the attacks more efficient.

Ransomware attacks, through intelligent targeting and evasion.

Convincing social engineering attacks at scale.

Data pollution, by identifying blind spots in detection rules.

Evasion of image recognition and voice biometrics.

In addition, further diverse projected indication and references toward safer digital future and countermeasures as follow:

Harnessing the prospective of AI technological aspects as a crime-fighting tool to future-proof the cybersecurity industry and policing.

Preventing and protecting against future cybersecurity attacks, by heightening all-inclusive methodology to safeguard infrastructure, incorporating countermeasures such as network encryption [protocols info-graphic], proxies, firewalls, and cyber liability insurance.

The continuation of research, assessments, training and field activities to incite improvement and growth of defensive technologies.

Enabling government's resiliency to businesses, and consumers with advanced connectivities and shared threat intelligence solutions across cloud workloads, endpoints, email, IIoT, and networks for better, faster protection.

Collecting, exchanging and disseminating of intelligence to the formulation and implementation of refined processes and understanding of artificial intelligence, robotics and related technologies, including integrative policies in the field of crime prevention, criminal justice, rule of law and emerging security threats.

Fostering and developing secure AI designs and strategic frameworks.

De-escalating legislative doctrine laden rhetoric on the usage of AI for cybersecurity resolves.

Leveraging public-private genuine partnerships and establishing multidisciplinary specialist groups.

## CONCLUSION

The world has absorbed numerous issues of painful lessons from the unencumbered and reckless enthusiasm with which technologies unveiled severe vulnerabilities that have been instigated and executed, and the unfettered creativities build of artificial intelligence into these critical aspects of society is weaving a fabric of immediate and future threats, in which policymakers, authorities and critical industry must address mandatory security compliances and enforced by the appropriate regulatory bodies in setting best practices in order to not stifle innovation, and to protect against these risks in this rapidly changing field.

However, there are commonalities in the challenges facing both critical infrastructures security, entities and public sector enterprises cybersecurity, which the lack of network visibility and inability to continuously review that history stands-out as the most prominent, and the “threat dwell time” is silently haunting today's policing, governmental agencies and security corporations. So the only question left to be asked is, are they doing enough?

According to cyber experts, approximately 1 million potential cyber attacks are attempted per day, and with the evolution of mobile and cloud technologies, this number is likely to increase. To help mitigate this growth, governments, law enforcement divisions, industries and corporations have been expanding their cybersecurity teams and efforts. Yet, in order to accurately identify potential hackers and/or attacks, cybersecurity teams should possess a firm understanding of whom cyber criminals are, what techniques they use and what counter-initiatives can be implemented in order to protect and prevent future cybercrimes.

The coordination between the government and the social media firms remains ad hoc – and moreover, the government needs to devote greater attention and resources to the technical challenges of detection, attribution, and media authentication. Hence, As the patterns of crime, policy and technology are changing in line with smart societies, law enforcement agencies

nationally and internationally are called upon to formulate future-ready legislative frameworks; (a) rethink crime prevention; (b) investigatory decision making and predictive policing; (c) prevent or mitigate potentially devastating cyber-attacks, and (d) ensure the security of operational capabilities, namely: Command, Control, Communications and Intelligence.

As intelligent as these AI and machine-learning scientific tools evolvment, civilizations are at the very forefront of the technologies enabled conversation, cybercriminals had bypassed layers of cybersecurity controls and defenses and their success are adept at adopting whichever variable degrees of sophistication methods or innovations that gives an edge over systems usage, which modeled on human behavior to execute specific tasks. Thus, given its potential uses, cybercriminals venture efforts in pursuing prospects that carry the expectation of highest return on investment, accelerate the volume of attacks, and the enhancement of malicious services to preserve anonymity and remoteness from law enforcement agencies where attributing and investigating crimes is already challenging.

The community working towards the safety and beneficial superintelligence that has grown worldwide, but there is great uncertainty and disagreement over timelines for the development of advanced cybersecurity AI systems that could be transformative with negative complexities as well as positive consequences, especially the reaction of mitigating risk and threat landscape -- and by implementing a heavy-handed security culture that ultimately achieving the unique governance processes into the safety implications, challenges and solutions, in which requires comprehensive universal cooperative and evocative strategies of cybersecurity posture, and perfection continuity.

At the International Police Association Asian Affairs Bureau, we extend a tradition of values-based education, where structured, disciplined, and rigorous analyses creates a challenging and rewarding experience.





# IPA

INTERNATIONAL POLICE ASSOCIATION  
VALLÉS OCCIDENTAL **BARCELONA**

## SUPER RUTA IPA

DE LOS MAYORES

**IMPERIOS Y CIVILIZACIONES DE LA ANTIGÜEDAD**

Del 9 al 23 Marzo 2023

# EGIPTO – GRECIA – ROMA



3rd edition

# TOUR OF GAMBIA

SOLIDARITY & ADVENTURE  
CYCLING ROUTE

[www.tourdegambia.com](http://www.tourdegambia.com)



From November 12th to 19th, 2022

25 bicycles, 25 riders, a route, an adventure, a direct charity action, a personal challenge, Africa the continent, Gambia the country and one event where everything is included, THE TOUR OF GAMBIA  
Probably it can be one of the most impressive adventures and personal experiences of your life..... and riding a bicycle !!

Are you really going to miss it ?

SUPPORTERS





# IPA

INTERNATIONAL POLICE ASSOCIATION  
VALLÉS OCCIDENTAL **BARCELONA**

## IPA Romantic Week

*St Valentine's* event  
February 14th/22nd 2023



### BARCELONA +

### VENICE CARNIVAL EXPERIENCE



## 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 九月版 / Sept 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 € (incl. consumables)
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 € (inkl. Verbrauchsmaterial)	22 30	Social Media Master Kurs	22.08. – 26.08.	890 €
22 08	Tactical First Aid 	24.02. – 25.02.	490 €   IPA 360 € (incl. consumables)	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 – Aufbauseminar	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 € (inkl. Verbrauchsmaterial)				