



预防犯罪和刑事司法委员会

第十六届会议

2007年4月23日至27日，维也纳

临时议程*项目4

世界犯罪趋势及对策：联合国毒品和犯罪问题办公室及
会员国在预防犯罪和刑事司法领域的工作的统一与协调

编拟欺诈、非法滥用和伪造身份资料问题研究报告政府间专
家组第二次会议结果

秘书长的报告

目 录

	段次	页次
四、经济欺诈与其他问题之间的关系	21-41	3
A. 欺诈和有组织犯罪集团的卷入	21	3
B. 欺诈和跨国性要件	22-24	3
C. 信息、通信和商业技术在欺诈中的作用	25-27	4
D. 欺诈、欺诈所得和洗钱	28-31	6
E. 欺诈与腐败的关系	32	8
F. 欺诈与恐怖主义的关系	33-37	8

* E/CN.15/2007/1。



G. 经济欺诈与波及身份犯罪之间的关系.....	38	11
H. 欺诈在重建或经济转型国家中的影响.....	39-41	11
五、国际合作与管辖权.....	42-53	12
A. 法律互助及其他调查合作.....	43	12
B. 引渡.....	44-45	13
C. 管辖权.....	46-51	14
D. 时效期限.....	52	17
E. 预防合作.....	53	17
六、公私部门之间的合作.....	54-57	18
七、预防经济欺诈.....	58-60	19

四、经济欺诈与其他问题之间的关系

A. 欺诈和有组织犯罪集团的卷入

21. 欺诈可以由个人实施，但专家意见和各国提供的材料都表明，多数严重欺诈都涉及《联合国打击跨国有组织犯罪公约》（大会第 55/25 号决议，附件一，第 2 和第 3 条）所说的“有组织犯罪集团”。各国既描述了老牌有组织犯罪集团或其代表实施的欺诈，也描述了为实施欺诈和有关犯罪而专门成立或组织的新集团的情况。吸引老牌集团的是巨大的潜在收益、较低的风险及与它们所从事的其他犯罪之间可能存在的互补性。较小、较灵活的集团之所以成立，是为了实施某些形式的欺诈，如提款卡欺诈或信用卡欺诈，有时要到处转移以避开执法部门，锁定新的受害人。第三类是法人或其代表实施的欺诈。在这方面，如果公司或一帮雇员实施欺诈或参与欺诈，就可以认为他们是有组织犯罪集团。有些国家报告说，有几种欺诈比其他欺诈更有可能涉及有组织犯罪集团；而且许多国家都认为，有组织犯罪集团实施的欺诈危害更重，这不仅是因为它给受害人造成了损失，而且也因为犯罪分子用此种欺诈所得搞腐败或其他方式扩大有组织犯罪集团实施的活动或影响。经济转型国家和地区特别关切这一问题，因为这些国家和地区的体制较薄弱，因此资金充裕的有组织犯罪集团构成的威胁要大得多。¹一些国家对涉及有组织犯罪集团的案件规定了更为严重的罪行和更严厉的惩罚。有几个国家说它们的打击有组织犯罪立法是一项对办理涉及严重欺诈的案件有用或可能有用的措施，特别是提到了涵盖调查权、减刑及追查和没收犯罪所得等领域的立法。有组织犯罪集团的卷入意味着，如果所指控的欺诈具有跨国性质，则可以适用《打击跨国有组织犯罪公约》，以促进法律互助、引渡和其他形式的合作。一些国家认为，它们的现行立法足以处理这一问题，而且有几个国家强调必须在技术援助和培训等领域开展工作，以确保尽可能有效地利用公约。

B. 欺诈和跨国性要件

22. 跨国欺诈很普遍，而且许多国家级专家也有处理跨国欺诈的丰富经验，但各国都没有关于跨国欺诈本身的统计材料。许多国家说，它们遇到了此类案件，其他国家则对仅仅可能遇到此类案件表示关切。大家主要关切的问题是，跨国欺诈似乎在不断增多，而且此类犯罪实施容易，调查起来则费用很大，又困难又复杂。有些国家看到有证据证明犯罪分子有意利用这种困难，只选定远离本地执法人员

¹ 见秘书长题为“未来可能进行的与商业欺诈问题有关的工作”的说明（A/CN.9/540，第 3、第 8 和第 9 段）。

的受害人下手。² 其他国家报告了小型犯罪分子集团行骗的例子，这些犯罪分子在国内或国与国之间窜来窜去，以锁定新的受害人，并逃避被起诉。

23. 一些国家注意到了跨国欺诈与信息、通信和商业技术的可利用程度及其利用情况之间的关系。它们认为一般性欺诈案件和涉及某种跨国要件的欺诈案件增多，是因为犯罪分子和潜在受害人可能利用种种技术的机会多了。技术和跨国性之间最明显的关系就是，犯罪分子和受害人之间可以利用传真机、电子邮件、电话和因特网建立联系，不过还有其他联系。有一个国家注意到，因为有了种种技术，不同管辖区的犯罪分子才能彼此开展有效合作。³ 其他国家注意到，欺诈所用信息是一种非法商品，犯罪分子买卖以“浏览”或网络犯罪手段获得的潜在受害人名单和信用卡数据，并常常用电子邮件转发。技术和跨国性还有一种联系，是犯罪分子常常利用呼叫转送的匿名重邮程序和类似手段，努力隐瞒身份和地址，以免受到执法部门的追查。

24. 有几个国家也描述了各种本身就具有跨国性质的欺诈。具体例子包括逃避支付关税的货物走私，各种各样的海上运输欺诈，移民、护照和签证欺诈以及涉及宾馆错时轮住安排等假期旅行或住宿的欺诈。人们发现，利用第三国家是洗钱阴谋和某些形式的税收欺诈的一个要件，把记录、其他证据或资产隐藏在第三国家，让调查人员调查不着；利用第三国家也是各种网上欺诈的一个要件，网上欺诈利用众多管辖区，让人很难追查电子邮件和其他通信的来龙去脉。

C. 信息、通信和商业技术在欺诈中的作用

25. 多数国家都没有把滥用技术和欺诈联系起来的记录或明确罪行，虽然许多国家觉得必须确保现有诈骗罪涵盖技术革新，因为犯罪已开始对技术革新感兴趣。

《欧洲委员会网络犯罪公约》⁴ 缔约国必须把计算机欺诈和伪造定为犯罪。信息、通信技术与付款卡和电子商务等商业技术之间，商业技术与许多种欺诈之间，都有明显的联系，利用技术实施或支持欺诈也有多种不同方式。联合国国际贸易法委员会在有关商业欺诈的工作已经注意到了这种联系。⁵ 报告中提供数据的国家

² 见 *the Report of the Canada-United States Working Group on Telemarketing Fraud*, (<http://www.justice.gc.ca/en/dept/pub/wgtf/headings.html>)；另见 *Mass-Marketing Fraud: a Report to the Attorney General of the United States and the Solicitor General of Canada*, pp. 11-12 (<http://www.usdoj.gov/opa/pr/2003/May/remmfinal.pdf>)。

³ 见 *Libman v. the Queen* [1985] 2 S.C.R. 178 (Supreme Court of Canada) and *Secretary of State for Trade v. Markus* [1976] A.C. 35 (United Kingdom House of Lords)。

⁴ 欧洲委员会，《欧洲条约集》，第 185 号，第 7 和第 8 条。

⁵ 见联合国国际贸易法委员会第三十六届会议工作报告（《大会正式记录，第五十八届会议，补编第 17 号》）(A/58/17)，第 236 段。

一般都描述了指明信息技术大增的模式，随之而来的还有向相应商业技术的逐渐转变，犯罪分子相应也开始实施以商业技术为目标或利用商业技术和利用信息技术降低风险、扩大潜在收益、增加受害人数的种种欺诈。其他国家没有关于这一问题的具体数据，它们要么报告了国家专家提出的类似意见，要么说它们预计会出现此类现象或对此类现象感到关切。目前有关这个的统计材料有限，应当审慎对待。向新技术、新商业惯例的过渡，犯罪分子的行为翻新以及执法和立法的新对策，都可能使所报犯罪率产生无法预料的迅速变化，而且有些国家已经描述了一些这种变化。统计材料之所以有出入，也是因为犯罪统计领域在不断变化，也是因为有时为了鼓励提交报告而使用种种技术，这就可能造成犯罪明显增加，因而无法反映实际变化。

26. 技术以各种各样的方式影响欺诈。技术为犯罪分子提供了机会，降低了他们的犯罪风险，但在预防、控制和威慑欺诈方面也可能非常奏效。有几个国家指出，技术的影响绝不是单方面的或只对犯罪分子有利。犯罪分子利用技术最常做的就是与受害人建立基本联系，包括初步查明、筛选和联系受害人；准备诱骗；要受害人做出反应；转移资金，先从受害人手中转到犯罪分子手里，然后再由犯罪分子转移，进行洗钱。许多欺诈案都在不同阶段使用了不同技术。例如，利用大众通信建立初步联系之后，接下来的劝诱就可能需要利用电话建立更密切的个人联系。同样，把资金从受害人手中转出，常用受害人能够合用的快速不可追索的手段，如信用卡或电汇，而随后犯罪分子彼此之间转移资金则使用不太可能被反洗钱措施发现的其他手段。技术也被用来联系犯罪分子，传送信用卡数据等信息，隐藏犯罪分子的真实身份和地址，给侦查通信制造最大困难。技术还有其他作用，包括利用扫描仪和打印机制造高质量的伪造证件；犯罪分子利用正在研制的技术把其欺诈阴谋弄得合理、可信；传播虚假信息，以此作为大型欺诈阴谋，如拍卖欺诈或股票欺诈的一部分。

27. 国家和私营商业信息来源都提出了若干利用技术预防、调查和起诉欺诈的具体事实和建议，而且有些国家已经注意到这些建议强调了公私实体开展有效合作的一个关键领域。一般说来，技术先进的调查措施给执法和售货员带来了种种好处，但有时也给商业实体造成了彼此不相容的压力：既要支持刑事司法，同时又要保护客户，还要确保业务仍然具有竞争力，在商业上立得住。控制网络犯罪本身就是一项重大商业活动，有些给出安全忠告、提供安全培训和安全技术的公司，都把它们作为商品卖给需要保护客户、防止经济及其他损失的公司。有些国家注意到需要在各个阶段密切合作，包括开发新的商业技术和控制犯罪技术，需要广泛的专门知识，也需要资源和承诺来解决多数国家视为迅速、经常发生变化的问题。所提到的技术用途包括安全和预防因素，如防火墙和加密；也包括调查方法，

如果拦截通信和利用“流量数据”追踪犯罪分子的通信。⁶有一个国家指出，当局追踪通信，不仅要查出犯罪分子、犯罪所得和证据，而且也要查明大宗欺诈案未提出诉讼的其他受害人。人们提出了一个问题，即执法当局想尽量长久保存此类数据，而商业实体则往往担心储存费用及其对客户和订户隐私的影响。还有若干国家提出，利用技术预防欺诈，迅速公开已败露的阴谋和新的事态发展，以提醒执法部门、私营公司干事和潜在受害人警惕。商业研究表明，多数商业欺诈，包括利用技术的欺诈，都涉及内部雇员，这突出表明了进行识别和预防欺诈培训的必要性及保护公司和客户利益的重要性。

D. 欺诈、欺诈所得和洗钱

28. 欺诈和洗钱彼此相连，但多数国家把二者当作两个不同问题。它们认为欺诈是经济犯罪，因为其动机是为犯罪分子创造经济或其他物质利益；而洗钱虽在经济环境中进行，却不被当作是一种经济犯罪，因为其目的只是在其他犯罪获得收益后隐藏和转移所得。除了提供有关立法的材料外，多数答复调查的国家都没有对打击洗钱措施发表广泛意见。有些国家从程序角度指出，欺诈和洗钱彼此相连，因此需要协调制订对策，但洗钱已经是其他机构广泛探讨的主题，未来有关欺诈的工作应当避免一切不必要的重复。多数国家认为欺诈是上游犯罪，目的是采取打击洗钱：有 30 个国家把一种或多数严重欺诈定为上游犯罪，有 12 个国家没有提供材料，只有 4 个国家不认为欺诈是上游犯罪。收到的答复中列有冻结、扣押、没收和归还欺诈所得的众多民事、刑事和证据条款。有关欺诈的关键问题包括必须评估各国和全球与欺诈有关的全部成本和欺诈所得；与其他主要上游犯罪相比，欺诈作为洗钱所洗收益的一个来源所具有的相对重要性；以及欺诈所得的最终目的。另外，商业利益集团和某些受害人辩护人对犯罪所得的没收额与工商企业损失挽回额的出入感到关切。

29. 只有几个国家提供了有关全部损失或收益的材料，但损失和收益显然数额巨大，在一些国家中欺诈所得高达数亿美元，损失总额有数十亿美元。⁷所报商业来源只限于特定部门，如保险和信用卡业，可它们的调查结果与上述数字吻合。反洗钱金融行动工作组（FATF）没有报告详细的统计材料和估计数字，但总的说来，它认为欺诈和有关形式的金融犯罪属于被定为非法收益来源的四大犯罪，其

⁶ 例如，见《欧洲委员会网络犯罪公约》第 1 条（d）项：“‘流量数据’指涉及计算机系统通信、由作为通信链一部分的计算机系统生成的任何计算机数据，指明了通信来源、目的地、路径、时间、日期、规模大小、持续时间或基本服务类型。”

⁷ 见“未来可能进行的与商业欺诈问题有关的工作：秘书长的说明”（A/CN.9/540），第 5 至第 11 段。

他三大犯罪是麻醉药品贩运、武器贩运及移民偷渡和人口贩运。⁸ 获得有关欺诈和其他犯罪全部所得似乎成了一种可怕的挑战。国家金融情报单位通过调查被举报可疑或归入其他类别的金融交易，如大宗现金交易开展工作，但所得资料只用于调查，而不用于统计。在调查阶段，通常不清楚资金是否在洗刷；等到清楚时，又不清楚这些资金与哪些上游犯罪有联系。此外，国家犯罪统计往往以事件、起诉、定罪和判决数量为根据。犯罪所得，即使知道，通常也是估计出来的，而且此类估计可能只反映了已知交易和已知受害人，在多数情况下它们只是实现总数的一部分。关于犯罪所得的最可靠信息都掌握在私营公司手中，这些公司为了业务而追踪损失。但这种信息只限于公司的特定业务领域，在某些情况下可以视为商业机密。再者，欺诈所造成的损失远大于犯罪分子所得的收益。报告、查出和计算的并非全部，而且损失计算也可能包括间接费用，有个商业来源称之为欺诈的“附带损害”。⁹

30. 欺诈和洗钱是两个不同概念，实际上却可能彼此相像。¹⁰ 二者的主要区别是，欺诈本质是把合法资金转为非法收益，而洗钱则涉及随后转移和隐藏这些收益，虽然欺诈或洗钱实际上常常没有那么简单。例如，来自受害人的、明显经过洗刷的钱，可能作为“投资收益”付给他人，以便引诱他人中计，甚至可能又付给同一受害人，怂恿他们深入参与或阻止他们向当局投诉。二者主要相似之处是，二者都使用欺骗手段，涉及隐蔽或不引人注目的交易。这种犯罪固有的欺骗性及其相似性，有时给执法当局制造了难题，但也可能是个机会。有几个国家指出，也可以利用或修改反洗钱机制，如可疑交易必须举报的规定，以摸清欺诈情况，而且有些银行、电信提供商和其他商业或金融机构已经对大宗交易进行过滤，以找出带有欺诈意味的异常模式进行跟踪。因为涉及其他上游犯罪，欺诈案有时可能导致对洗钱的调查和起诉，反之亦然；这突出表明，有关政府实体和商业实体彼此开展合作是有用的。

31. 多数国家都说，它们已经出台了处理没收欺诈和其他犯罪所得的法律规定。这些规定包括以判定犯罪分子的刑事罪为基础的计划，对物诉讼，各种民事没收或追索可以基于刑事诉讼的混合诉讼程序以及由受害人或至少在一起案件中是由国家提出的单纯民事追索计划。有一个国家提到在无法从犯罪分子身上追回损

⁸ 见反洗钱金融行动工作组，*Report on Money Laundering Typologies 1995-1996*（巴黎，经济合作与发展组织，1996年6月），第10和第11段；和反洗钱金融行动工作组，*Report on Money Laundering Typologies 2000-2001*（巴黎，经合组织，2001年2月），第52和第53段。

⁹ Price Waterhouse Coopers Global Economic Crime Survey 2005, sect. 3.3.

¹⁰ 见反洗钱金融行动工作组，*Report on Money Laundering Typologies 2000-2001*，第13和第58段。

失时可以向国家本身索取某种补偿的计划。追索和归还收益实际上可能构成巨大挑战，在重大商业欺诈和大宗欺诈中更是如此。在商业欺诈中，受害人常常是法人，也间接涉及投资者、股东和客户，只是他们的权利很界定。在大宗欺诈中，许多管辖区中提出的许许多多的小型竞合求偿可能极其复杂，致使评估、判决和归还费用超过了损失或现有收益。民事求偿也面临着巨大障碍，包括通常缺乏有关追踪、冻结、扣押和没收的刑事司法权和救济。

E. 欺诈与腐败的关系

32. 调查问题表没有直接要求提供有关欺诈和腐败之间的联系信息，但会员国在答复中却揭露了某些联系。这些联系包括反欺诈和反腐败法规都适用于一起犯罪行为案件的情况，也包括两种罪行虽然适用不同法规，事实上彼此却有联系的情况。例如，挪用资金，如是外部人所为，则可能被视为欺诈；如是内部人，则为贪污。提供有关重大跨国欺诈信息的多数国家都注意到，这种欺诈往往涉及有组织犯罪集团，这也就是说，欺诈收益用来资助此类集团的其他活动，在许多情况下，包括贿赂官员和搞其他形式的腐败，以此掩护犯罪活动不败露。各国也讨论了用贿赂支持各种采购欺诈的情况，如贿赂奉派侦查和预防欺诈性交易的官员。有一个国家指出，其立法把几种常见腐败犯罪定为一种侵害国家或政府的欺诈。

《联合国反腐败公约》（大会第 58/4 号决议，附件）¹¹ 要求定为犯罪行为的各种欺诈，在某些情况下可以构成不同形式的欺诈或与欺诈有联系，因为从腐败罪可以作为欺诈的一部分实施或欺诈收益用于腐败官员。例如，除了贪污外，窝藏腐败所得财产罪（第 24 条），可能很难与欺诈窝藏区分开来。影响力交易（第 18 条）也可以视为一种欺诈，意思是说出售影响的公职人员事实上是在出售非他或她所有、因而他或她也无法出售的东西，这至少在答复调查的一个国家的领土上被认为是侵害政府的欺诈。

F. 欺诈与恐怖主义的关系

33. 与隐瞒等可能没有经济动机的身份欺诈不同，实现经济欺诈的是为获得物质利益，因此经济欺诈对恐怖主义分子很有用，它主要是作为资助恐怖主义分子组织和（或）行动的一种手段。¹² 安全理事会第 1526（2004）号决议所设分析性支助和

¹¹ 大会第 58/4 号决议，附件。《反腐败公约》要求定为犯罪行为的罪行包括贿赂（第 15、第 16 和第 21 条）、贪污（第 17 和第 22 条）、影响力交易（第 18 条）、滥用职权（第 19 条）、洗钱（第 23 条）、窝赃（第 24 条）及妨害司法（第 25 条）。

¹² 尽管没有就普遍适用的“恐怖主义”定义达成共识，但为打击供资罪行，《联合国条约集》，第 2178 卷，第 38349 号）第 2 条阐明这一术语。“恐怖主义”一词的定义和范围问题留给各国去处理，而且不清楚答复是基于公约还是各国自己的定义和描述。

制裁监测组，负责监测对基地组织和塔利班实行的制裁。它的报告确认，欺诈与其他犯罪，如绑架、勒索、抢劫和贩卖麻醉药品一起，共同构成了恐怖主义资金的潜在来源。¹³ 金融行动工作组在其有关恐怖主义筹资问题的工作中也报告了一系列类似犯罪。¹⁴ 有几个国家说，它们遇到了虽然少见，却与恐怖主义活动有关联或被认为与恐怖主义活动有关联的欺诈案，其他国家则表示它们对此问题感到关切。本地小型欺诈和信用卡欺诈用于或有助于维持个人或小组生存资助小型行动的嫌疑；范围较广、策划较周密的信用卡欺诈诡计可能用于资助大型行动或为其他目的创造数额较为巨大的、源源不断的收入。¹⁵ 各种消息来源表明，由于许多恐怖主义活动费用很低，大型、跨国活动容易受到监视，基地组织已分崩离析，作为资金来源的欺诈或其他犯罪日益缩小、日益立足本地的趋势。¹⁶

34. 各国遇到的重大经济欺诈包括保险欺诈、走私和消费税欺诈、汇兑欺诈、公共养老金方案欺诈及业务或商业欺诈。目前发现，养老金欺诈和信用卡欺诈，既被用作本地小型恐怖主义行动的单个直接资金来源，也被用于大规模、有组织阴谋诡计的基础。有几个国家还对以电信提供商为目标的欺诈表示关切，因为这种欺诈的真正动机不是要获得免费服务，而是获得无从追查的匿名因特网、电子邮件或移动电话服务。这种欺诈有段时间涉及网络犯罪分子和有组织犯罪，现在则由恐怖主义组织为了同样缘故而实施。¹⁷

35. 有几个国家在答复中，对可能利用慈善欺诈资助恐怖主义表示特别关切，而且有些国家遇到了已查明或怀疑实施了慈善欺诈的案件。金融行动工作组¹⁸及学

¹³ 见安全理事会第 1267 (1999) 号决议；关于基地组织和塔利班及有关个人和实体的第 1526 (2004) 号决议所设分析性支助和制裁监测组第三次报告 (S/2005/572)，第 69 至第 70 段；分析性支助和制裁监测组第四次报告 (S/2006/154)，第 63 至第 66 段。

¹⁴ 见反洗钱金融行动工作组, *Report on Money Laundering Typologies 2001-2002* (巴黎, 经济合作与发展组织, 2002 年 2 月), 第 10 至第 12 段。

¹⁵ 同上, 第 11 段, 例一。

¹⁶ 见分析性支助和制裁监测组 第三次报告 (S/2005/572), 第 67 至第 70 段; 和 Mark Rice-Oxley, "Why terror financing is so tough to track down", *Christian Science Monitor* (《基督教科学箴言报》), 2006 年 3 月 8 日。

¹⁷ 比如, 见 the testimony of Richard A. Rohde before the Senate Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary of the United States of America, 24 February 1998 (http://www.fas.org/irp/congress/1998_hr/s980224r.htm); and Alan Sipress, "An Indonesian's prison memoir takes holy war into cyberspace: in sign of new threat, militant offers tips on credit card fraud", *Washington Post* (《华盛顿邮报》) 2004 年 12 月 14 日。

¹⁸ 见反洗钱金融行动工作组, 《关于恐怖主义分子筹资的特别建议》(2004 年 10 月 22 日), 特别建议八; 反洗钱金融行动工作组, 2002 至 2003 年附件, 附件 B, 题为 "打击滥用非赢利组织" 一节。

术权威和新闻权威人士¹⁹也已确定恐怖主义组织滥用慈善机构和非赢利组织是个令人关切的问题。除了把欺诈和挪用慈善捐款作为资金来源外，犯罪分子还利用慈善机构作为洗钱或从其他来源悄悄转移资金的手段。²⁰安全理事会反恐怖主义委员会注意到了各国在根据安理会第 1373 (2001) 号决议制止滥用非赢利组织作为恐怖主义资金来源或渠道现象方面遇到的特殊困难。²¹2004 年，被确定当受针对资助基地组织和塔利班行为的措施制裁的个人和实体的综合名单，收入了 17 家慈善或非赢利组织，它们活跃在 37 个国家，开展了 75 项行动。²²

36. 令人担忧的主要情况有两种，一是创立假慈善机构，欺骗捐助者，为恐怖主义直接供资；二是渗入合法的慈善机构中，盗用捐款资助恐怖主义，盗用方式可能是欺诈或偷盗慈善机构本身。合法慈善机构也有自己的问题。严格会计规定令它们支付和筹资行政管理费用，即使是毫无根据地说它们与欺诈或恐怖主义牵联的谣言也有重大影响，会吓住捐助者。现在已发现，对慈善机构来说，对多数工作都靠慈善资金开展的国家来说，国家和慈善机构缺乏反渗透、反盗用能力，是一个令人关切的严重问题。²³

37. 还有一个令人关切的问题涉及针对特殊宗教、族裔或文化群体，从事与冲突地区有关的事业的慈善组织，因为犯罪分子可能效用收益资助恐怖主义组织，因为会计和监督保障措施难以适用。在这种情况下，很可能难区分欺诈和其他犯罪。如果捐助者受骗，通常都认为用于资助恐怖主义的捐助是欺诈；如果捐助者未受骗而受到恐吓，则认为用于资助恐怖主义的捐助是勒索。如果捐助者清楚组织的真正目的，而且也未有遭受强迫，捐助者和接受捐助的慈善机构都可能在实施与资助恐怖主义有关的内部犯罪，包括在执行《制止向恐怖主义提供资助的国际公约》²⁴所建立的机构。除了充当资金来源外，慈善机构还可能被用作其他犯罪获得资金的渠道或正当来源的渠道，在这种情况下就可适用供资和洗钱罪。

¹⁹ 比如，见 Martin Rudner, “Using financial intelligence against the funding of terrorism”, *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), pp. 42-43; and Jeremy Scott-Joynt, “Warning signs for the funding of terrorism”, *BBC News* (<http://news.bbc.co.uk/2/hi/business/4692941.stm>)。

²⁰ Martin Rudner, “Using financial intelligence against the funding of terrorism”, *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), pp. 43-44。

²¹ 见反恐怖主义委员会主席关于执行安全理事会第 1373 (2001) 号决议方面所遇到问题的报告 (S/2004/70, 附件), 第二节 A。

²² 见分析性支助和制裁监测组第三次报告 (S/2005/572), 第 84 段。

²³ 见分析性支助和制裁监测组第三次报告 (S/2005/572), 第 85 至第 88 段。

²⁴ 《联合国条约集》第 2178 卷, 第 38349 号。

G. 经济欺诈与涉及身份犯罪之间的关系

38. 为了避免重复，经济欺诈与涉及身份犯罪之间的关系在涉及身份犯罪的有关增编（E/CN.15/2007/8/Add.3，第13至第14段）中讨论。

H. 欺诈在重建或经济转型国家中的影响

39. 经济欺诈及有关各种腐败，在基本经济结构受到削弱或处于某种过渡的地方，构成了新挑战，各国提供了几个这样的例子。在经济大转型、发展、重建或刚摆脱冲突或自然灾害而逐渐恢复的情况下，各种条件利于行骗，而不太利于开展预防、威慑或控制欺诈工作。在这种情况下，防范欺诈和腐败的保障措施可能比较弱，所以就为欺诈和腐败创造了更多机会，涉及腐败或欺诈得手的案件、尤其是重要案件造成的损害，可能比类似犯罪在其他条件下造成的损害大。重大欺诈造成的经济损失可能极大，足以破坏被其他问题削弱或搞得失去稳定的经济，重大欺诈所得资金可能会大大加强面临业已削弱的刑事司法体系的有组织犯罪集团，这种情况只会加剧腐败，只会加重其他问题。重大欺诈得逞，腐败无处不在，可能会削弱对新的经济结构的信心，妨碍改革的有效实施。欺诈也是一种诈骗罪，在经济转型国家行骗的可能增大了，因为人对新的社会经济规则和做法的了解还不深。在某些情况下，冲突和重大自然灾害也为犯罪分子创造了机会，因为要从慈善机构和其他来源募集巨额现金，而且必须迅速用在很难实施平时本可以适用的反欺诈和反腐败保障措施的地方或此类措施可能那么奏效的地方。

40. 欺诈和腐败可能密切相关，在某些情况下这两种犯罪是一回事或有所重叠交错。例如，通常认为挪用开发项目资金是欺诈，如果挪用罪是内部人所为，那就可能归为贪污罪。²⁵ 在其他情况下，此类犯罪可能是单独进行的，却因犯罪分子的行为而产生了联系。如采购欺诈和其他常见欺诈一样，欺诈分子常常贿赂或诱感知情人，以确保欺诈得逞而不败露。

41. 有些国家和专家报告几个此类案件的例子。所报的有以重建和过渡项目为目标的欺诈，包括以新的税收方案、新的采购程序和私有化方案为目标的欺诈。有一个国家报告了以税收程序和私有化程序为目标的欺诈，有组织犯罪集团以此作为一个资金来源。另一个国家报告了以其新的增值税返还程序为目标的欺诈，这一欺诈极为严重，足以给国家预算造成消极影响。国际以慈善和保险为基础在

²⁵ 比如，见《反腐败公约》第17和第21条。

2004 年亚洲海啸等重大自然灾害之后开展的重新努力，也被利用，²⁶ 而且至少有两起案件称重大的“Ponzi”金字塔方案欺诈是破坏经济转型国家局势稳定的一个因素。²⁷

五、国际合作与管辖权

42. 重大跨国欺诈案对国际合作构成了巨大挑战。它们往往规模巨大，错综复杂，费用高昂，横跨许多管辖区，涉及许多犯罪分子，大量受害者及调查机构和私营部门机构。在合作规则和惯例已经改变以应对少数重大案件的国家里，大宗欺诈可能变得像是许许多多较小的欺诈。阴谋得逞的欺诈骗取了巨额收益；这些收益可以用来支持有组织犯罪集团，保护目前正在进行的欺诈行动，窝藏和洗刷收益，加大对司法互相和引渡的持久挑战。已收到的许多评论意见都强调开展合作的必要性，但主导观点认为，现有法律文书，特别是《打击跨国有组织犯罪公约》，对《欧洲委员会网络犯罪公约》缔约国来说，《欧洲委员会网络犯罪公约》为此类合作提供了充分的法律依据，而且重点是采取措施确保现有文书能够得到切实利用，而不是拟订新的文书，并且现有文书过去已得到了有效利用。人们还指出，在打击欺诈的一些重要合作领域，特别是预防等领域，不需要任何种类的正式法律权威或依据。

A. 法律互助及其他调查合作

43. 一些国家强调普遍需要提供有效的法律互助。一般说来，调查人员和检察官需要犯罪分子和受害人往来通信及资金转移的材料和证据。这包括确定通信来源和目的地、犯罪分子和受害人以及通信内容的信息，以便证实欺骗等要件。也需要证据经济利得转移的金融记录。重要的是追踪和查出收益，包括最初资金从受害人到犯罪分子手中的转移以随后的洗钱。证明涉及跨国欺诈所造成损害的证据也很重要，这可以包括来自受害人个人的直接证据或专家法庭证据。要证明犯罪分子的行为不符合正常的商业惯例，可能需要专家证据。有几个国家提出了有效

²⁶ 有几个国家的执法工作专门打击利用赈灾工作的欺诈；例如，大不列颠及北爱尔兰联合王国前国家刑事情报处发出一项公开警告（“Tsunami fraud threat: advice to the public”）；另见美国联邦调查局的网页（“Tsunami disaster relief fraud alert: don't be scammed”

（<http://www.fbi.gov/page2/jan05/tsunamiscam010505.htm>）。美国司法部成立了卡特里娜飓风反欺诈工作组，以处理各种欺诈，包括慈善欺诈、公私部门的养恤金欺诈、盗用身份、保险欺诈、采购欺诈及政府腐败行为（http://www.usdoj.gov/katrina/Katrina_Fraud/index.html）。

²⁷ 在 1996 至 1997 年期间一项金字塔投资计划失败之后，阿尔巴尼亚遇到了严重问题，包括暴力和从武器库抢夺小武器（见 Carlos Elbirt, “Albania under the Shadow of the pyramids”, *Transition Newsletter*, 2001（<http://www.worldbank.org/html/prddr/trans/so97/albania2.htm>））。同样，有些材料来源称政府核准的金字塔方案失败是海地政府 2004 年垮台的一个因素。

传递证人证据，专家提醒注意根据《打击跨国有组织犯罪公约》的条款使用录像连接证据。²⁸ 破获欺诈案的有效合作并非总是需要正式法律互助，因为有些通信和证据可以调查犯罪的管辖区内截获或获取。业已查明这方面存在的主要困难是案件错综复杂，合作所需时间长。有几个国家强调调查人员彼此开展快速、非正式合作很重要。多数合作都涉及信息共享，这必然要求兼顾调查和适当的安全保障。有一个国家指出，在破获跨国欺诈案中快速分享信息通常很重要，但也需要平衡和透明，以确保所分享的信息准确无误，并根据有关法律规则加以利用。

B. 引渡

44. 多数国家都表示它们可能引渡嫌疑犯，有些国家表示，如果它们不能引渡，就有权起诉在其领土管辖范围之外实施的犯罪，拒绝引渡请求的一些理由，如是引渡国民禁令、大赦法律和时效期限，都可能成为破获欺诈案的障碍。专家指出，《打击跨国有组织犯罪公约》第 11 条第 5 款要求为破获有组织犯罪案件，特别是规避司法的案件规定长久时效期限，办理较复杂的欺诈案也适用同样原则。

45. 《打击跨国有组织犯罪公约》规定缔约国有义务引渡被控犯有最严重欺诈罪的犯罪分子，或根据第 16 条规定的除外条款起诉此类犯罪分子，但只有在拒绝引渡是因为罪犯的国籍时才适用起诉义务。引渡的基本要求是，所实施的欺诈被两个缔约国的国内法视为严重犯罪，此罪涉及有组织犯罪集团，且具有跨国性质。²⁹ 公约还要求缔约国确保，它们如因为国籍缘故不能引渡，则对其某个国民实施的域外犯罪拥有管辖权，而且它还考虑把已定罪的犯罪分子移送到本国服刑。³⁰ 鼓励缔约国对被指控人在其领域内而它们不予以引渡的犯罪确立管辖权，但不是非确立不可。³¹ 在公约框架范围内，可以探讨的空白包括确保所有缔约国都充分执行公约，确保它们保证严重欺诈符合严重犯罪标准，确保不引渡其国民的缔约国执行“不引渡，即审判”原则的规定。另有两种情况可能也存在着空白。各国在执行选择性的第 15 条第 4 款时，应当确保它们原则且能够起诉只因是本国公民而未被引渡的欺诈犯。最后，多数重大欺诈案件都涉及有组织犯罪集团，

²⁸ 见 *the Report of the Canada-United States Working Group on Telemarketing Fraud* 和《打击跨国有组织犯罪公约》要求利用电视会议提供证据的第 18 条第 18 款。《反腐败公约》第 46 条第 18 款中也有类似规定。

²⁹ 《反击有组织犯罪公约》第 2 条 (a) 和 (b) 款，第 3 条第 2 款。

³⁰ 《打击跨国有组织犯罪公约》第 15 条第 3 和第 4 款，第 16 条第 1 和第 10 款，第 17 条；见《联合国打击跨国有组织犯罪公约及其议定书执行法律指南》（联合国出版物，出售品编号：E.05.V.2）和《网络犯罪公约》“解释性报告”所载管辖权讨论，第 233 和第 239 段（<http://conventions.coe.int/Treaty/en/Reports/html/185.htm>）。

³¹ 《打击跨国有组织犯罪公约》第 15 条第 4 款。

但个人也可能实施跨国犯罪，因此针对具体案件的协定或安排等应对措施可以就此作出规定。《欧洲委员会网络犯罪公约》³²也规定，如果有关国家是缔约国，就要引渡，而且这不只限于欧洲委员会成员国。然而，根据该公约规定，只有在某些情况下，在犯罪涉及使用计算机、计算机系统或数据时，欺诈和造假犯罪才可能实行引渡。不过，《网络犯罪公约》不只适用于涉及有组织犯罪集团的案件，在个人利用计算机实施欺诈或造假的情况下也可以适用。

C. 管辖权

1. 属地管辖权

46. 跨国欺诈是对常规领域管辖权提出挑战的最常见犯罪之一。³³ 犯罪分子可能在一个国家策划犯罪，以第二国家为基地进行实施，在第三个国家坑害人，在第四个国家积累和洗刷犯罪所得。受害人常常分布许多国家，犯罪分子还会利用更多国家达到其他目的，比如，用作“丢下盒子”（以转移资金）的地点，用作假网址的基地。在复杂的跨国欺诈案中，犯罪分子清楚管辖范围，也完全能够精心安排不同交易，以便最大限度地利用任何空白或弱点。作为对策，属地管辖权概念也有发展演变，属地管辖权已扩大，可管辖两国或多国同时发生的犯罪，在一段时间内从一国到另一国连续不断发生的犯罪，或在一国发生但对另一国产生某种明确影响的犯罪。现在，肯定始于起诉国而终于他处的犯罪或任何基本要件在起诉发生的犯罪的管辖权，似乎很普遍。³⁴ 有些国家确定属地管辖权的基础是策划犯罪的地方，犯罪最终要件或任何基本要件发生的地点，包括犯罪实施地点不确定的情况。³⁵ 是否可以根据一国领土上存在的非基本要求确定管辖权，则不那么清楚。只有一个国家报告说，有可能走得更远。³⁶ 在该国，必须证明与其领土有真正实质性联系，包括有策划、筹备等非基本要件存在，或有所得存在，但不

³² 《网络犯罪公约》第3和第4条（定为犯罪）及第24条（引渡）。

³³ 比如，见 Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003) pp. 158-180。

³⁴ John Seguin, “The case for transferring territorial jurisdiction in the European Union”, *Criminal Law Forum*, vol. 12, No. 2 (2001), p. 249。

³⁵ 比如，见 the United Kingdom *Criminal Justice Act, 1993* (c. 36), part I (http://www.opsi.gov.uk/ACTS/acts1993/Ukpga_19930036_en_1.htm); 和 Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003), pp. 163 ff。

³⁶ 在加拿大，检验是否与其领土有“真正实质性联系”，则取决于判例法。这种情况涉及在加拿大策划但牵涉其他国家受害人和所得的欺诈。确定管辖权的基础是，欺诈在加拿大策划，欺诈所得通过其他国家送回加拿大，有些基本要件也发生在加拿大（见 *Libman v. the Queen* [1985] 2 S.C.R. 178（加拿大最高法院））。

清楚是否只根据这些因素就可以确定管辖权。规定以一项基本要件存在为基础确定属地管辖权的国内法，在很大程度上也取决于如何阐述犯罪，取决于什么要件被列为基本要件。比如，同谋型犯罪通常范围更广，阐述网络犯罪和电信犯罪的文字可以明确包括某些要件，如为使犯罪落入一国的管辖范围必须在该国发生的作用或影响。《欧洲委员会网络犯罪公约》第 11 条规定，把企图、协助或怂恿实施该公约规定的实质性犯罪，包括与计算机有关的欺诈或造假是犯罪行为。

47. 通常受害人所在或受到不利影响的国家起诉动机最强。许多国家都根据其领土是否出现了犯罪结果或影响来肯定管辖权。多数国家限定此类影响只指被认为是犯罪基本或事实要件的影响，若是欺诈案通常必须有受害人。有些国家可能更宽泛地适用同一原则，包括间接损失。例如，坑蒙公司的欺诈可能影响股东和市场。妨碍起诉的最强大因素，特别是在重大欺诈案中，有案件的费用和复杂程度，一罪不二审原则及证人和证据等基本要件引入而且可能不符合国内证据标准。即使国家有管辖权，上述障碍也可能妨碍该国行使管辖权或导致与其他国家讨论哪个国家是最方便的起诉地。

48. 欺诈本身的性质和犯罪分子在策划和实施欺诈诡计时可能考虑到了管辖漏洞和限制这一事实，对现行属地管辖权造成巨大挑战。一方面，必须确保犯罪在任何情况下都可以起诉，必须避免留下犯罪分子可钻的漏洞，提出了一种较宽泛的管辖权模式。另一方面，管辖权可能有冲突，起诉费用高昂、错综复杂的跨国犯罪会遇到种种问题，又表明要采取更审慎的办法。属地管辖权逐步扩大的趋势可能会继续下去，这部分是因为跨国欺诈阴谋别出心裁，接触信息技术的机会越来越大。不可能对所有案件都可行或都奏效的确定管辖权的单一直接办法，现有模式也不可能适用各种可能出现的情况。最好的办法大概就是确保有尽可能多的国家拥有较宽泛的属地管辖权，各个有关国家进行有效合作，由提出起诉条件最好或最方便的国家实际提出起诉。

49. 为了确保能够有效地起诉跨国欺诈，目前有若干法律 and 实际可能，关键要看每个国家已经有何种措施可以利用。这些措施包括确保有基于本报告所讨论的种种管辖模式的充分管辖权，在适当的情况下还要考虑非基本要件，如策划、准备和所得，因为这些要件在欺诈案件中可能比在涉及其他类型犯罪的案件中来得重要。制订惩治欺诈罪立法也很重要，在依被界定为犯罪一部分的基本要件确定属地管辖权时尤其重要。如果欺诈阴谋把基地设在或发生在缺乏执法或起诉能力的国家，则可以提供建设必要能力的全盘技术援助，还可能援助处理特别犯罪，以此作为国际合作方案的一部分。

50. 鉴于适当的管辖权要求，常常有几个国家可以要求行使管辖权，而且协商应由哪个国家起诉很重要。这可能涉及法律、外交和实际问题，从每个国家提出的

管辖权和其他合法诉讼请求的相对优势和是否可以把犯罪分子引渡给想要提出起诉的国家的的问题，到种种实际考虑，如把证据从一国移送到另一国的费用和障碍，确保证据为诉讼程序所接受，并在法庭上加以有效陈述。如果决定几个可能的国家中应由一个起诉，就可以有效地转移管辖权。《刑事事项诉讼转移示范条约》（大会第 45/118 号决议，附件），《打击跨国有组织犯罪公约》第 21 条和《联合国反腐败公约》（大会第 58/4 号决议，附件）第 47 条对此都有规定。³⁷ 如果有两个或更多国家拥有管辖权而且想起诉，则可以考虑下述标准：

(a) 受直接和间接损害最大的国家。损害提供了起诉的动机和理由，通常也意味着有证据可用；

(b) 犯罪要件在其中实施最多的国家；

(c) 调查案件最用力的国家。除了资源承诺外，这通常意味着该国掌握了起诉所必需的证据；

(d) 证人和证据所在地。转移大量证据，特别是在复杂或欺诈案中，会大大增加费用，也会影响证据的法定可采纳性，影响证据是否能够得到有效利用；

(e) 理由最充足的国家。考虑到可以集中或转移给每个国家的证据的整体性，考虑到每个国家的证据法和类似标准，显然某个国家进行成功起诉的机会更好；

(f) 能力最强的国家。大型欺诈案错综复杂，从费用和专门知识的角度来看，对调查人员和检察官的要求非常高。经验丰富或资源雄厚的国家可以考虑，如果在法律上可行，就接受管辖权，或者向另一个理由较充足或请求较强烈、但能力稍差的国家提供援助；

(g) 犯罪分子的国籍及其是否可能被引渡。从其他方面看诉讼请示较弱的国家，如果不能引渡稳步发展的国民，可能就必须起诉他们；

(h) 所涉或可以起诉的其他犯罪。管辖权通常与特定犯罪相连，但重大欺诈阴谋常常包含其他犯罪，包括与身份有关的犯罪和洗钱。在某些情况下，考虑哪个国家最有能力同时起诉案件所涉各项犯罪，可能有好处；

(i) 卷入或可以被起诉的其他犯罪分子。同样，在具体情况下，不妨决定起诉某个犯罪集团若干成员的最方便诉讼地，然后引渡其余成员，以便一直审判；

³⁷ 另见 John Seguin, “The case for transferring territorial jurisdiction in the European Union” *Criminal Law Forum*, vol. 12, No.2 (2001), Seguin, loc. cit., p. 249。

(j) 各自的判决制度。一般说来，各国都愿意把管辖权对所犯罪行为给予类似惩罚的其他国家，而不太可能把管辖权让给它们认为其预期判决过于严厉或宽大的国家。

2. 域外管辖权

51. 属地管辖权概念已经扩展，以跟上欺诈和其他普通跨国犯罪的发展演变，但欺诈案适用域外管辖权却比较少见。有些国家办理本国国民或在其领土上有住所或有其他联系的人在国外犯罪的案件，特别是在国家宪法禁止引渡本国国民的情况下，就适用域外管辖权。³⁸ 管辖权也可以基于受害人的国籍（消极人格），虽然在经济欺诈中可能很难把此种依据与基于影响或结果的属地管辖权区分开来。有些国家报告说，它们根据保护性原则，采取了域外犯罪，以保护它们所认为的重要利益免遭特殊类型的欺诈。所举例子包括伪造货币、护照或其他重要文件和影响国家移民制度的欺诈。还有一个领域没有提及，但可能导致援引保护性原则，那就是坑蒙政府的重大欺诈，这种欺诈也可以认为是腐败罪。

D. 时效期限

52. 专家注意到，由于需要时间适当调查和起诉复杂的跨国案件，许多案件有可能出现时效期限问题；专家还注意到《打击跨国有组织犯罪公约》和《反腐败公约》³⁹ 的条款在考虑该《公约》涉及的罪行以及罪犯逃避司法的案件后要求确定适当的时效期限。审议了确保适用适当时效期限的若干办法，包括根据适用于欺诈罪的规约确定基本时限，制定在有些情形下中止限期的规定，如罪犯拖延诉讼或规避司法的情形，以及制定法律规定，虑及在法律规定的适当情形下从法律上延长时效期限。有些专家认为，涉及司法延期的办法与法无明文者不为罪这项基本原则不符；而在其他人看来，这种办法可能侵犯基本法确定的权利，因而不是可行的办法。

E. 预防合作

53. 国际反欺诈合作主要侧重于反应性措施，如在案件正在发生或者已经发生时调查和起诉欺诈行为。大多数国家在它们提供的国际合作资料中没有讨论预防问题。但在有的领域，国际合作在预防方面可发挥重要作用，与调查和起诉跨国欺诈大案相关的费用和复杂性表明，合作预防工作的益处也许很大。跨国欺诈包括

³⁸ 《打击跨国有组织犯罪公约》和《反腐败公约》的缔约国，如不能引渡其国民，就必须规定此种管辖权（见《打击跨国有组织犯罪公约》第 16 条第 10 款和第 15 条第 3 款，《反腐败公约》第 44 条第 11 款和第 42 条第 3 款）。

³⁹ 见《打击跨国有组织犯罪公约》，第 12 条第 5 款和《反腐败公约》第 29 条。

在个别国家从事的活动，如果有关官员及时掌握对跨国欺诈活动采取行动的必要资料，在国家一级采取措施通常就可以预防这类活动。总的来说，协助发展和改进预防技术、交流所获教训和最佳做法以及交流发展这类技术并使其收到成效所需的信息都是重要的。此外，可交流关于具体案件、方法或欺诈行动的信息，这种信息不一定包括需要正式法律互助程序的个人信息或调查信息的类型。

六、公私部门之间的合作

54. 经济欺诈是一种商业犯罪。因此，商界和刑事司法界既有合作的需要，又有合作的动力。联合国国际贸易法委员会（贸易法委员会）在关于其第三十六届会议的报告中指出需要开展这种合作，并要求预防犯罪和刑事司法委员会采取行动，贸易法委员会将继续开展其工作；这一要求是开展本项研究的部分原因。⁴⁰ 然而，刑事司法及商业惯例和目标并非总是一致。有些形式的商业欺诈依照刑法也许不属于犯罪。刑事司法界往往赞成调查、起诉和处罚，而商界常常主张采用纠纷解决机制和追回损失。其共同点是在迅速对进行中的欺诈采取行动方面的直接利益以及在预防和制止欺诈和似乎对一大部分案件负责的有组织犯罪团伙方面拥有的支配性战略利益。

55. 但在其他领域，公私利益不同。尽管私人利益受商业、市场以及对股东承担的信托义务的支配，但公共利益可从更广义的范围做出解释，人权、环境问题和共同利益等非商业因素是主导性更强的因素。法治和维护有效的司法和刑事司法制度要求关键职能，尤其是检察和司法职能保持不受外界影响。虽然有效的合作非常重要，但必须制定适当保障措施，确保商业利益不损害司法和检察独立性。在广泛的战略意义上，公私部门在有效的刑事司法系统拥有共同利益。对于商业治理和监管以及建立和维护可使商业企业繁荣发展的稳定的社会和经济环境，法治价值观念和体制至关重要。

56. 各国的答复表明，扩大公私合作不仅很有必要，而且可能性很大。大多数国家没有提供多少有关合作的信息，但许多国家表示认识到有必要扩大合作。许多答复仅描述了强制措施，如关于举报违法行为或透露涉骗法人或雇员的信息的法律规定。有些国家提到规章标准和立法标准。美利坚合众国描述了其 2002 年的立法，该立法制定了许多旨在处理欺诈活动与法人治理事宜的标准。⁴¹ 其他几个

⁴⁰ 《大会正式记录，第五十八届会议，补编第 17 号》(A/58/17)，第 238-241 段；另见经济及社会理事会第 2006/24 号决议，第 6 段，以及《经济及社会理事会正式记录，2004 年，补编第 10 号》(E/2004/30)，第 82 段。

⁴¹ 《美国上市公司会计改革和投资者保护法（2002 年<萨班斯·奥克斯利法案>）》(Pub. L. 107-204, 116 Stat. 745) 15 U.S.C. 7201 ff.

国家提到制定了商法和商事规章来鼓励用于阻止和预防欺诈的标准和做法。这些规章除其他外提高了公司报告和审计的透明度，鼓励注意到不法行为的人进行举报或者与当局合作，并要求高级官员对会计和财务信息的准确性承担责任。少数国家报告了本国的工商业发展战略，包括与欺诈有关的各种问题以及涉及共同利益的其他犯罪问题。这些发展战略对协商会议或会议做出了规定，商业和刑事司法专家可在会议上鉴别新问题并制定共同办法或协调办法。有些国家还表示成立了联合咨询机构来处理欺诈和洗钱等具体问题。

57. 强制措施的存在不一定能体现全面的公私关系。许多国家报告了与私人公司保护经营过程中获得的隐私和个人信息有关的法律规定，如果泄露保密信息，除非法律另有强制性规定，否则许多公司将承担民事责任。尽管如此，在许多国家似乎都出现了大好机会，即以适当的公私部门实体之间的联合协商为基础制定规章标准，并进行合作性而不是强制性的商事和刑事审判实践。商业企业共享信息是最常见的合作领域。由于顾客进行了举报或者由于观察到异常的活动模式或商业做法，这些实体往往首先认识到发展中的欺诈案件。有必要迅速提醒执法当局以便采取有效调查措施阻止正在实施的欺诈活动，这一点很重要。另一个主要的潜在合作领域是预防领域。以下第七节讨论的欺诈预防措施大致可分为两类：针对潜在受害者的措施，以便使欺骗他们成为难事；以及针对特定商业组织的措施，加大违法者袭击或利用它们的难度。

七、预防经济欺诈

58. 问卷答复中提出了许多可能的预防措施。欺诈行为涉及对受害人的欺骗，一些国家在其答复中讨论了告诫和教育潜在受害人的宣传运动。提出的其他措施则以预防措施为重点，这些措施运用技术增加了进行欺诈活动的难度，提高了在重大欺诈活动完成之前或大批人沦为集体欺诈的受害者之前及早查明和中止欺诈活动的可能性。若干国家提到快速准确地进行信息共享以便及时、顺利开展教育工作和反欺诈工作的重要性。有些国家提到对受害人以外的人，尤其是有可能遭遇欺诈的银行和金融机构雇员的教育。还有些国家提到在预防和减少欺诈的过程中运用各种方法打击洗钱和腐败。有一个国家提到禁止被定罪者在将来从事某种职业（例如，通过取消许可）可能会对欺诈惯犯产生作用。另一个国家指出一些简单的预防措施，例如，如果企业和消费者在将来实施与改变邮政地址和重寄邮件的程序有关的保障措施，就有可能在实质上起到预防作用。

59. 许多国家表示技术保障措施是重要的预防措施。例如，现代密码系统的创建和应用由于使现代缴费卡技术成为可行而获得广泛信誉，国际工商界已经带头使

用数字签名和其他顺应措施来减少较大商业交易中的欺诈行为。⁴² 技术措施被视为商业体系中几乎所有部门的必要措施，包括个人用户掌握的部门、商业体系各部门之间的通信以及处理和存储数据的部门。另外还指出，由于商业和鉴别行为的全球性，大多数技术措施都必须在全球范围内应用。否则在某个国家应用的安全措施在另一个国家可能会失效，或者可能会阻碍卡或者其他技术的合法使用。制定新的安全技术时面临的另一个挑战是技术、商业应用和罪犯的技术在不断发展。因此，非常重要的一点是，公私实体应始终保持警惕，一旦现有的预防措施过时，就投入必要的资金和资源来制定和传播新的预防措施。

60. 对于商界来说，在制定和实施技术预防措施的同时，也出现了成本和竞争问题。有时会出现相关的争论，即犯罪控制部门，尤其是帮助进行调查和逮捕的部门应当由政府还是由使用技术的公司和用户支付费用。商界往往使用成本效益术语衡量做出的选择，其关注的问题是：如果其他管辖区域的竞争者没有这种规定，那么合并某些安全部门可能会降低其在全球市场的竞争地位。虽然最好是让市场来制定和实施技术预防措施，但某些方面还需要政府的参与。许多国家表示它们规定了保护消费者免受欺诈和欺骗性或误导性广告等相关违法行为的最低标准，有些国家规定了确保保护消费者信息的最低标准。各国可单独或联合发挥有益作用，确保市场鼓励有效地进行预防和采取安全措施，并确保那些执行有效的反欺诈措施的公司的竞争地位和利益不会因采取这些措施受到损害。

⁴² 见《联合国国际贸易法委员会电子签名示范法》（《大会正式记录，第五十六届会议，补编第17号》和更正（A/56/17 和 Corr.3），附件二）。