

## 大數據對反恐工作至關重要

國際恐怖主義是困擾和威脅當今世界和平與發展的重大難題。時至今日，面對世界範圍內暴恐案件此伏彼起的頻發趨勢，可以說，沒有任何國家和地區能夠完全置身事外。因而各國各地區都高度重視對恐怖主義犯罪活動的法律治理和綜合防控。

在對恐怖主義犯罪活動的防控對策中，世界各國各地區一項重要的舉措和成功的經驗，就是借助警務大數據應用的研究成果，積極而有效地預防和懲治恐怖主義犯罪活動。



何謂大數據？美國 IBM 公司提出大數據應具有 5V 特徵：Volume（大量）、Velocity（高速）、Variety（多樣）、Value（低價值密度）、Veracity（真實性）。大數據的價值在於，通過對海量數據的高速規整、分析以盡可能地準確預測出接下來相關事物的發展趨勢或找出特定的規律。

從各國各地區的相關研究及實務經驗來看，可以運用大數據及相關計算技術，從以下幾個方面有效地預防及遏制恐怖主義：

首先，最為重要的，是在恐怖活動發生前，可以基於海量的數據之整理與分析，建立一套行之有效的預警措施。這一措施美國政府早在“9•11”事件發生之後就已開始施行，他們通過多種數據流程挖掘及涉恐風險特徵

提取這兩個步驟最終得到一套積分預警系統。所謂多種數據流程挖掘方法，實際上是把大量涉恐人員及恐怖襲擊事件的資訊進行拆分、歸類。這種收集並不局限於本國家或本地區，而完全可以借鑒其他國家和地區的已有數據，特別是聯合國安理會及其下屬反恐機構所公開的以及提供給會員國的資料。緊接著是涉恐風險特徵提取，實際上是將多種數據流程挖掘所規整出來的涉恐人員以及恐襲事件的各種數據再進行篩選，僅留下與恐怖主義相關的部分。最終這些通過檢驗的特徵會被納入積分預警系統。一旦某人或某一特定環境超過一定的積分閾值，則會成為重點關注對象。



其次，大數據在應對突發恐怖襲擊中也可以起到巨大作用。“9•11”事件之後，雖然歐美恐怖襲擊事件仍然頻發，但大規模的襲擊再也沒有發生，同類型恐怖襲擊的平均傷亡人數也在逐漸下降。這一方面歸功於預警機制的建立和各國警方應對恐怖襲擊經驗的積累，另一方面也是大數據分析應用於反恐工作的功勞。通過對大數據演算，人工智慧可以模擬恐怖分子的行為模式，並可以通過後續獲取的資料不斷修正。如此一來，即便沒有事前阻止恐怖襲擊的發生，警方也可以通過大數據分析結論進行戰略部署，以儘早阻止恐怖活動的蔓延，並將損害降至最低。據報導，美國馬里蘭大學所開發的全球恐怖主義資料庫涵蓋了全球超過 17 萬起恐怖襲擊的案例資料，美國警方利用人工智慧對資料庫所做出的分析，已經對近幾

年應對恐怖活動犯罪起到了顯著的作用。



再次，利用大數據也便於警方在事後快速找到恐怖分子，搗毀恐怖組織。防患於未然是最好的，但實際上警方不可能事先阻止所有的恐怖活動犯罪，因此事後追捕與緝拿恐怖分子、搗毀恐怖組織也是反恐工作中的重要一環。近年來，隨著基於大數據的音頻分析及人臉識別等技術的發展和有效應用於涉恐案件，恐怖分子無處遁形。最著名的莫過於“基地”組織頭目本·拉登的追捕過程，其中美國人工智慧公司帕蘭提爾開發的“帕蘭提爾科技”（Palantir Technologies）發揮了巨大作用。而這一技術的實質也是基於人工智慧對大數據所做出的分析。



最後，大數據在遏制網路恐怖主義方面同樣發揮著巨大作用。據報導，

利用 Twitter、Facebook、YouTube、Instagram 等社交媒體在網絡上招募潛在恐怖行為支持者，已經成為“伊斯蘭國”（ISIS）等極端恐怖組織影響力擴張的重要途徑。針對這一嚴峻的反恐形勢，這些社交媒體公司已經著手共建歐盟互聯網論壇和共用行業資料庫，利用大數據內容檢測和分類技術，確定恐怖主義相關內容並加以刪除。借助新的大數據分析演算技術，僅 2017 年上半年，Twitter 就刪減了近 30 萬個恐怖分子的帳戶，清除效率提升了約 20%；Facebook 則刪除了 99% 的基地組織和“伊斯蘭國”的材料。



由於大數據龐大的承載量，以其為對象進行高速分析和演算，可以得出比傳統抽樣計算精確得多的結果，這在反恐工作中意義重大，有助於提高反恐工作的準確性和效率，從而兼顧到維護人權和防治恐怖犯罪的需要。