国际商会网络安全问题简报 1：呼吁政府对网络安全采取措施

摘要

全球工商界在保障技术安全和开发防御性网络工具、技能和程序方面持续进行了大量投入。虽然已采取这些举措，但仍不能解决网络攻击日益增长的破坏性危害。为了有效遏制不断增长的网络威胁，无论发生概率还是社会影响等方面考量，各国政府都亟需在本国和国际合作方面采取切实有效的行动。

国际商会呼吁世界各国政府：

>坚持履行对国际法和国际规范的承诺；

>采用多利益攸关方协同模式，在保护关键基础设施方面保持政策互通和相互协作；

>加强跨境合作，有效解决网络犯罪问题；

>遏制攻击性网络工具和手段的扩散；

>加强网络安全能力建设，提高对网络风险及网络暴露资产脆弱性的理解；

>支持私营部门积极构建系统化的网络威胁预防方案。

目录

简介

2020 年，网络犯罪对全球经济造成的损失预计达 5.5 万亿欧元，该数额是 2015 年的两倍。这表明史上最大的经济转移比全球毒品贸易额还要高。随着公众对网络攻击的敏锐度和关注度日益上升，由此造成的非经济损失也在增长。2021 年的一份报告显示，来自全球 28 个国家的受访公民表示，他们对网络攻击的恐惧与他们害怕感染新型冠状病毒肺炎的恐惧程度相当。本报告将阐述网络攻击对公民和社会带来的心理影响，及其对各国政府和企业带来的直接和间接挑战。

网络攻击有多种形式，大范围利用个人信息和技术的主要工具仍然是数据盗窃篡改、网络钓鱼、勒索软件。然而，实施恶意行为的主体目前也在瞄准第四次工业革命提创新成果，并意图产生潜在破坏。根据世界经济论坛《2020 年全球风险报告》显示，针对关键基础设施的网络攻击已成为继能源、医疗卫生、公用事业、交通等领域之后的第五大风险。

令人震惊的是，网络犯罪分子并不是公民和企业要防范的唯一实施恶意行为主体，越来越多的国家也在网络空间从事攻击活动。个别国家逐渐将技术和网络空间视为地缘竞争的新领域，有能力和意愿进行复杂的在线或离线网络攻击的国家逐渐增多。现在，个别国家将恶意软件、网络钓鱼、中间人攻击（MitM）、分布式拒绝服务攻击（DDoS）等传统的网络攻击（如与虚假信息活动结合起来，形成复杂的混合网络威胁，进而损害公众信任度，削弱社会凝聚力，影响经济发展。与此同时，这些活动威胁国际安全稳定，降低互联网为经济、社会、政治发展带来的巨大动力。

最近，几起严重的网络攻击案例生动地展示了其巨大的危害。。在新冠肺炎疫情期间，某医院遭受攻击导致无法正常运行，某网络犯罪团伙利用勒索软件使美国科洛尼尔管道运输公司系统瘫痪，并造成汽油短缺且几乎使美国东部地区生产停滞。2020 年初，美国信息技术公司 SolarWinds 遭受复杂网络攻击，此次攻击在该公司包括多家 500 强公司和政府部门的 1.8 万家客户系统中隐匿数月，覆盖面和危害性极大。2021 年前几个月，微软 Exchange 服务器软件中发现了四个零时差攻击漏洞。攻击者首先获得服务器管理员权限，进而访问受影响服务器上用户的电子邮箱地址和密码，以及访问同网络的连接设备。预估有 25 万台服务器成为了此次攻击的受害者，其中包括属于美国约 3 万家机构的服务器以及英国 7000 台服务器，还涉及欧洲银行业管理局、挪威议会、智利金融市场委员会服务器。受恶意攻击活动快速增长的影响，私营机构和公共部门经常面临网络攻击，以上案例只是其中的几个典型。

采取果断行动以遏制这些活动已不再需要选择，而是必要措施。目前，私营部门在开发部署安全技术方面进行了大量投入。据悉，2021 年与网络安全相关支出在超过 1500 亿美元，比上年度增长 12.4%。此外，企业花费大量时间开展网络安全倡议活动，推动负责任地使用信息技术规范的制定。目前已启动的倡议包括世界网络安全技术论坛、网络安全技术协议、《网络空间信任和安全巴黎倡议》、国际互联网协会互联网路由安全规范（ISO MANRS）。

各国政府必须采取行动，控制网络安全，帮助扭转网络安全状况恶化的趋势。本期简要阐述(i)企业必须面对的不断扩大的网络安全风险状况，(ii)网络安全威胁对企业界和更广泛的社区产

生的经济和社会影响，以及(iii)政府必须采取紧急措施，以遏制网络威胁并保护其公民和经济免于承担网络攻击的破坏性后果。

第一部分：企业面临的网络安全风险日益增加

当今人们的生活通过智能家居、智能工厂、智能城市等实现了互联互通维护网络空间正变得越来越复杂。关键基础设施和未经安全认证的嵌入式软件之间高度连接又紧密交织，这样相互依存的关系正在产生比以往更多的威胁和漏洞。预计到 2025 年，全球将将存在 670 亿个物联网终端，关键物联网基础设施的攻击面将达到前所未有的范围，并以这样指数级的速度增长。

恶意攻击企业网络在规模、频率、复杂性等方面不断增长。每天有约 35 万个新恶意软件变体被发布，为恶意行为提供了多种攻击性网络能力（OCC）选择。正因如此，一种被称为“勒索软件即服务”(RaaS)的模式催生更多勒索软件攻击事件。在此模式下，网络犯罪分子可以以低成本向任何个人或机构提供现成的勒索软件工具。这大大降低了参与这种有利可图的网络犯罪的门槛，助长了网络攻击，加大了攻击的潜在破坏性。

僵尸网络攻击在不断发展，并且变得越来越复杂。在 21 世纪初，犯罪分子主要利用僵尸网络进行初级的 DDoS 攻击，但今天的网络攻击者往往在更大的范围内进行恶意攻击活动。例如，在巴黎，一次 DDoS 攻击导致了 44 家医院的远程工作人员数小时内无法访问工作网络。

这种不断变化的威胁可以通过动态而灵活的解决方案来应对，而不是规范性的、以合规为重点的方法。同时，政府和所有相关行业部门之间的合作也是应对这些新型攻击的关键。

预防勒索软件的必要性

虽然实施恶意网络攻击者有众多网络载体选择，但勒索软件在过去 24 个月中仍然占据了主导地位，并在 2021 年成为了商业和政治议程的重中之重。例如，为了应对包括与勒索软件有关的问题在内的网络安全问题，美国宣布将“召集 30 个国家，加快在打击网络犯罪方面的合作。”

勒索软件是企业、基础设施供应商、供应链、学校、医院、政府和社区面临的最普遍的威胁之一。平均而言，每 11 秒就有一次针对企业的勒索软件攻击，每 40 秒就有一次攻击成功，并且没有一次攻击是相同，同时勒索软件的勒索金额也在增长。

最重要的是，一旦受害者受到勒索软件的攻击，几乎就无计可施了。2021 年，遭受勒索软件攻击的中型机构的平均被勒索金额为 170404 美元，从勒索软件攻击中恢复正常的总平均成本为 185 万美元。正如英国国家网络安全中心首席执行官 Lindy Cameron 最近指出的那样，“去处理一个勒索软件案件……感觉就像消防部门去面对一个已经烧毁的房子。可能会有一些法庭证据表明警察会追查...但是犯罪组织知道警察会怎样行动，因此行动很难获得成功。通常情况下，勒索软件案件一旦发生，就需要从头开始重建。”

威胁者正利用网络领域日益增长的复杂性，并在几乎完全不可抵抗的情况下开展恶意攻击行为，这使得本就已令人生畏的局面更加复杂。同时，这种能够在越来越隐蔽的情况下行动的能力正

在鼓励更具破坏性的网络攻击的增长——事实证明，在 2021 年，每次事件的平均损失达到了惊人的 424 万美元，同比增长 10%。像 Wiper 这样的恶意软件，包括：删除整个硬盘数据、多方面攻击，以及数据泄漏，都表明我们的网络对手越来越得心应手。

这种情况发生时，全球有近 400 万个网络安全职位空缺，并且网络保险费率飙升至 40%。这样日渐脆弱的网络保护现状和可能的严重后果为企业创造了一个极其不利的环境。网络攻击对企业和个人的影响已经变得如此普遍，以至于网络风险现在成为了全球首席执行官们最关心的问题，我们迫切需要保护企业、社区和经济免受恶意网络活动的影响。

OCC 的扩散和接触 OCC 的程度有可能进一步破坏国家间关系的稳定。由于复杂的网络环境提供了掩盖事实的可能，国家行为和个人犯罪行为之间的界限变得模糊不清，复杂的网络攻击不再只属于国家行为。随着国家对网络攻击发生的打击并对减轻其影响的尝试，同时也会出现无辜的受害者，例如，2017 年单方面针对乌克兰的 NotPetya 攻击，迅速蔓延到了全球，波及到了多家公司，并在全球范围内造成超过 100 亿美元的损失。考虑到目前全球网络的连通情况，随着网络攻击范围超出其最初的目标，附带损害的概念可能会成为一个越来越频繁出现的术语。这最终会造成进一步的混乱，让网络威胁者在“战争迷雾”中进行更肆无忌惮的攻击。

在此必须要引入社会安全的概念，因为现在不应只仅仅关注机构内部的信息安全和网络安全，还需要了解网络安全事件对社会的影响。由于缺乏针对恶意行为主体的明确有效的法律与政策手段（特别是在国家和国际层面），再加上法官和行政机构缺乏对网络安全问题的了解，网络安全事件对社会的负面影响更加严重。由于互联网的国际性，许多国家没有能力或没有意愿实施监管措施。随着 OCC 的“准入门槛”普遍放宽，特别是“接入即服务”（AaaS）模式的出现，网络领域可能会变得更具不稳定性和风险性。正如其他全球性安全威胁一样，仅靠法律和政策措施是不足以阻止这一趋势，强有力的国际政府合作、公私自愿合作，以及对网络犯罪分子和国家的威慑和惩罚措施才是当务之急。

第二部分：网络安全风险对经济和社会的间接影响

网络攻击破坏了经济机会，扼杀了经济增长，并造成了大批的失业。据估计，60%的小型公司在遭受网络攻击后倒闭。欧盟委员会的科学和知识服务机构联合研究中心（JRC）最近的一份报告指出，网络犯罪的成本从 2015 年的 2.7 万亿欧元上升到了 5.5 万亿欧元。随着网络攻击的类型和多样性的增加，企业越来越认识到直接和间接经济成本带来的货币影响，如果这一趋势仍未得到解决，我们可以合理地预测，到 2030 年，这一成本将加倍，达到 11 万亿欧元，相当于德国、法国和日本的名义 GDP 总和。

网络事故有可能导致几种不同类型的损失，包括有形和无形资产的损害、业务中断和盗窃有关的损失以及对客户（包括政府）、供应商、员工、股东和整个社会的各种形式的损失责任。据估计，与知识产权（IP）盗窃和金融犯罪有关的直接成本占目前货币损失的三分之二。知识产权盗窃每年给企业造成数十亿美元的损失，并影响了国家通过就业和税收提供的经济安全性。同时，与这些犯罪相关的额外间接成本正越来越多地被认识到，2020 年，一份基于对 1500 多家公司调查的报告指出，受网络犯罪影响的机构所承受的间接成本有以下几个例子。

1. 系统停机。对于大约三分之二的受访者机构来说，停机是一种常见的情况。2019 年，各组织因最长停机时间而导致的平均损失为 762,231 美元；33%的受访者表示，导致系统停机的 IT 安全事件给他们带来的损失在 10 万至 50 万美元之间。根据行业的不同，系统停机也会导致相关联的机构停机，而且这些停机往往包括那些关键的和政府提供的服务的暂停。
2. 效率降低。由于系统停机，各机构平均每周损失 9 个有效工作小时，从而导致效率下降；同时运营的平均中断时间为 18 小时。效率的降低可能会导致关键产品和服务的中断或减少。
3. 事件响应成本。根据该报告，大多数机构从发现事故到补救平均需要 19 个小时。一些安全事件可以在内部处理，但重大事件往往需要外部支持，并且占比较高，构成大规模事件损失的重要部分。
4. 品牌和声誉损害。重塑品牌的外部形象，与外部咨询公司合作以减轻品牌损害，或雇用新员工以防止未来的事件发生等，也是网络犯罪损失的一部分。26%的受访者指出，因网络攻击而导致的停机时间给他们的品牌声誉造成了损害。在这个充斥着不信任感的时代，机构已经面临着公众信任度的急剧下降，品牌和声誉的损害可能很难恢复。

除了金钱上的损失，网络攻击的社会影响更难检测和量化。在许多方面，它产生的影响更加隐蔽而深远，因为它将随着时间的推移加剧了所有其他因素的影响，而且较难被立即发现或以统计学方式加以衡量。网络威胁的社会影响表现在三个主要的、相互关联的方面：(i)个人的心理反应，(ii)机构行为的改变，以及(iii)对社会各阶层的非货币性的、现实的影响。

1. 个人的心理反应：网络威胁对个人（包括潜在的和实际的受害者）的心理影响可能会导致焦虑、担心、愤怒和抑郁，从而导致对数字技术和更广泛的技术创新的负面心态，甚至采取网络攻击作为报复手段。最近一份关于 COVID-19 影响人们对技术的态度的报告指出，三分之二的美国人表示他们担心自己的信息会在 2020 年被泄露。在一份基于美国、英国、法国和德国的 3264 名消费者的调查报告中，四分之一的消费者表示，他们将完全停止与出现漏洞的品牌互动。如果一个品牌出现漏洞的话，78%的受访者会停止与该品牌的在线互动，超过三分之一（36%）的人将完全停止互动，近一半（49%）的人不会注册和使用最近发生数据泄露的在线服务或应用程序。由于最近的数据泄露事件，近一半（47%）的人已经改变了他们保护个人数据的方式，超过一半（54%）的人比一年前更关心和保护他们的个人信息。随着企业（和政府）越来越多地通过在线渠道提供商品和服务，并依靠网络设备连接来实现公共服务，网络威胁的长期负面影响可能会阻止许多个人与企业和公共部门实体的互动。

2. 机构行为的变化：近年来，各种形式和规模的机构已经深刻地意识到网络攻击的潜在负面影响，并将网络安全作为一个生存问题来对待。除了明显的金钱和所有权损失、业务连续性的中断、以及法律风险和监管制裁，机构认识到了网络安全问题对其声誉的潜在损害，以及对供应链中的客户和商业伙伴的信任损害，这都将导致销售和利润额的下降。最近的一项研究回顾了在纽约证券交易所上市的 34 家公司的 40 起数据泄露事件，发现受到攻击的公司的股价平均下跌了 3.5%。尽管不同的行业部门和机构在网络安全的保护程度上存

在差异，但针对其的投资和改善都呈增长趋势。许多机构已经改变了他们收集和存储信息的方式，以确保敏感信息不受攻击。除此之外，客户也对与他们打交道的企业是处理安全问题方式更感兴趣，他们更有可能选择那些对网络安全保护措施进行正面宣传的企业。然而，并非所有的机构都有足够的能力减轻网络风险例如，一些公司由于担忧无法充分保护自己免受网络攻击，选择关闭或缩小其网店规模。这些趋势将继续为企业带来巨大的损失或失去商业机会。

3. 对社会各阶层的非货币性现实影响：除了上述讨论的大规模网络犯罪的经济影响外，还有其他由于扰乱了正常的生活活动，而对社会造成的影响。除了最近几个月发生的众所周知的事件，如 SolarWinds、微软 Exchange 服务器和科洛尼尔管道运输公司的数据泄露、阻止系统访问或能源供应链冲击等，更多的地方性事件则表明无论规模大小，网络攻击都具有瘫痪效应。2019 年，勒索软件攻击了德克萨斯州的一个 22 个城镇共享的软件供应商，恶意行为者要求 250 万美元的赎金来恢复行政服务，否则这些城镇的居民将无法查看支付记录或支付水电费。2020 年 9 月 10 日，杜塞尔多夫大学医院（UHD）遭遇了一次网络攻击，导致系统和数据访问逐渐失效，迫使医院取消预约，不再提供紧急护理，来院的患者被迫转移到其他医院；这一事件成为全球头条新闻，因为有一名需要紧急入院的妇女不得不因此被送到大约 30 公里外的另一家医院，这致使她的治疗被推迟，并导致了死亡。该医院花了近两周的时间才恢复了基本服务并允许急救服务重新开放，而要完全恢复运作则需要更多的时间。

上述趋势清晰地表明，虽然企业在预防和防御网络安全问题方面的投资十分重要，但仅靠私营企业本身无法阻止、预防免受网络攻击的破坏性影响。网络安全是私营企业和公共部门的共同责任，双方必须共同努力，以遏制威胁和减少风险。因此，企业敦促政府采取更加果断的行动，遏制影响个人、社区和经济的网络安全威胁。以下部分列出了政府需要采取的必要行动，以减轻网络威胁的普遍性、扩散性和后果的严重性，并为社区的繁荣建立一个更安全的网络空间。

第三部分：呼吁各国政府执行国际法和国内法并采取有效的行动倡议

1. 政府必须恪守关于网络空间领域的国际法，根据规范履行负责任的国家行为：

2021 年，联合国 (UN) 网络安全领域的全权工作组 (OEWG) 和政府专家组 (GGE) 通过了两份报告，概述了对网络空间领域国家行为的预期。这些最近的预期框架建立在先前协议的基础之上，例如 2015 年的政府专家组报告，以及该领域的其他双边和多边承诺。

在全球都存在大量颠覆性和破坏性的网络攻击的情况下，对于政府及国家行为的规范是值得注意的，现在是时候去实施这些规范、确保它们被有效遵守，同时不合规的国家责任被有效追究。

2. 各国政府必须加强跨境合作以有效应对网络犯罪：

各国合作找寻一个全球统一、信息共享、通力合作以及打击网络犯罪的方式是至关重要的。网络犯罪并不局限于一个国家，然而立法和监管权力仅适用于特定的司法管辖区，因此使执法部

门有能力且有保障地进行信息共享、合力抓捕以及司法管辖区达成充分承诺十分重要。《布达佩斯公约》创建了一个框架来支持这种信息交流，但各国需要确保公约的执行在资源和行动上得到充分的国内支持。我们呼吁尚未加入的国家能够加入该公约。

联合国（UN）全权工作组（OEWG）和政府专家组（GGE)是对遏制网络犯罪的现有承诺的补充，例如《布达佩斯公约》中所载的网络犯罪相关的承诺。除了履行其在《布达佩斯公约》下的承诺外，各国政府还必须进一步采取多边方法来应对目前增长的勒索软件和其他网络攻击的风险。在 2021 年 6 月的 G7 峰会上，各国领导人承诺会采取措施改善网络安全，推动形成用于网络空间的国际法共识，并且识别和破坏勒索软件以及犯罪网络。此外，各国政府还参考了经合组织 2015 年《关于促进经济和社会繁荣的数字安全风险管理的建议》，以获取国内安全计划基础构建的一般原则以及相关方案实施的操作指南。

各国政府现在必须采取行动，通过投资集体安全来履行这些承诺，并优先考虑以预防为先的方法来应对网络威胁。只要存在缺陷、安全漏洞和激励，违法分子就会发动攻击。因此，主导国家之间的统一战线对于加强全球网络防御至关重要。其中一个重要方面可能是对违反规范行为的关注，这加强和改进了网络安全国际协议中有关网络安全内容的必要性。除此之外，将网络攻击归咎于违反国际规范的国家时，应直接地说明其违反了哪些规范以及以何种方式违反。在合理的情况下，提升得出这些结论的信息透明度将使其具有更大的可信度，并进一步加强规范的认可。

3. 政府必须实施和执行法律文件，以阻止恶意网络活动的发生：

国家法律制度必须为各国提供必要的依据，以有效打击网络威胁并保护企业和社区免受由带有政治和犯罪目的环境的影响。要扭转网络冲突愈演愈烈的趋势，各国除了作出高级别的承诺外，还要专注于各国国情下的具体实施，并确保违反规则的恶意行为人会被追究责任。然而，20%的国家没有现代网络犯罪立法，大约一半没有国家计算机事件响应小组(CIRT/CSIRT)，因此各国政府应当重新作出承诺以确保资源可用于各国，保证必要行动的落实而与其他国家及各行业开展合作。

迄今为止，联合国的工作通过建立和加强负责任的国家的网络行为规范（例如 2015 年联合国 GGE 通过的 11 项规范）奠定了宝贵的基础。未来，我们需要以一个全球社区的身份共同努力，以确保对恶意行为者的追责。一旦超越界限、违反规范和法律，就应该承担相应后果。破坏信息和通信技术（ICT）供应链安全、攻击医疗保健组织、威胁能源运输和危害粮食资源不能因政府的不作为而正常化。

4. 政府必须遏制攻击性网络工具、设备和武器的扩散：

网络空间中反扩散政策的设置还未得到充分利用。当进攻性的网络功能随着复杂性的提升而不断增长并形成新的种类，减缓和对抗其传播就显得额外重要。但是要应对这一日益严峻的挑战，国际政策制定者就必须了解其背后的形成过程和激励措施。网络能力问题通常表现为对入侵软件的出口控制，尤其是恶意软件组件，因此各国迫切需要制定旨在遏制 OCC 扩散的国际标准的统一政策工具。

政府迫切需要在更广阔范围上将网络扩散理解为多种能力的扩散，这将为政策制定者提供足够的空间来制定可行的反扩散政策。了解犯罪市场、政府机构和私人性质的 AaaS 所提供的最先进的网络攻击产品的方式，还可以让政策制定者在不损害网络安全行业整体利益的情况下针对特定参与者采取行动。具体而言，揭示 AaaS 团体在扩散进攻性网络能力中所发挥的作用（半监管或自我约束，以及犯罪）将有助于推动更有效的反扩散政策的出台。同样，政府对提供恶意软件和监控服务的地下市场的快速发展，以及对将公民、记者和政府官员等作为目标并对在线生态系统造成威胁的网络工具和功能的干预也迫在眉睫。

5. 政府必须采取兼顾多方利益的方法来制定政策并保护关键基础设施：

虽然各国政府在实施国际协议以及保护企业和公民免受国内外网络威胁方面负有独自的责任，但网络空间的共享性质决定了利益相关团体之间需要协作以保护网络空间的安全和完整。利益相关的各国的共同行动对规则的制定、建设和实施而言至关重要。例如，企业为制定 2015 年经合组织安全指南的专家组提供了宝贵的技术知识，以确保该框架在商业和技术上都是可行的。同样，全球网络专业知识论坛（GFCE）可以作为各国的资源，协调区域和全球的网络安全项目，并且通过媒介来分享知识和专业技术，从而使得个人对网络安全的需求与社区提供的支持相匹配。另一方面，ISO、ISA、IEC、NIST 等提供的重要的技术标准和良好实践，是充分发展信息安全、网络安全和隐私管理系统的基础技术资源。

ICT 基础设施主要由私营企业建设和维护，因此关于网络空间和平与安全的讨论需要包含非政府机构的参与。上述联合国报告还强调了保护关键基础设施的必要性。考虑到这一点，各国应优先考虑对这些重要部门的网络安全进行投资建设，并利用全球公认的自愿标准和实践来创建国家网络安全框架，这也必将会为国际合作建立一致的基准。除此之外，明确地承认这些部门需要保护将推动对其安全性的更多投资。也应当就针对 ICT 基础设施的恶意行为划定红线，相关网络行为一旦越界，将被追究责任。

埃及和法国代表在全权工作组会议上提出了关于制定一项行动纲领的联合倡议，以促进网络空间中负责任的国家行为，其旨在建立一个考虑各国在国际安全背景下使用信息通信技术的联合国论坛，并确保全权工作组迄今实施的保护各利益相关方的做法，继续成为联合国在该领域所有工作的一部分。该提议提供了一个充满前途的解决方案。

企业协同的作用

虽然政府必须采取行动将风险降至最低，但行业也需要采取预防措施。特别是，鉴于本文件的重点，软件供应链的安全和关键基础设施保护具有战略和经济重要性。

提高软件和信息系统供应链的安全性。软件供应链涉及众多第三方开发人员和组件。在许多情况下，ICT 系统的用户对其控制系统中嵌入的软件组件知之甚少，因此开源软件的普及是非常重要的。专家指出，超过 90%的商业应用程序包含过时或废弃的开源组件，因此持续更新正是消除软件中潜在漏洞的方法之一。政府和软件开发者应该进行合作以提高关键基础设施和设备的软件供应链的透明度和安全性。这意味着需要采用安全的软件开发生命周期来缓解软件供应链风险；同时利用顶级技术进行软件组合，并实施人工智能驱动的、已被证明可以防止勒索软件和恶意软件的终端安全工具。

在这样做的同时，政府需要确保软件开发者的知识产权和商业秘密得到保护，并且不强制要求开发者公开专有软件的源代码。但是需要注意的是，软件开发人员及时披露漏洞必须确保负责任，且符合相关披露原则，如 CERT®协调漏洞披露指南。这将有助于开发人员、制造商和关键基础设施运营商监控软件组件的漏洞，管理供应链风险，并使有安全、性能或可靠性问题的历史产品退役。除此之外，及时和适当的事件报告，如果利用得当，有可能成为一个有用的政策。

通过建立预防为主的专门安全框架，提高关键基础设施的安全性。例如，美国国家标准与技术研究所（NIST）创建了一个网络安全框架，为美国政府和私营企业改进关键基础设施的网络安全。该自愿框架是基于现有的标准、指导方针和实践情况创建的，旨在帮助机构更好地管理和降低网络安全风险。NIST 网络安全框架由以下部分组成：框架核心、框架实施和框架概要。框架核心有五个功能：识别、保护、检测、响应和恢复，可与 ISO/IEC 27035 和 BS11200 标准系列中定义的功能结合使用，并且支持多学科团队之间的有效沟通。框架实施的目的是确保网络安全风险决策符合机构目标，且实际可行。框架概要旨在使机构要求、风险偏好和资源与核心框架中确定的预期结果保持一致。这三个框架组成部分共同努力，通过协调网络风险管理和增加政府与私营企业之间的信息共享，实现网络管理弹性。

结论

网络攻击的破坏性影响已经达到了惊人的程度，如果各国政府和更广泛的多方利益相关者不采取大胆、果断、全球协调的行动，这种影响将继续恶化。他们帮助维持的企业和社区迫切需要有效的补救措施，以减轻网络安全风险和网络攻击的影响。相关损害与损失已经形成了一个增长趋势，因此政府应该尽早关注网络安全。

各国政府主要负责保护本国公民免受国外和国内、有政治和犯罪目的的威胁伤害，这同时也适用于网络空间。政府采取果断行动遏制网络威胁并与利益相关者合作，将有助于增强经济信心，防止全球贸易中断，并确保维护一个更安全的网络环境，让企业和社区能够蓬勃发展。

十分重要的是，增加政府行动必须以广泛的利益相关者为基础，以便充分理解和解决网络安全问题，而不妨碍企业的发展和创新。各国政府还必须寻求最大程度地协调和调整，从而采取行动有效解决这些网络安全问题。

这份文件提出了政府在五个领域采取行动的紧迫性，如果得到实施，这些领域的网络安全问题将取得切实进展。除此之外，其还指出了公私合作的必要性，以及私营公司在持续投资技术和供应链安全方面的关键作用。之后的文件将提供关于政府采取具体行动的进一步细节和指导，并强调私营企业提出建议和实施举措的重要性，尤其着重于国际规范的执行、网络犯罪的减少和关键基础设施的保护。

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。

官方英文版地址: https://iccwbo.org/publication/icc-cybersecurity-issue-brief-1/

中国国际商会/国际商会中国国家委员会 组织翻译

翻译：娄鹤 北京德和衡（上海）律师事务所高级联席合伙人