INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

国际商会网络安全政策报告

目 录

介绍

私营部门已经并将继续在信息通信技术（ICT）领域的发展进程中发挥重要作用并承担重要责任。作为拥有 100 多个国家和地区的 4,500 多万家各类型行业及企业会员的国际组织，国际商会（ICC）致力于让数字技术随时随地为世界各地的所有人服务，从而充分发挥数字经济潜力，保障关键基础设施正常运行。这是国际商会的重要的目标，尤其在当前新冠肺炎疫情全球蔓延的背景下，这个目标已变得更为重要。国际商会的安全、可靠、弹性的数字网络政策，对维持社会和经济的正常运转以及保护生命和生计是至关重要的。

近年来，网络攻击和实践案例不断激增，国际商会加强与世界各国政府和企业开展合作，就何为强有力的网络安全政策达成共识，进而为企业和用户营造更安全的互联网环境。

国际商会广泛征集全球行业专家起草本报告，国际商会认为，政府和企业就网络安全的风险、目标、影响、应对措施等概念达成共识，其中包括国家法律法规和国际规则。虽然政府和企业在解决网络安全问题上扮演着不同角色，但双方应起到相互促进的作用。

本报告强调了企业和公众面临的主要问题和关键挑战。第一部分提供了一份确定关键问题的简略清单，以供所有利益相关方共同寻求有效的解决方案；第二部分概述了国际商会及成员进一步制定政策文件的关键领域，为私营机构和政府部门提供进一步的参考工具和政策建议。

中国国际商会/国际商会中国国家委员会　组织翻译
北京德和衡（上海）律师事务所　翻译

背景：网络威胁对商业的影响

预计到 2021 年[1]，网络犯罪将导致每年 6 万亿美元的损失，企业、政策制定者、用户都在关注快速上涨的网络威胁。目前，网络犯罪对所有规模和各个区域的企业均产生着影响，而其中约 50%的网络攻击是针对中小型企业 (SMEs)的。[2]

数字经济和互联网，以及作为两者技术支撑的跨境数据流已为许多国家的国内生产总值（GDP）带来了可观的增长。[3] 可以说，数字经济对经济的最大影响源于传统行业的数字化转型，因为各行各业的企业都在寻求运用技术以改进业务运营的模式。[4] 然而，用户和企业对网络安全的担忧表明，网络犯罪可能会阻碍信息通信技术和数字技术在经济发展中发挥作用。[5]

随着新冠肺炎疫情在全球的大规模蔓延，基于确保业务连续性、保护员工安全等因素，多数机构开始将大部分业务转移到线上。后疫情时期，在线数字工具的使用激增，为网络恶意行为者创造了新的机会，他们利用疫情本身及其对行业产生的破坏，大肆对中小企业进行网络攻击。

疫情前，网络攻击的影响就已令人担忧。2019 年，数据泄露的平均损失为 392 万美元。[6] 超过 40%的网络攻击目标是企业，每次攻击的平均损失超过 18.8 万美元。[7] 然而，网络入侵给企业带来的不仅是经济损失，因商业秘密、专利信息泄漏或声誉受损可能会威胁乃至摧毁一个企业。[8] 在美国，60%的中小企业受到网络攻击后的 6 个月后会陷入瘫痪。[9] 制造业、能源等传统经济都在进行数字化转型，以提高自身竞争力，这也为网络犯罪提供了新的机会，尤其是在国家行为体及非国家行为体中寻找攻击目标，并破坏重要的基础设施建设。[10]

互联网、数字经济、物联网的无边界属性所导致的互联网物理性依赖等，为网络安全描绘了复杂的法律和运营图景，几乎所有机构都利用信息通信技术和互联网来完成从最简单到最具战略意义的各项任务。全球供应链关联性日益增强，这些供应链上的信息通信技术系统都拥有因业务运营所需的内部和外部设备，然而这些相互关联的系统创造了相对复杂的环境，在这种环境下，打击网络犯罪具有较大的挑战，因为恶意行为者可以很容易地利用业务流程中的漏洞，并将贯穿供应链各环节的个体作为攻击目标。除了操作和行为风险之外，网络攻击的技术表现形式也在不断发展，从恶意软件到勒索软件，再

---

1 网络安全风险投资（2020 年），网络犯罪报告
2 网络安全风险投资（2017 年），网络犯罪报告
3 麦肯锡（2011）《伟大的变革者：互联网对经济增长和繁荣的影响》
4 UNCTAD（2017）《2017 年世界投资报告：投资与数字经济》
5 麦肯锡（2015）《数字化价值链》
6 Ponemon (2019)《数据泄露报告的成本》
7 Verizon（2019）《数据泄露调查报告》
8 Eubanks（2017）
9 米勒（2016）“60%遭受网络攻击的小公司在六个月内停业”《丹佛邮报》
10 McKinsey (2019)《释放数字化运营在发电领域的价值》；UNCTAD (2017) 《2017 年世界投资报告：投资与数字经济》

从勒索软件到供应链网络攻击。

此外，政府在提升网络能力方面的投入在很大程度上也推动了复杂攻击的升级。[11] 报告显示，因为工商界持续受到日益加剧的以国家支持的间谍活动的影响，[12] 60 多个国家都已采取行动来提高自身网络能力。[13] 因国家支持的间谍活动呈上升趋势，20%的全球企业将此列为最严重的业务风险。[14] 目前许多最为复杂的网络攻击都可直接归因于国家及其代理行为，或即使是由独立恶意行为者发起的攻击，也可能是政府行为的下游后果，因为网络能力通过窃取、出售等方式重新用于犯罪目的时将更为迅速地扩散。与此同时，我们看到越来越多的先进网络力量出现在恶意行为的金字塔顶端，而他们的手段和策略则会向下扩散，并进入一个危险的且具有政治和犯罪目标的直接或间接关联的威胁行为生态系统。

与此同时，在网络攻击方面，攻击者和防御者在技术、工具、成本等方面存在严重的不对称性。在上万次网络攻击中，防御者需要实施上万次成功的防御，而进攻者只需要一次攻击得逞即能达到攻击目的。而与企业、尤其是中小微企业的防御能力相比，进攻者通常拥有更大和更强的工具储备。网络犯罪的回报率很高且攻击者的成本相对较低，而防御性成本则要高得多。因此，在没有国内政府和国际组织支持的情况下，企业和用户在这场斗争中必输无疑。

无论是政府还是企业，都无法单独应对无国界网络威胁。网络安全是一项资源密集型活动，可同时利用私营部门和公共部门的储备。鉴于企业和监管机构都在寻求有效的方法来缓解网络安全问题，因此需要通过加强合作来提高对网络安全漏洞等的认识，并提高受网络威胁攻击后的恢复能力。

私营部门依靠安全、稳定、值得信赖的政策和监管环境来创造机会和刺激创新，并为利益共同体创造价值。破坏这种有利的环境不仅对安全构成威胁，而且也将对经济发展和生计构成威胁。因此，出于以下两个原因，整个工业体系都必须参与网络安全相关的国际规则制定。

第一，构建国际法和国际规范解释，对维护法律确定性和国家行为可预测性极有必要，这反过来也会对投资决策及跨国业务的风险量化产生非常重大的影响。

第二，受数字经济和网络威胁的无国界的关联影响，国家网络安全方案需要根据国际公约和国际合作来制定。

11《2018 年高科技犯罪趋势》IB 集团，2018 年 10 月，
https://www.group-ib.com/media/hi-tech-crime-trends-2018/

12 外交关系委员会（n.d.)《 国家资助的网络操作跟踪者》

13 Valantino-DeVries, Jenniter, Lam Thuy Vo, Danny Yadron《环球网络警察》编辑部,《华尔街日报》,
http://graphics.wsj.com/world-catalogue-cyberwar-tools/

14 Businesswire (2017) “网络间谍在 2017 年全球企业面临的最严重威胁中名列前茅”

客观反映国家对网络空间监管的具体成果指标是非常有必要的，虽然为实现有效监管而开拓渠道、设立机制、制定规范的流程更至关重要，但完成以上环节任务后还亟需进行有效的落实与改进。此外，确定短期和长期的现有成果指标、后续的行动方案也至关重要。私营部门最适合向政策制定者提出这些监管措施的制定用途和预期效果，并指出可能影响其执行效果的潜在障碍。

第一部分：目前网络安全所面临的挑战

1．社会普遍缺乏对网络安全威胁及其定义的了解

由于网络攻击参与者的性质、动机、目标、威胁类别以及攻击事件的频率、程度、后果严重性等因素的不同，网络攻击的影响也大为不同。当前，对形成全面的网络安全保护措施的挑战之一即缺乏对威胁类型的定义和共识。这种复杂和不断变化的环境使得威胁的概念化变得困难，网络安全的保护措施支离破碎，也为网络犯罪猖獗环境的营造提供了便利。

2．现行法律法规对网络安全威胁尚无明确规定

网络犯罪国际合作对创建有效的全球网络恢复机制非常重要，虽然已有针对企业和关键基础设施的网络攻击的国际和双边政策声明，但在管理和约束各国网络空间行为的国际规则制定方面，仍然进展缓慢。[15]

（1）国际层面

虽然许多人认为线下法律也应适用于线上行为，但目前各国在国际法的解释、适用性、实施、执法等方面仍存在重大差异。如果就国际法整体应用于网络空间不能达成共识，那么要界定和实施网络空间的国家行为就希望渺茫，因此也无益于推进所有利益相关方改善信任格局的局面。

如果没有符合法律和国际条约、约定及符合国际合作机制的共同有效的跨境刑事侦查和起诉规定，打击网络犯罪的跨境合作也将面临挑战。执法机构之间的约定和国际合作机制，通常是处理跨国网络犯罪的有效途径。目前，欧洲委员会的《网络犯罪公约》（布达佩斯公约）是唯一一份旨在提高打击网络犯罪合作水平的具备约束力的国际文书。不论是双边还是区域性的司法协助条约（MLAT）都可帮助执法部门更高效地访问其他司法管辖区的数据。《跨国组织犯罪公约》也可对此发挥重要作用。

15 政府专家组（GGE）是联合国授权的、在国际安全背景下促进网络空间方面国家行为的工作组，自 2004 年以来工作至今。参见联合国大会第 73/266 号决议。

（2）国家层面

企业需要依靠政府来确保必要的法律保障，从而使网络犯罪活动受到法律制裁。政府应确保对特定网络犯罪及其在网络空间实施犯罪进行类似刑事定罪，从而避免“网络犯罪天堂”的出现。跨司法管辖区、区域之间缺乏协作、对类似协作缺乏认识等对政策和法规一致性构成进一步挑战，跨区域协作将有助于降低对数字生态系统的不确定性、提高信任度。

3．面对网络安全威胁的能力和信任保护措施不足

首次使用互联网的儿童、妇女等特定群体最常受到网络犯罪、网络欺凌和其它网络风险的影响，包括这些群体在内的互联网用户需要具备有效识别风险和管理威胁的能力，才能有效利用互联网。

从商业的角度来看，企业规模无论大小、企业类型无论是混合电子商务还是高科技，具备识别自身网络安全风险并有效管理信息系统的威胁的能力是至关重要的。与此同时，所有的企业管理者，无论是小型家族企业的董事还是大型跨国企业高管，都必须认识到绝对安全是难以实现的目标。与许多商业挑战不同，网络安全风险管理仍然是无法轻易解决的问题。

此外，需要考虑的关键问题是，许多发展中国家希望并需要技术援助来制定法律法规、完善相关基础设施建设，从而为创建安全、可信、基于规则的数字环境提供支撑。但同时，很多国家仍然未设立国家互联网应急中心，且未制定数据保护法、网络安全立法、国家网络战略，甚至不能提供必须的技术和基础设施支持。

4．监管不平衡所产生的“寒蝉效应”

信息通信技术供应链是全球性的，有效整合和相互依存是营造良好数字环境的关键，而这依赖于各司法管辖区之间原则规定的兼容性和全球数据流之间的无缝衔接。

各国需要通过进一步合作和努力来规范实践行为，确保网络安全措施在提供必要保护的同时，还能够支持数据驱动创新。全球跨境数据流动促进了经济增长和社会效益，但过度限制跨境数据流动或减少市场准入的网络措施可能会对贸易、投资、创新造成负面影响。

安全性认证是新兴技术的基本要素，也是影响所有互联网相关机构的因素，但安全性并非万能钥匙，且不适用于自上而下的解决方案，随着新技术的不断发展和涌现，安全性对网络安全的影响需要进行具体分析。

第二部分：互联网安全挑战的应对

为了应对此报告第一部分提及的挑战，国际商会建议所有利益相关方：

- 在私营部门和公共部门之间就网络安全威胁、参与方、应对路径等方面努力达成共识。
- 承认国际法在网络空间治理中的适用，基于此，政府经与所有利益相关方磋商后，应当秉持公认的国际规则，并建立相应的制度作为有效补充，同时酌情考虑制定新的国际法规则或国家立法。
- 致力于引入保护商业与社会环境免遭网络犯罪侵扰的国家刑事政策。
- 承认政府间国际刑事领域协作机制对打击网络犯罪的重要性。
- 在增强能力建设与信任措施方面共同努力。
- 根据国际法律和规范，基于风险的方法逐案审议与现有及新技术相关的网络安全标准和措施。

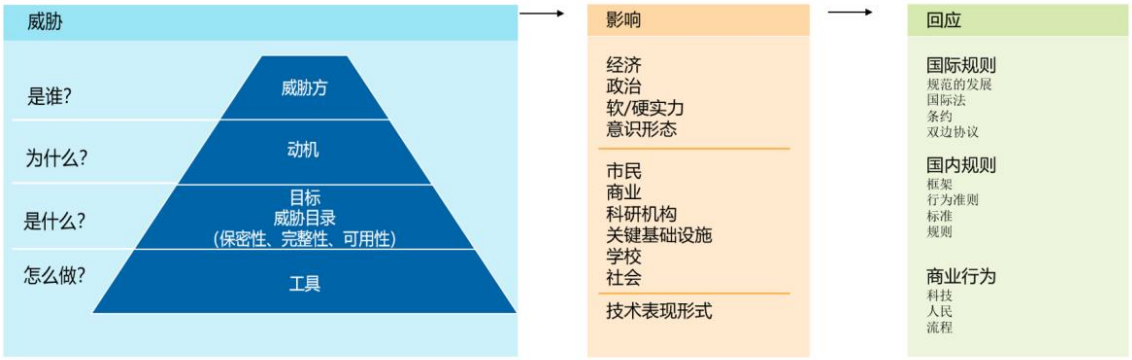
1．网络威胁的参与方及网络威胁应对的概念化

企业在确保自身财产和经营安全以及保护用户安全措施方面，越来越意识到推进全面网络安全管理流程的重要性，企业不断针对保护网络安全、用户、基础设施、网络系统存储内容等采取相应措施，这些措施不仅包括识别并减少网络威胁，也包括感知和应对威胁，还包括提升网络安全的响应速度和恢复能力等。

然而，考虑到网络攻击威胁的持续性，企业能采取的网络安全应对措施也仅限于此，而有效的政企合作对提升网络安全和应对网络安全威胁来说十分必要，建议政府与企业应在如何定义网络安全威胁、影响、应对等方面达成一致。

解决网络安全问题的方法必须是全面的、跨部门的，且各方均应认识到国内与国际环境相互依赖关系的关键因素。当政府力求制定应对网络威胁的有效管理措施、并期待其被高效利用时，应当意识到不同的司法管辖区与地区之间也在做着同样的努力，政府应在这些政策与规则之间寻求协调，从而将其可行性达到最大化。

应对网络威胁的国际协作可以促进互通，提升跨国经营实体之间的可视化及认知程度。因此，政府和企业就如何定义网络安全威胁及其影响和应对措施等方面达成共识十分重要。表格 1 就为我们勾勒了构筑网络安全的基本路径。



表格 1 网络安全的基本路径

2．制定及执行共同规范

尽管企业必须尽力确保其资产和经营的安全，并采取最大化措施保护其用户，但他们仍需依靠政府来确保必要的立法与执法，从而判定具体的网络安事件是否违法。

基于此，国际商会建议各国政府执行并遵守此前联合国在全球网络安全治理中的规范，并制定系列制度以有效执行这些规范。

首先，政府应遵守国际规范，并与各利益相关方共同制国际规范以及符合各国实际的实践方案，增加透明度。具体如下：

- 与行业合作并制定国际规范以确保稳定的经济系统。
- 推动各国对现有的国际法适用的实践达成共识。
- 基于原有规范的基础上，为确立更具体的标准提供指引，促进跨境数据自由流动。各国履行阻止源自本国网络犯罪的承诺，禁止进行国家行为的网络攻击，包括借助网络实施国家支持的商业秘密盗窃、以及破坏关键基础设施等行为。

工商界应支持联合国政府专家组（GGE）在 2015 年制定的规范，并为实施和强化规范贡献自身力量。

此外，私营部门正在联合并发起制定负责任技术使用规范，包括：世界网络安全技术论坛（Global Forum on Cyber Expertise），《网络安全技术协议》(Cybersecurity Tech Accord)，《网络空间信任与安全巴黎倡议》(The Paris Call for Trust and Security in Cyberspace)，《网络社会路由安全相互协议规范倡议》（Internet Society MANRS initiative）等。国际商会将继续参与支持各项工作，并积极推进各项倡议间所强调的信息共享与合作机制。

当我们同网络犯罪做斗争时，各国政府可以开展联合执法，落实调查和引渡流程。《布达佩斯网络犯罪公约》（The Budapest Convention）是全球唯一一个针对网络犯罪所

制定的国际公约，各国可以考虑成为公约成员国或利用公约作为本国的立法指引；各国也应当充分利用《联合国打击跨国有组织犯罪公约》（the Convention on Transboundary Organised Crime）来改进网络犯罪司法协助；政府也可以考虑确立多边或者区域性的司法互助协定（MLATs）来促进和便利跨境执法合作，并确保隐私与安全受到保护。

各国政府在寻求网络威胁管理的有效路径时，也应当意识到其他司法管辖区也在做着同样的努力，所以应寻求协调机制来最大化实现跨区域协作。这些路径也可以确保本国各类机构能够获得技术、服务和产品的最优配置，并通过直接融入跨市场或跨地区供应商的产品中，从而扩大其业务范畴。

3．强化能力建设

网络安全意识和网络安全常识的增长不仅能够强化个人、企业以及相关机构的能力，同样能够提升整个国家保护关键网络基础设施以及抵御网络威胁的能力，这在新冠肺炎疫情期间体现地尤为突出。一个国家成熟的网络安全体系能够推动营造互联网诚信环境，促进社会群体开展意义的沟通，有助于解决互联网分歧。

国际商会在为企业提供商业实践工具和自律指南上具有悠久的历史。国际商会数字经济委员会曾于 2015 年制定了《国际商会网络安全商业指南》（The ICC Cyber security guide for business），旨在通过简约清晰的指引来帮助企业在解决日益加剧的网络安全挑战中发挥作用。该指南参考了全球网络安全指南和国家战略，提出了帮助企业识别网络安全风险的五项原则，并借鉴各方最佳实践指出了企业应该实施的六项关键行动。

国际商会近期也同网络预备研究所（CRI）开展了合作，该机构主要由各行业和各地区的高级商业领袖组成，旨在融合有效的网络安全所需的人员管理、流程设计、技术实践，重点帮助中小企业解决网络安全风险管理问题。基于此，国际商会积极推动全球 4500 万会员能够适用国际网络防御计划，免受网络威胁。

尽管如此，部分国家的法律缺乏类似的基础法；部分国家缺乏数据保护框架；部分国家未建立国家互联网应急中心或者计算机安全事件响应团队（CERT/CSIRT），同时网络犯罪及其他网络立法也处于过时或者甚至是完全缺失的状态。[16]

我们亟需加强网络安全能力建设，确保有能够构建网络信任所需的基本法和基础设施，并使人们能够参与全球互联网安全发展进程。

16 更多细节请见联合国贸易和发展会议所支持的全球互联网立法追踪，网址为 https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commercelegislation-worldwide

4．网络安全应用与标准

各方必须继续加强对信息系统和互联网的可用性、可靠性和弹性的信任，以充分实现可持续经济增长，确保全球业务的顺畅运行，所有利益相关方需要齐心协力推动有效的网络安全实践以及构建开放、安全、稳定、有弹性、全球互通的网络空间。

各方必须强调该问题的重要性，并鼓励各界持续研究和部署适当的安全解决方案。在落实安全解决方案时，还要适当注意确保安全措施和相关风险与期望结果是一致且相称的，同时还要考虑跨技术手段的互操作性。

在需要国家层面做出监管回应的情况下，首先要通过适度的监管准来确估计网络攻击对企业和社会的影响；其次要在合适的监管目标及有效的监管干预时，通过平衡网络攻击的影响和受攻击后修复所需资源之间的关系，来实现投入与产出的平衡，因为通常体量较小的机构较难承受这类支出。

当政府在针对网络立法时，必须努力在贸易、投资、创收与真正的国家安全之间做出平衡。在需要考虑国家安全的情形下，政府应当寻求采取透明、可预见、适度以及非变相限制贸易的措施。

实现网络安全标准的最佳途径往往是市场参与者的自律、多样的标准倡议以及现有相关组织之间的合作成果等。网络安全测试应当以有助于推广通用标准的方式进行，同时还应与现行法律保持一致。通用标准可以促成动态适应，以便各方在技术革新、多样化挑战、不同风险场景等因素的背景下随时做出调整。

结论

为达成有效成果，政府应当与其他利益相关方合作，推进网络安全文化，制定惩治网络犯罪的法律。同样，数据保护和隐私等相关政策与法律框架，对确保消费者和普通民众继续信任信息通信技术和使用网络服务而言也是十分必要的。

各利益相关方的合作推动了对网络攻击多方面影响的共识，有助于借助现行国际法规范各国的互联网行为达成共识。这些交流将反映我们对持续演变的网络威胁环境认知的不断深化，有助于探索网络安全风险管理的整体方法，例如：欧洲互联网安全行业领导者（European Cybersecurity Industry Leaders），第三代合作伙伴计划（3GPP），经合组织数字经济安全与隐私工作组（OECD WPISP），以及事件响应与安全团队论坛（FIRST）等机构的专家所做努力都值得肯定，他们为业界提供了详细的指导方案。另外，国家与地区的计算机事件响应团队（CIRTS）也扮演着利益相关方召集方的角色，为互联网安全领域提最佳实践。

因此，本报告认为，有效的公私合作模式对加强网络安全和应对全球网络安全威胁非常有必要。

国际商会（ICC)

国际商会 (ICC) 是世界最大的商业组织，拥有来自 100 多个国家和地区的 4500 多万家会员。国际商会的核心使命是让商业随时随地为所有人服务。通过发挥政策建议、争议解决和规则制定等职能，我们致力于促进国际贸易发展，倡导负责任的商业行为，制定国际商事规则，并提供市场领先的争议解决服务。我们的会员涵盖全球领军企业、中小企业、商协会及地区性商会。