澳门网络安全风险管理与应对机制探讨

■ 陈思晶　酆　达

摘　要　关键基础设施关乎社会利益及社会正常运作，面对难以洞察、攻击范围蔓延至诸多行业领域的网络攻击，澳门特区政府构建和完善网络安全风险管理与应对机制、提升网络安全防范能力和应急处置能力，其必要性和重要性日益突显。本文从澳门网络安全生态出发，从立法、组织架构、技术支撑和执法等多个层面深入探讨澳门的网络安全风险管理与应对机制，旨在针对持续维护澳门网络安全环境所面临的困难提出有针对性的对策建议，并藉此倡议海峡两岸和港澳地区共同构建互助互惠的网络安全合作机制。

关键词　网络安全　网络安全风险　澳门《网络安全法》　应对机制

一、前言

当今时代，随着网络信息技术的不断创新，互联网对整个经济社会发展的融合、渗透、驱动作用日益加深，极大地改变和影响人们的社会活动、学习、生活及工作方式，尤其是在2020年新冠肺炎疫情防控期间，网上电商零售、网络视频会议、网络在线教育等众多网络应用以前所未有的速度和规模呈现在社会公众面前，并在抗击新冠肺炎疫情、保障物资供应、助力复工复产等方面发挥了重要作用。

与此同时，伴随而来的网络安全威胁和风险也在日益增加，并加速向社会安全和国家安全各个领域传导渗透，各类网络攻击和入侵、网络窃密、网络诈骗等事件在全球各地频发。网络安全关乎国家安全体系的方方面面，如果网络安全出了问题，国家安全就没有保障。网络安全已经成为事关国家和地区安全、社会经济发展、保障广大市民日常生活和合法权益的重大战略问题。故此，构建和完善网络安全风险管理与应对机制、提高对网络安全风险的防御能力和应急响应效率，其必要性和重要性日益突显。

作者：陈思晶，澳门司法警察局信息及电讯协调厅厅长；酆达，澳门司法警察局一等高级技术员

本文为第十五届海峡两岸暨香港、澳门警学研讨论文。

本文从澳门网络安全生态出发，从立法、组织架构、技术支撑和执法等多个层面深入探讨澳门的网络安全风险管理与应对机制，旨在针对持续维护澳门网络安全环境所面临的困难提出有针对性的对策建议，并藉此倡议海峡两岸和港澳地区共同构建互助互惠的网络安全合作机制。

二、澳门网络环境概述

（一）澳门网络发展现状

根据澳门互联网研究学会 2020 年 6 月出版的《2020 澳门居民互联网使用趋势报告》，澳门居民的上网率从 2001 年的 33%，持续上升至 2020 年的 91%，在亚洲处于靠前位置，上网率高于全球平均（59%），也高于香港特别行政区（89%），与上网率一直在亚洲领先的韩国（96%）、日本（94%）逐渐靠近；2020 年居民的手机拥有率为 94%，使用手机上网的比率也连续五年达到 89%，较 2012 年（46%）上升了 43 个百分点。

在网络普及的进程中，澳门特区政府一直重视电子政务建设，于 2015 年 10 月发布《2015 年 -2019 年澳门特区电子政务整体规划》，不断从制度和基础建设着手，积极推进电子政务发展。目前已有二百多项对外公共服务实现不同程度的电子化，约五十个部门提供下载超过一千种电子表格；针对手机移动上网的普及化，特区政府推出了各类型手机应用程序，例如新闻局的“澳门政府新闻”、澳门基金会的“虚拟图书馆”、市政署的“漫步澳门街”、旅游局的“旅游信息交换平台”及“智能客流应用”等。随着电子政务的推广，澳门成年网民电子政务的使用率也呈现出逐年上升的趋势，2020 年达到 65%。此外，为进一步加强推动电子政务建设，特区政府于 2020 年 3 月颁布第 2/2020 号法律《电子政务》，该法对政府部门以电子方式作出的行为和手续作出规范并赋予相应的法律效力，为提供更多便民便商的电子化服务创设有利条件。

同时，特区政府亦一直主张透过善用信息科技和新兴技术来提升城市的综合管理水平，提供更高效和更便民的公共服务，早在《澳门特别行政区五年发展规划（2016-2020 年）》文本中就提出了“加快智慧城市建设，推动产业与互联网融合”的发展方针，并于 2018 年 5 月 17 日至 6 月 30 日期间完成了对《澳门智慧城市发展策略及重点领域建设》为期 45 天的公开咨询并发表总结报告，为智慧城市的建设制定了方向与目标。目前，澳门智慧城市建设已取得一些喜人成果，例如停车无感支付、医院网上挂号、大部分商户接受手机电子支付、旅客可实时查看各热门景点的人流情况等。

（二）澳门面临的网络安全风险与威胁

在全球网络安全威胁和风险日益突出的背景下，澳门作为一个国际城市，亦无法独善其身。如前文所述，目前澳门政府正积极推进电子政务和智慧城市建设，整个社会运行对网络的依赖程度越来越高，相应地所面对的网络安全风险也进一步加剧。每年澳门都有一些网络攻击事件发生，仅 2020 年上半年，就已发生多起针对澳门关键基础设施的网络攻击和入侵。在全澳市民共抗“疫情”的艰难时刻，黑客乘人之危于 2020 年 1 月 28 日白天繁忙时段对卫生局“网上健康申报”及“保障口罩供应澳门居民计划”系统发动分布式阻断服务（DDoS）攻击，导致相关服务一度中断，直接影响了全澳口罩等医疗物资的调配发放，以及出入境口岸的实时健康监察，对市民生活造成严

重干扰。此外还有涉及经济、教育、交通、社会民生等多个重要部门和机构的系统遭到网络攻击，虽没有造成严重后果，但与过往对比，明显看出2020年的网络攻击越趋频密，攻击手法也更为激烈和多样。

另外，澳门历年相关案件统计数据也反映出澳门目前网络安全形势不容乐观、面临风险日趋严峻的态势。从澳门2016至2019连续四年的信息罪案年度统计数据和变化趋势可以看出，2016年至2019年澳门治安保持稳定良好，四年的整体犯罪活动案件数大致相仿，但相较于2016年度和2017年度，2018年度和2019年度信息罪案有了一个台阶式跃升，案件数由约五百五十件增多到八百余件，增加约46%。在整体犯罪活动案件数基本没变的情况下，信息罪案占整体犯罪活动百分比也由3.8%增加到5.6%，上升了1.8个百分点。

综上所述，澳门的网络安全形势日益严峻，关键基础设施面临风险倍增，已成为澳门可持续发展、居民安居乐业的潜在不稳定因素之一。为此，特区政府于近年投入了大量资源与精力，从完善网络安全保护方面的法律法规入手，积极构建良好的网络安全风险管理与应对机制，以达到有效治理澳门的网络环境，不断提升预防和应对网络风险能力的目的。

三、立法层面的网络安全管理与应对机制

古人曰：“小智治事，中智用人，大智立法。”坚持立法先行才能保障政府重大行为于法有据。基于此原则，为了适应网络安全工作的新形势、新需求，特区政府先后出台了两部与网络安全保护密切相关的法律——《打击计算机犯罪法》和《网络安全法》。

（一）《打击计算机犯罪法》及其修订

随着计算机及互联网的使用越来越普遍，越来越多不法分子利用便利的信息科技作为犯罪的新平台。计算机犯罪的类型多样化，且具有广泛性、开放性、智慧性、隐匿性、迅速性及侦查难等特点，传统的打击犯罪方法面对在互联网上所实施的虚拟行为时往往显得束手无策。针对这些滥用信息科技的不法行为，早在2009年，特区政府就已经颁布了第11/2009号法律《打击计算机犯罪法》。该法针对多种损害计算机系统和数据的犯罪进行定罪及处罚，配合《刑法典》中的有关规定，为澳门有效打击涉及计算机及网络犯罪提供了重要的法律保障。其内容主要包括以下两大方面：

1．在刑事责任方面，将不当进入计算机系统、不当获取、使用或提供计算机数据、不当截取计算机数据、损害计算机数据、干扰计算机系统、用作实施犯罪的计算机装置或计算机数据、计算机伪造以及计算机诈骗等八大行为定为犯罪，并规定了实施该等犯罪的相关刑事责任。

2．在刑事诉讼规定方面，赋予具职权当局在打击计算机犯罪时更有效的调查手段，包括明确规定计算机系统、计算机数据存储载体、计算机数据或计算机程序可作为证据，并对执法人员在电子载体中搜集及保存电子证据的措施及行为作出规范。

因应近年新出现的计算机及网络犯罪手法，为更好地满足执法需要，并与《网络安全法》相配合，在保安司的领导下，2020年司法警察局在总结过往执法经验的基础上，对《打击计算机犯罪法》进行了修订完善。第4/2020号法律《修改第11/2009

号法律〈打击计算机犯罪法〉》已于 2020 年 7 月 1 日起正式生效。是次主要包括将困扰澳门市民多年的伪基站独立成罪、加强对关键基础设施营运者和其他重要实体计算机系统的刑法保障、法官可批准执法机关提取澳门以外的计算机数据副本作为电子证据，以及将违反职业保密、不正当揭露计算机安全严重漏洞的行为独立成罪等四个方面，让司法当局和执法机关拥有更完善及更具针对性的法律工具，提升预防和打击网络和计算机犯罪的成效，更好地保障广大市民的合法权益和整个社会的长治久安。

（二）《网络安全法》及配套的行政法规

随着全球网络安全威胁日益严峻，为确保涉及社会正常运作、经济发展等重要信息网络运作畅顺，以及保护计算机数据的保密性、完整性及可用性，有必要在原有着重于“事后侦查打击”的法制基础上，进一步制定专门规范网络安全行政管理的法律制度，构建属于澳门的网络安全防护体系，更好地维护澳门的网络安全环境，为电子政务及智慧城市的建设与发展保驾护航。

为此，特区政府自 2015 年起遵从“保障市民安全，尊重个人隐私”、“适度立法”及“架构设置精简有效”三大原则构思，开展《网络安全法》的立法工作。先后经历研究草拟、公开咨询、立法会讨论和审议等多个阶段，《网络安全法》于 2019 年 6 月 6 日获得立法会细则性通过，并于同年 12 月 22 日起正式生效，为澳门的网络安全工作提供切实法律保障。

《网络安全法》保护标的是澳门关键基础设施营运者的信息网络、计算机系统及计算机数据。所谓“关键基础设施”是指对社会利益及社会正常运作具有重大意义的资产、计算机系统及信息网络，一旦有关的网络及系统遭到扰乱、破坏、数据泄漏、停止运作或效能大幅降低，就会直接危害公共安全及秩序，以及广大市民的福祉，无可避免地将对社会正常运行造成严重冲击。

《网络安全法》订定了特区政府网络安全管理体系的组织架构，设立网络安全委员会（下称委员会）、网络安全事故预警及应急中心（下称预警及应急中心）和各领域的网络安全监管实体（下称监管实体），并赋予其相应职责。此外，明确了关键基础设施营运者（下称营运者）须履行的网络安全义务，以及订明对违反网络安全义务之机构与人员进行处罚的罚则及程序。另外，为更有效打击透过互联网实施的犯罪，要求网络营运商对预付式电话卡实施实名制以及保存及依法提供网络 IP 地址的转换记录等措施。作为一部框架性法律，《网络安全法》的有效实施仍需要配套的行政法规予以保障。与《网络安全法》同日生效的第 35/2019 号行政法规《网络安全委员会、网络安全事故预警及应急中心及网络安全监管实体》对委员会及预警及应急中心的组成、职权及运作方式等进行了补充性规范，并指定了不同行业领域私人营运者的监管实体。

《网络安全法》及其配套的行政法规共同构建及规范澳门的网络安全体系，确保关键基础设施的网络、系统及数据得到适切保护以维护其良好运作，并持续强化本澳营运者的网络安全防护能力，有效降低其遭受网络攻击的风险。此外，《网络安全法》与《打击计算机犯罪法》相互配合、优势互补，共同形成事前预防和事后打击相结合的工作模式，达至更有效预防和打击网络及计算机犯罪，更好保障澳门社会以至国家安全及利益的总体目的。

（三）司法警察局增设网络安全专职部门

《网络安全法》赋予司法警察局统筹预警及应急中心运作的职责，为该法的有效实施，更有效应对与网络安全有关的犯罪，目前特区政府已完成对第 5/2006 号法律《司法警察局》进行修订，连同据该法修订的《司法警察局的组织及运作》行政法规一同于 2020 年 10 月 12 日生效，进一步明确该局关于维护网络安全及打击计算机犯罪方面的权限，并增设网络安全专职部门，负责执行法律赋予预警及应急中心以及司法警察局关于维护网络安全方面的职责，包括检视营运者的网络安全态势、发出预警信息、协调事故应急等各方面。

四、组织层面的网络安全管理与应对机制

《网络安全法》及其配套行政法规的生效实施意味着本澳已具备必要的法律基础，全面启动网络安全体系的构建工作。

（一）建立三层架构的网络安全管理体系

根据《网络安全法》有关组织的规定，澳门网络安全管理体系由委员会、预警及应急中心及监管实体共同组成，其为一个上下贯通的三层架构格局。

1．委员会

委员会是澳门网络安全的顶层决策机关，由行政长官领导，负责引领澳门网络安全的总体发展、监督整个网络安全体系的运作。

2．预警及应急中心

预警及应急中心是一个预防和应对网络安全事故的专门技术性机构，由司法警察局统筹，并与行政公职局及邮电局共同组成。预警及应急中心作为整个网络安全体系的沟通协调枢纽，其职能主要涉及三大核心业务。

一是网络安全风险预警：收集分享各类网安情报，并依法实时检视关键基础设施营运者的网络安全状况（不包括网络通讯内容），于发现攻击苗头时发出预警讯息，协助营运者及早防范，避免事故发生；

二是网络安全事故应急协调：集中接收营运者的网络安全事故通报，与监管实体共同跟进事态发展，协调网安事故的应急处理工作，促进事故处理的效率和成效，致力减低事故对社会造成的影响；

三是行政及技术支持：向委员会提供行政和技术支持，协助推行委员会制订的政策方针；同时为监管实体和营运者提供技术支持，例如协助分析网安事故的成因并建议改善措施，避免同类事故再次发生。

预警及应急中心围绕上述三大核心业务，建立一个事前预防、事中应急、事后改善的全方位网络安全管理循环，环环相扣、不断完善，时刻守护澳门的网络安全环境，推动澳门网络安全工作持续进步。

3．监管实体

监管实体作为监管角色，负有对不同行业领域的营运者进行管理与监察的责任，其职责主要包括：为受其监管的营运者制定相应行业领域的专属性网络安全管理制度；监察营运者的网络安全计划及行动，确保营运者履行《网络安全法》及技术规范等法律法规所定的网络安全义务；对违规营运者开展处罚程序，行使处罚权；与预警及应急中心合作制定预警及应急程序，并于事故发生时实施该程序；收集营运者的网络安全年度报告和事故总结报告等。

根据《网络安全法》，关键基础设施分为公共和私人两个领域。公共领域的关键基础设施主要是指政府部门，并由行政公职局负责监察公共营运者履行义务的执行情况；而私人领域的关键基础设施是提供重要公共服务的私人公司，涵盖包括通讯、电力、供水、交通运输、医院、银行、博企等 11 个不同行业领域的业务范畴，并分别由指定的 11 个公共部门监察该等私人营运者履行网安义务的执行情况。

（二）整个网络安全体系的运作

保障网络安全是政府、企业和社会各界的共同义务，靠政府的单方面努力是远不足够的，社会各界的支持和配合极为重要。因此，除了委员会、预警及应急中心和 12 个监管实体外，整个网络安全体系的参与方还包括分属 12 个不同行业领域的公共和私人营运者。

澳门网络安全体系可以分为两个范畴：决策范畴，指的就是委员会，负责订定网络安全总体方针、目的及策略，并监督执行范畴各实体的网络安全活动及运行；执行范畴，包括预警及应急中心、监管实体及营运者。执行范畴各实体就网络安全重要事宜等向委员会报告，并由预警及应急中心负责向委员会提供行政与技术支持。

执行范畴具体运作如下：

1．预警及应急中心由司法警察局作总体协调，行政公职局和邮电局则分别负责公共领域和私人领域网安工作方面的协调事宜，三个组成部门之间相互合作，信息共享。预警及应急中心就网络安全风险向监管实体和营运者发送预警讯息，并应监管实体的要求，在其履行职责时给予技术支持；

2．监管实体监管营运者的网络安全活动及运行，并将营运者提交的年度报告副本送交预警及应急中心；

3．营运者是整个网络安全体系的主角，负有组织性义务、程序性、预防性及应变性义务、评估及报告义务与合作义务等四大方面的义务。当不幸发生网络安全事故时，营运者需及时向预警及应急中心和监管实体进行通报。另外，营运者需要每年向其监管实体提交一份网络安全报告，载明其网络安全风险评估结果、倘有已记录的网络安全事故，以及已采取或计划采取的改善措施。

在委员会的领导和监督下，本着“谁营运，谁负责”原则以及“最少介入”原则，预警及应急中心与各监管实体密切协作配合，携手共同管理与应对网络安全风险，推动各营运者做好对澳门关键基础设施的网络安全保护工作，切实履行法定义务，提升澳门总体的网络安全管治水平。

五、网络安全风险管理与应对机制的落地与实施

除上述法律及管理体系外，网络安全风险管理工作尚需执法落实和技术能力等层面的支撑及相应具体工作予以保障，下面将详细介绍有关的落实情况。

（一）公布营运者名单，明确《网络安全法》具体适用对象

为明确《网络安全法》的具体适用对象，负责监管公共营运者的行政公职局对公共营运者名单进行了统计与整理，共有 64 个公共营运者。此外，特区政府透过第 92/2020 号行政长官批示，指定了分属 11 个行业领域的私人营运者名单，共有 134 个私人营运者，将来并会定期检视、按需修订营运者名单。

（二）发布通用性技术规范，明确网络安全义务要求

保障网络运行安全，必须首先明确营运者网络安全的义务和责任。鉴于信息科技发展日新月异，营运者须因应不同情势，适时更新调整所需采取的防护机制及技术措施。故此特区政府遵照适度立法原则，在《网络安全法》这部基础框架性法律中并没有直接规范营运者履行网安义务具体运作和技术要求，而是透过向营运者发出具约束力的技术规范来明确有关规定。

为此，预警及应急中心三个组成部门，自2018年中就开始着手制定《网络安全——管理基准规范》及《网络安全——事故预警、应对及通报规范》两份适用于各行业领域营运者的通用性网络安全技术规范，并已于2020年5月13日刊登于《澳门特别行政区公报》，自公布翌日起正式生效。

1.《网络安全——管理基准规范》主要内容

规范旨在订定营运者在日常网络安全管理和运作中，包括管理制度、操作程序、等级评定、安全措施、风险评估等各方面的基本要求。其核心内容要求营运者根据各个信息网络和计算机系统对维持社会正常运作、保障市民合法权益的重要程度，评定系统的网络安全保护等级并实施分级保护。营运者需要根据信息网络和计算机系统所属的网络安全保护等级，在安全建设管理、安全运维管理、物理和环境安全、网络和通讯安全、服务器安全、应用和计算机数据安全等六大面向范畴中，实施与该等级相应的管理措施和技术防范等安全措施，履行相应的网络安全保护义务。例如，评为“一般级”的系统需要满足总共46项措施要求，而评为“高级”的系统则需要满足总共130项措施要求，从而引导营运者将各类资源合理分配到所需之处，达致按需分级保护、妥善管控风险之目的。

2.《网络安全——事故预警、应对及通报规范》主要内容

规范旨在订定预警及应急中心、监管实体和营运者之间发出预警信息和接收事故通报的双向沟通协调机制，并向营运者提供预防及应对网络安全事故的一般性指引。其中，预警及应急中心负责从不同渠道收集与分析各类网安风险及威胁信息，及时向营运者发出预警信息和处置建议，协助营运者防范事故发生。而当营运者不幸发生网安事故时，须根据事故的性质、对社会和市民造成的影响等因素进行评级，根据其严重性在规定时限内向预警及应急中心和监管实体作出通报，并定期汇报事故的应急处置工作进展情况，以便特区政府及时掌握相关最新信息、协调事故处理并于必要时提供适当的支持及协助，以尽量减轻事故对社会及市民所造成的损害。此外，营运者完成事故的应急处置工作后，需向其监管实体提交事故的总结报告及改善计划，避免同类事故再次发生。

（三）协助各参与方进入法治轨道，促进网络安全体系顺畅运行

当前，《网络安全法》的落实现正处于起步阶段。为协助网络安全各参与方步入法治轨道，有条不紊地开展及推进健全澳门网络安全体系的建设工作，促进网络安全体系顺畅运行，预警及应急中心与各监管实体在委员会领导下积极开展相关工作，多项工作正稳步有序推进，并已取得一定进展。

1．预警及应急中心投入运作，发挥沟通协调枢纽作用

预警及应急中心于《网络安全法》生效

当日同步投入运作，办公地点设于司法警察局总部大楼内，实行每周 7 天、每天 24 小时全天候运作模式，由专业的技术人员轮值无间断守护各个关键基础设施的网络安全，并配置有各类先进的网络安全软硬件设备。

一是网络安全态势感知系统：为有效履行《网络安全法》赋予司法警察局的职责，透过网络安全态势感知系统实时检视本澳各关键基础设施营运者网络与互联网之间传输，每日逾 15 太字节（Terabyte）的计算机数据流量及特征（不包括网络通讯内容），从而感知各营运者的网络安全状态，及时发现网络攻击苗头或其他异常情况，协助营运者及早处置各类网络安全风险，避免发生网络安全事故，或将事故的危害尽量降低。

二是网络安全事故预警及通报平台：鉴于网络安全环境瞬息万变，维护网络安全的工作需争分夺秒，为实现预警及应急中心、监管实体及营运者之间的电子化便捷信息分享渠道，预警及应急中心正分阶段向各监管实体、公共及私人营运者推出使用网络安全事故预警及通报平台，以便能及时发出网络安全事故预警信息、进行事故通报及跟进等各项相关工作。

预警及应急中心自 2019 年 12 月 22 日投入运作后，持续向营运者发出各类预警信息，以及协助跟进处置多宗网络安全事故；同时与各参与方保持紧密合作，并提供适切的行政及技术支持，包括协助举办委员会全体会议、与监管实体举行技术会议、向营运者举办网络安全技术规范在线讲解会等，从而积极发挥预警及应急中心沟通协调的枢纽角色，协助各方有序开展各项网络安全工作，并已初见成效。

2．监管实体密切配合，助力营运者履行网络安全义务

在预警及应急中心有序推进建立健全网络安全风险管理与应对机制的过程中，监管始终一如既往地予以积极支持与配合，做了大量细致性的具体工作，主要包括协助确定公共营运者和私人营运者名单、收集营运者为履行网安义务所需提交的数据、协助开展对私人营运者拟指定的网络安全负责人之适当资格审查工作等，从而带领及促进营运者开展履行各项网络安全义务。

六、持续维护澳门网络安全环境所面对的困难与展望

透过上文所述的各项措施，在委员会的领导下，各参与方携手合作、各司其职，澳门的网络安全建设工作现已取得一定的进展成果，在多个方面实现了“从无到有”的跨越。然而，有关工作亦正面临各种困难和挑战，尤其是人力资源十分紧缺、难以及时掌握有助防范事故发生的威胁情报以及应对和打击跨境网络攻击活动存在障碍等三方面尤为突出，必需加以克服才能保证相关工作的可持续发展，切实维护并不断优化澳门的网络安全环境。

（一）持续维护澳门网络安全环境所面对的困难和挑战

1．网络安全专业人才十分紧缺

澳门特区虽小，但信息科技要求齐全且广泛，本澳市场上一直缺乏足够的信息科技人才，更严重缺乏会技术、懂侦查并且具有网络安全和计算机法证专业资格，适合于预警及应急中心工作的复合型人才。在澳门，各政府部门间互相争抢信息科技人才的问题本来就存在已久，《网络安全法》的实施更进一步加剧了全澳社会对于网络

安全专业人才的热切需求，而且本澳大多数私人企业，尤其是博企能给予更优越的条件来争夺人才。在网络安全人才高度紧缺、高度竞争的情况下，能够成功招聘到出色的网安人才已属难能可贵，更遑论能招聘到足够数量的人才以满足业务需求。

2．难以及时掌握有助防范事故发生的威胁情报

有效的风险管理措施对维护网络安全至关重要，而当中的网络威胁情报收集及分析环节一直发挥着极为关键的作用，精确和及时的威胁情报有利于防守方迅速制订防范及应对策略，有效减轻面对各类网安风险的负担。然而，由于澳门各类网络基础设施和应用服务规模有限，十分依赖由其他国家和地区所提供的网络服务，导致特区政府在收集网络威胁情报方面的可行方法面临制约，未能广泛并准确地掌握本地区总体的网络安全态势。虽然市面上提供相关服务的供货商众多，但由于其情报源并非针对本地区进行收集，往往有很多与本地区相关的威胁情报没有被及时发现及提供，当中只有很少部分信息对本地区有所作用，导致分析人员需要花费大量精力和时间从海量及零散的威胁情报中分析提炼出数量有限的有价值信息，极不利于网络安全风险管理工作的有效实施。

3．应对和打击跨境网络攻击活动存在障碍

由于网络环境的高度相连性及自动化，一旦遭受具高度专业性及针对性的进阶持续威胁攻击（APT），或来自四面八方的DDoS 攻击等网络攻击活动，必需争分夺秒完成有效的封阻或控制措施，方能降低其危害性，避免造成严重后果。由于大多数网络攻击的源头皆来自境外，往往需要请求相关国家或地区提供协助，对事故应急处理工作的及时性产生了极大阻碍，致受攻击一方处于极为被动的境况。同时由于上述原因，在针对跨境网络攻击或网络犯罪活动的刑事侦查工作中，依靠条件限制多、流程时间长的国际司法互助机制并不适合应对具高度隐蔽性、易变性、取证难的网络攻击罪案，容易导致证据灭失、线索中断的困境，最终让犯罪分子逍遥法外。

（二）应对困难和挑战，求同存异加强海峡两岸和港澳地区警务合作

上述澳门特区所遇到的各种困难和挑战，相信也是世界各地执法部门所共同遇到的问题。因此，倘若海峡两岸和港澳警方能够把握住民族、地域、语言、文化和经济等各方面皆关系密切、紧密相连的优势，抓紧建立彼此间的网络安全合作机制，必定能够在很大程度上互相促进彼此的网络安全事业发展，纾缓有关困境。为此，本文就有关方面提出如下三项合作建议：

1．人才培养及经验交流机制

建立海峡两岸和港澳地区的网络犯罪侦查及网络安全技术人员的人才培养及经验交流机制。参考国际刑警的做法，以在线或线下形式定期举办特定议题的培训课程及交流会议，教授刑侦及技术人员专业知识、交流各地的网络犯罪和网络威胁形势、分享具代表性的案件侦查、事故应急处理及威胁防范心得等，从而提升相关人员的专业能力和技术水平。另外，透过举办上述活动，将能促进各方人员之间建立良好关系，有助于在实际工作中的沟通合作。

2．网络威胁情报分享机制

海峡两岸和香港澳门警方建立网络威胁情报分享机制，当发现可能涉及四方的威胁情报，例如恶意 IP 及域名、恶意软件、

APT 组织相关信息等，或于发生针对政府部门、关键基础设施等重要信息系统或涉及重大民生福祉的网络攻击活动时，及时互相分享相关信息，让各方都能及早作出预警及防范措施。此外，透过共同的网络安全威胁情报进行综合分析和研判，将有助于发掘潜在的网络犯罪组织团伙、攻击手法和威胁形势，从而协助提升各方的网络威胁发现和防御能力，并可藉此推动开展联合打击行动。

3．重大网安事故紧急互助及联合侦办机制

建立重大网安事故紧急互助及联合侦办机制，就针对政府部门、关键基础设施等重要信息系统或涉及重大民生福祉的网络攻击活动，采取快速的共同拦截措施，例如处置涉嫌发动攻击的 IP 地址、散播恶意软件的网站、协助进行网络流量清洗等，以便及早制止事件进一步蔓延及恶化，避免受攻击方面临的损失进一步扩大。与此同时，亦需共同探讨适当措施，协助各方提高案件侦查工作的便捷性，例如可考虑在正式收到司法互助请求前，预先协助采取措施保存相关的犯罪证据，避免证据灭失，保障之后的司法协助工作能够有效开展。

七、结语

关键基础设施关乎社会利益及社会正常运作，面对难以洞察、攻击范围蔓延至诸多行业领域的网络攻击，澳门特区政府透过《打击计算机犯罪法》及《网络安全法》两部法律，形成事前预防与事后打击双结合的网络安全风险管理与应对机制，建立健全本澳的网络安全防范性管理体系，为发展电子政务和智能城市保驾护航，响应社会发展实际需求，体现了特区政府保障网络安全、推动信息化发展的坚定决心。

同时，面对着人力资源不足、网安威胁情报收集能力受限、应对和打击跨境网络攻击活动存在障碍等各项阻碍网络安全持续良好发展的困难和挑战，我们倡议海峡两岸和港澳警方与有关方面加强交流，建立各项合作机制，共同致力提高整体应对网络安全风险的能力，有效打击网络犯罪，维持一个天朗气清、生态良好的网络环境，持续造福亿万民众。

参考文献：

[1]澳门互联网研究学会．2020澳门居民互联网使用趋势报告．2020．6

[2]澳门特别行政区政府行政公职局．2015年－2019年澳门特区电子政务整体规划．2015．10

[3]澳门特别行政区政府．电子政务．第 2/2020号法律．2020．3．30

[4]澳门特别行政区政府建设世界旅游休闲中心委员会．澳门特别行政区五年发展规划（2016-2020年）．2016．9

[5]澳门特别行政区政府科技委员会．2018年澳门智慧城市发展策略及重点领域建设咨询总结．2018．5

[6]澳门特别行政区政府司法警察局．刑事案件年度统计数据．2018年统计数据

[7]澳门特别行政区政府保安司司长办公室．最新罪案数字．2016．1-2019．12

[8]澳门特别行政区政府．打击计算机犯罪法．第 11/2009号法律．2009．7．6

[9]澳门特别行政区政府．修改第 11/2009号法律．打击计算机犯罪法．第 4/2020号法律．2020．4．27

[10]澳门特别行政区政府．网络安全法．第 13/2019号法律．2019．6．24

[11]澳门特别行政区政府．网络安全委员会、网络安全事故预警及应急中心及网络安全监管实体．第 35/2019号行政法规．2019．11．25

[12]澳门特别行政区政府司法警察局．第 5/2006号法律．2006．6．12

[13]澳门特别行政区政府．修改第 5/2006号法律．理由陈述．2019．11．21

[14]澳门特别行政区政府．第 92/2020号行政长官批示．2020．4．7

[15]澳门特别行政区政府．澳门特别行政区公报——第二组．2020．5．13

责任编辑　黄新春