UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

通过国际合作减少针对关键基础设施的网络行动

规范性预期及新兴良好实践

安德拉斯·卡斯特利兹 (ANDRAZ KASTELIC)

致谢

联合国裁军研究所核心资助方提供的支持是研究所从事一切活动的基础。该项研究由“安全与技术项目”的“网络稳定”研究组开展，该研究组由法国、德国、荷兰、挪威和瑞士政府以及微软资助。作者谨此感谢以下个人，即Kerry-Ann Barrett（美洲国家组织）和Giacomo Persi Paoli（联合国裁军研究所）为本报告提供的宝贵建议和协助；感谢我们于 2020 年 7 月 3 日举办的利益攸关方多方对话“实施网络规范：关键基础设施保护”的参与者，他们分别是：Oleg Abdurashitov（卡巴斯基）、Kaja Ciglic（微软）、Marc Henauer（瑞士国家网络安全中心）、Wolfram von Heynitz（德国联邦外交部）、Daniel Klingele（瑞士联邦外交部）、Timo S. Koster（荷兰外交部）、Chris Kubecka (HypaSec) 和 Andre Salgado（花旗集团）。同样感谢来自卡巴斯基的 Evgeny Goncharov、Gleb Gritsai 和 Anastasiya Kazakova 提供的行业洞察。

出版物设计与排版：Eric M. Schulz; Kathleen Morf
图表：Uros Podgorelec

说明

目录

作者简介

安德拉兹·卡斯泰利奇 (Andraz Kastelic) 是裁研所“安全与技术项目”网络稳定研究组首席研究员。在加入裁研所之前，他曾在世界多地的国际组织和研究机构担任不同的研究职位。

联合国裁军研究所简介

联合国裁军研究所（裁研所） 是联合国系统内由自愿捐款资助的自治机构。作为全球范围内少数几个专注于裁军领域的政策研究所之一，裁研所在裁军和安全问题方面发展新观点并促进对话和行动。裁研所总部设在日内瓦，旨在协助国际社会发展实际、创新的想法，以找到应对关键安全问题的解决方案。

首字母缩略词

GGE	政府专家组
ICT	信息和通信技术
OEWG	不限成员名额工作组
UN	联合国
UNIDIR	联合国裁军研究所

执行摘要

恶意网络行动对关键基础设施构成威胁，进而危及社会福祉。重大事件可能会影响国家稳定并危及国际和平与安全。

针对关键基础设施的网络威胁的复杂性和有效性日益激增。为此，国际社会利用各国在网络空间的预期行为规范来促进合作。本报告调查了有关敦促各国在针对关键基础设施的恶意网络行动发生时，响应国际援助或缓解请求的相应规范。该规范由联合国关于从国际安全角度看信息和电信领域发展的政府专家组于 2015 年提出。[1]

报告建议各国和国际社会应采取下列措施以执行这一规范：

- 各国应制定本国和国际关键基础设施的明确定义，确定产品或服务符合关键基础设施定义的部门，并维护关键资产清单。作为一项建立信任措施，应与国际社会分享此类定义和划分。
- 各国应在相关国内参与者之间建立危机应对网络。
- 国际社会应建立国家主管单位内单一联络点网络，并授权这些联络点与国际对口单位联系。
- 各国应通过国际网络安全演习，定期测试其与其他国家通信的能力，及其响应援助和缓解请求（特别是通信渠道、协议和程序）的能力。

1 联合国大会（2015b，III：第 13(h) 段）。

- 发出援助或缓解请求时，各国不需要寻求制定通用国际协议，但应在相关国际和国内背景下，遵循关于事件报告的现有最佳实践。
- 可能参与合作应对针对关键基础设施的恶意网络行动的所有国家，都应使用预先建立的国内多方利益攸关方危机解决方案网络，并在此类网络行动中依靠国家及非国家行为体提供的专业缓解技能。
- 需要注意的是，援助和缓解的规范性预期视具体情况而定。出现针对关键基础设施的恶意网络行动时，恶意操作发起国（即发动国）应采取合理的措施，终止相关网络行动，或者最大限度地减少在该网络行动中起中心作用的恶意代码的传播。
- 任何收到援助请求的国家都应尽最大努力，按照受影响国家要求的形式提供援助。援助的概念不仅限于针对恶意网络行动的直接行动，还包括旨在最大限度地减轻针对关键基础设施的网络行动后果的任何形式的帮助。

1. 了解背景和问题

针对关键基础设施（即，对于维持社会福祉至关重要的功能所必需的所有资产[2]）的恶意网络行动，不仅对目标国的福祉构成威胁，而且还会危及国际和平与安全[3]。这些部门通常定义为关键基础设施，包括能源、运输、医疗保健、政府、粮食生产和供应、供水、金融服务、电信以及关键制造业。[4]

针对影响关键基础设施的网络事件，尽管很难可靠地确定其具体程度和影响，但一些记录的实例证明了此类事件的破坏潜力。鉴于关键基础设施的基本性质，相关网络事件可能会给我们的社会带来可怕的后果，包括经济损失、物质损失，甚至还包括人身损害。

2015年，联合国关于从国际安全角度看信息和电信领域发展政府专家组(GGE)提出了一项国际规范，旨在敦促各国在发生针对关键基础设施的网络行动时采取国际合作。该报告的目的是协助理解如何实施上述规范；该报告的结构如下：

- 第一章的余下部分将详细介绍保护关键基础设施免遭网络威胁时所面临的挑战，

  并将概述上述规范。

- 第二章将列举各国在发生网络事件之前就应考虑采取的措施。

- 第三章将就需要从国际层面采取的行动提供相关建议。

- 第四章将提出在发生网络事件之后落实政府专家组规范的具体措施。

- 第五章将指出一些尚待解决的问题，并为未来开展国际讨论或研究提供方向。

1.1 影响关键基础设施的网络事件普遍存在

最近，有几次臭名昭著的网络行动破坏了多个关键基础设施。[5] 但这类事件的确切数目仍然很难确定，因而这类事件是否会变得越来越普遍或破坏性越来越大，也很难确定。造成这一计算困难的因素包括：

---

2 国际上没有达成对关键基础设施的统一定义。该报告中采用了由欧洲联盟理事会发起的现行定义（2008年，第 2(a)条），同时还给出了一些其他案例（见第 2.1 节）。

3 不限成员名额工作组（2021年，第 18 段）。

4 关于哪些部分可以认定为关键基础设施，这将取决于具体的环境。参见第 2.2 节。

5 例如见 Steffen (2016)，关于一系列针对德国医院的网络行动的报道；Gallagher (2020)，关于针对世界各地医疗机构的网络行动的报告；US Cybersecurity and Infrastructure Security Agency (2020)，关于网络行动导致天然气压缩设施遭受产能损失和收入损失的报道；以及 Statt (2021)，关于一次网络行动干扰了一家水处理工厂的报道。

- 各个国家和地区的定义不同
- 衡量网络行动频率和影响的方法不同
- 网络行动的实际数量存在较大不确定性

量化方面造成挑战的第一个原因是，关键基础设施的概念还没有明确或通用的定义；其意义在很大程度上取决于各个国家具体国情。例如，一些国家的国内生产总值中有相当大一部分依赖旅游业，因而可能将支撑旅游业的基础设施视为至关重要[6]，但该项基础设施对其他国家可能就没有那么重要。因此，任何统计数据中如果存在针对通用定义的“关键基础设施”的网络事件趋势，都应该谨慎看待。

此外，关键基础设施也是一个多层面的概念，不同部门会表现出不同的网络事件趋势。如果直接说针对关键基础设施各个部门的恶意网络行动正在增加或减少，会过于笼统：要全面评估威胁状况的变化，需要进行更加具体、针对特定部门的分析。

最后，许多影响关键基础设施的恶意网络行动可能未被发现，或未能得到报告。因此，有记录的影响关键基础设施的网络事件数量可能多于可用统计数据和报告中显示的数量。卡巴斯基的报告称，大多数影响关键基础设施的网络事件仍未得以披露与告知公众，这可能是出于基础设施运营者的明确要求，也可能是因为地方立法部门禁止基础设施运营者披露此类事件。[7] 同样，红十字国际委员会强调“很难评估有多少（网络）行动未被发现，攻击者真正侵入基础设施的范围有多大，或者攻击者是否已经建立了后门以备未来使用，例如作为切断开关。”[8]

因此，不同安全公司的调查反映不同的、有时甚至相互矛盾的发展趋势，也就不足为奇了。例如：

- IBM 报告称，2019年发生的影响（关键基础设施经常使用的）工业控制系统和运营技术网络的网络事件数量超过了过去三年总和。[9]
- 卡巴斯基的研究则表明，2019 年下半年和 2020 年上半年，针对工业控制系统计算机的恶意代码攻击比例实际上有所下降。这一趋势直到 2020 年下半年才出现逆转。[10]

---

6 例如见Republic of Mauritius (2014)。

7 与Kaspersky实验室 ICS CERT 负责人 Evgeny Goncharov 的私人通信，2020 年 10 月。

8 Gisel & Olejnik (25 ,2019).

9 IBM X-Force Incident Response and Intelligence Services.

10 Kaspersky ICS CERT (2020b, 15 ,13); Kaspersky ICS CERT (2021).

1.2 关键基础设施中断所造成的后果

无论针对关键基础设施的网络行动的确切数量如何，已经有足够多的真实事件可证明各国对保障日益互联的关键基础设施安全性的广泛关切，是有所依据的。例如，在2020年初，一场针对捷克布尔诺大学医院的恶意网络行动迫使该医院暂停原定的手术，并将病人紧急转移至附近的医院。[11] 在此四年前，乌克兰电网公司报告称，一场针对其计算机、监控和数据采集系统的网络行动造成了长达数小时的网络中断。约有22.5万用户遭受电力短缺。[12]

并非所有针对关键基础设施的网络行动都会造成关键服务中断，但这些行动确实有可能造成严重的后果。例如，2020年4月，以色列当局报告了一起针对该国水处理系统的网络行动，此次行动试图破坏该地区的水网。2021[13] 年初，位于美国佛罗里达州的一所水处理设施也曾发生类似事件。[14]

过去十年中，越来越多的国家政府与私营企业[15] 和安全专业人员[16]一样，将这类事件认定为属于最突出的网络安全问题。2015年，政府专家组在其报告中指出，“针对关键基础设施的有害的[信息和通信技术]攻击存在真正、重大的风险。”[17]

按照定义，破坏关键基础设施可能会造成广泛的后果，危及社会所依赖的重要功能，并有可能造成实质破坏和人身伤亡。[18] 例如，一场针对关键能源分配要素的有效网络行动，至少在理论上，可能会导致整个国家电力中断。[19] 上述针对乌克兰电力供应系统的网络行动的确切后果虽尚不明确，但过去发生在其他地区[20] 和国家范围[21] 的停电事件所带来的经济后果已经得到充分证实。同样得到证实的是，停电会导致非意外死亡率的上升。[22]

针对其他基础设施的网络行动可能不会直接造成人身伤害，但有可能会严重削弱社会。例如，如果通过恶意使用信息和通信技术(ICT)来攻击各国国内和国际金融系统，就有可能会“危及金融稳定”[23]进而危及到依赖稳定金融流来运转的社会各个方面。2007年针对爱沙尼亚银行部门的网络行动导致人们无法使用网上银行。尽管该国的计算机网络基础设施没有受到机械性损坏，但由于该国97%的银行交易都发生在网上[24]，爱沙尼亚据称经历了临时瘫痪。[25]

---

11 Khalili (2020).

12 Lee et al. (2016).

13 Cimpanu (2020).

14 Statt (2021).

15 Siemens Gas & Power (2019).

16 欧洲网络与信息安全局（2019年, 109）；Security Magazine (2020)。

17 联合国大会（2015b，II：第 4 段）。

18 在 2020 年从国际安全角度看信息和电信领域发展不限成员名额工作组会议上，各国强调，针对关键基础设施的攻击“不仅会对安全构成威胁，而且危及经济发展和生计，最终威胁到个人的安全和福祉”（不限成员名额工作组，2020年，第22段）。

19 Smith et al. (2019).

20 Shuaia et al. (2018).

21 Schmidthaler & Reichl (2016).

22 Anderson & Bell (2012).

23 G-20（2017 年，第 7 段）。

1.3 管理针对关键基础设施的网络威胁时所面临的挑战

随着网络威胁形势的不断演变，发生重大基础设施事件后产生可怕后果的风险也在加剧，其特征包括以下一系列因素：

- 新型的和日益复杂的攻击。[26] 恶意行为者不断设计新的攻击载体并开发相应的攻击手段。目前，针对关键基础设施的恶意软件正变得越来越有目标针对性，因而也越来越复杂。
- 攻击面迅速扩大。[27] 这主要源于关键基础设施资产中使用的信息和通信技术系统的互联性日益增强。 为应对2019冠状病毒病大流行而实施的远程办公政策进一步加速或加剧了这一问题。[28]
- 现存过时的系统对新的威胁没有足够的抵御力，导致关键基础设施脆弱性不断扩大。例如，根据美国国会的一份报告，作为关键基础设施的组成部分，工业控制计算机系统是“特定的漏洞点，因为过去没有将这些系统的网络安全视为首要考虑的事项”。[29] 微软[30]和相关学术成果[31]也得出了类似的评价。
- 用于预防工作的资源不足。[32] 例如，2018年的网络行动严重影响了英国国民医疗服务体系 (NHS) 提供医疗服务的能力[33]， 如果运营商在事件发生前投入资源并及时修补（从而免疫）计算机系统，就可能避免这一事故的发生。[34] 当然，不够审慎负责并不是本例独有的情况；在其他司法管辖区和关键基础设施部门也可以看到这种情况。[35] 据微软统计，71%的工业控制系统都依赖过时的Windows操作系统，微软已不再为这些操作系统定期更新安全补丁。[36]

---

24 Herzog (51 ,2011).

25 Ilves (2007).

26 “威胁的格局变得极其难以绘制。不仅攻击者正在开发新的技术来规避安全系统，而且在有针对性的攻击中，这种威胁的复杂性和精确性也在增加”（欧洲网络与信息安全局，2020c）。正如Kaspersky指出的，“威胁正变得越来越有针对性和集中性，因而也更加多样化和复杂化”（Kaspersky ICS CERT，2020b）。

27 例如，据Bhunia & Tehranipoor (2019, ch. 1)称，“攻击面是所有可能暴露的安全风险的总和。”换句话说，攻击面代表了恶意行动者可以在网络行动的实施过程中加以利用的一组潜在的接入点。另请参见欧洲网络与信息安全局的预测（2020c，10）。

28 例如见US CISA（2020b）。

29 Shea (2004).

30 “工业和关键基础设施环境中使用的操作技术 (OT) 网络过去通常与企业 IT 网络和互联网隔离，但数字化转型提高了这些环境的连通性和设备数量，从而导致了更高的风险。此外，这些环境中许多老旧的物联网 (IoT)/OT 协议和嵌入式设备都是几年前设计的，缺乏加密、强身份验证和硬化软件堆栈等现代控制，因而进一步增加了风险”（微软，2020年，31）。

31 例如，Muthuppalaniappan & Stevenson (2020) 曾指出“医疗保健组织和大学机构往往缺乏防范网络攻击所需的资源”。

32 BBC (2017); Maglaras et al. (42 ,2018).

33 Ghafur et al. (2019).

34 Morse (2017).

35 例如，参阅US DOE (2019)。

36 微软（2020年, 31）。

影响，包括影响范围，都存在不可预测性。关键基础设施之间的相互依赖已得到充分证实，但网络事件却有可能会带来不可预测、影响广泛的负面后果，甚至远远超出一个国家的领土范围。这种相互依赖的影响可以从2006年11月德国电网元件故障中看到，后者造成了欧洲及其他地区20个国家的电力短缺，影响了约1500万户家庭。[37] 尽管这起事件不是网络行动的结果，但它得以说明针对关键基础设施的网络行动可能造成的广泛性破坏。

37 Van der Vleuten & Lagendijk (2010).

1.4 保护关键基础设施：引入规范

前一章描述的所有因素都表明，需要通过国际合作来防止或减轻针对关键基础设施的恶意网络行动。过去十年来，国际社会一直在设法寻求保护关键基础设施，提高（国际）国内安全以及防止对人类可能造成的破坏和损害。其中一个途径着重于网络空间中负责任行为的规范。[38]

为了“减少对国际和平、安全与稳定的风险”[39]，特别是为了最大限度地减少网络恶意行动对关键基础设施的影响，2015年政府专家组提出了关于网络空间中负责任的国家行为的三项具体规范，详细阐述了各国在网络时代针对关键基础设施安全方面的行为期望。这些规范指出各国应：

- 避免对他国管辖范围内的关键基础设施采取网络行动
- 保护本国关键基础设施免受恶意网络攻击
- 考虑在发生针对关键基础设施的网络行动时采取国际合作[40]

有关关键基础设施的其他负责任的国家行为规范

国际社会将关键基础设施的保护置于国际网络安全关切的首位，这一事实也从多个联盟设想和推动类似或相关的规范中得到具体体现。例如，“网络空间信任与安全巴黎倡议”成员承诺，在现有论坛及相关组织、机构、机制和进程中，共同努力，相互协助，落实合作措施，特别是防止可能对个人和关键基础设施造成重大、无差别或系统性损害的恶意网络活动，并从中得以恢复。[41] 这些规范将有助于弥合数字鸿沟，体现睦邻友好，提高事件应对的有效性[42]，并普遍有助于互联世界的稳定与安全。特别是当基础设施的关键要素超出一个国家的边界时就是如此，可见于国际或跨国关键基础设施[43]，例如互联网的公共核心组成部分。[44]

---

38 技术解决方案、国际法、能力建设和建立信任措施等也发挥了重要作用，尽管对这些问题的探讨已超出了本报告的范围。例如，请参见Baker et al.（2020，503）；Gusev（2020，314）；联合国大会（2015b，V）。

39 联合国大会（2015b，第 10 段）。

40 联合国大会（2015b，第 12(f)–(h) 段）。

41 Ministry of Europe and Foreign Affairs, France (2018).

42 NIST (45 ,2012)。

43 不限成员名额工作组（2020年，17）。

44 Government of the Netherlands (2 ,2020 ;2017).

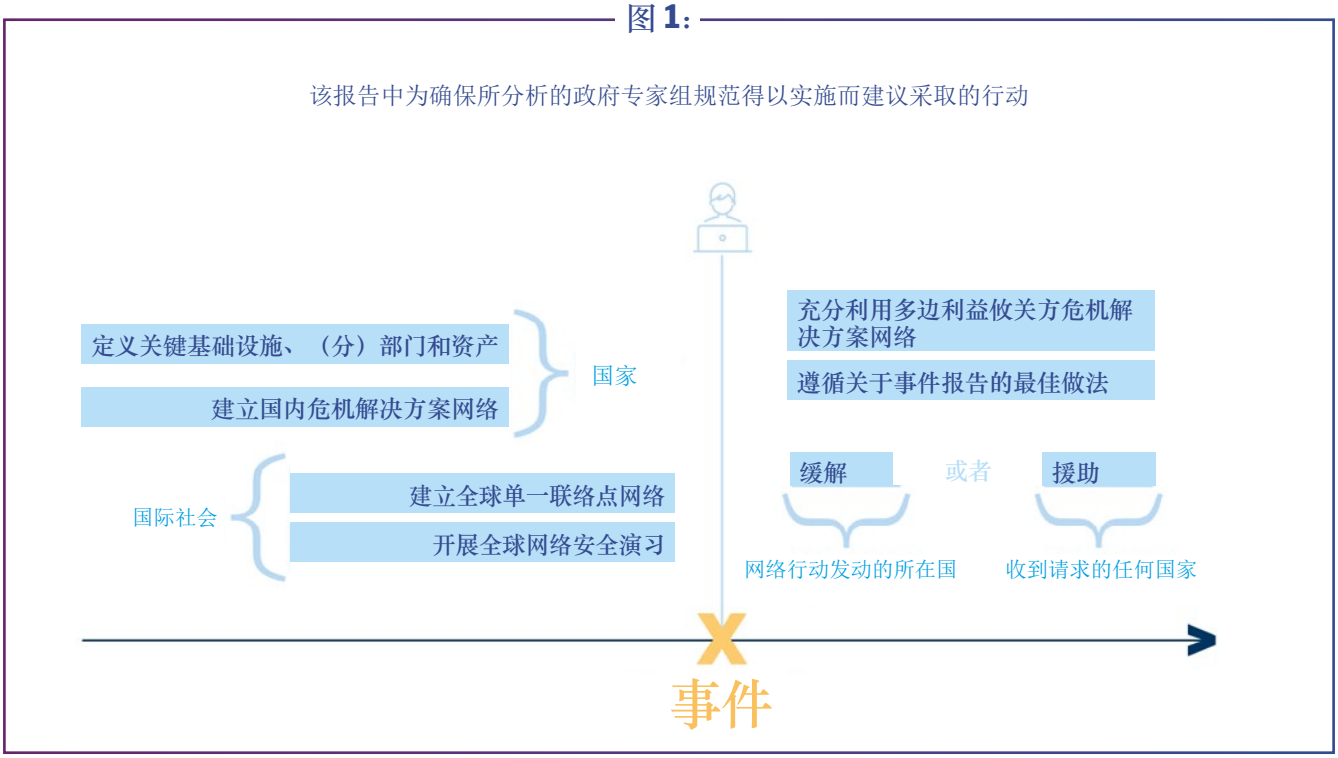
1.5 界定报告的范围

尽管上述2015年政府专家组报告中所包含的三项规范相互关联、相互促进，但**本报告将侧重于国际援助问题**，更具体地说，侧重于各国如何在必要时更好地准备应对请求或回应此类援助。

尽管目前已有很多有关关键基础设施保护的研究[45] ，但在关键基础设施保护范围内，特别是在相关的政府专家组规范范围内，尚未纳入国际援助和缓解的有关要求。尽管这一规范侧重于应对针对关键基础设施的恶意使用信息和通信技术行为，但具体实施还有赖于事件发生之前和之后在国家、地区和国际层面采取的一系列行动和活动。该报告中详细介绍了这些活动，并在图1中作了总结。

该报告讨论的许多行动和活动均涉及提高国家防范、缓解和应对针对关键基础设施的恶意网络行为的能力，以及从中得到恢复的能力。但该报告的重点仍在于国际合作的方式，因此其中所描述的措施不包括在网络能力发展这一更广泛背景下要考虑的全部因素。特别是，该报告未讨论各国为避免发生网络事件可以采取的预防措施。

图 1:



45 例如见欧洲网络与信息安全局（2020a）。

2. 实施规范：全国性准备行动

政府专家组规范的实施需要在发生任何潜在的恶意网络事件之前制定好相关国家结构性框架，以确保做好充分准备。因此，**各国应制定关键国家基础设施的一般定义，确定符合条件的（分）部门，并编制相关资产清单；此外，各国还应建立起国内危机解决网络**。

在确定关键的国家基础设施、部门和资产的过程中寻求指导的国家可以利用国际组织编制的各种援助方案[46]、指导性文件[47] 和现有国家良好做法汇编。[48]

2.1 哪些基础设施确实至关重要?

确定关键基础设施的范围是每个主权国家的特权。这不仅符合国际法中的主权原则，而且也得到了联合国安全理事会第 2341 号决议的明确确认，即“各国有权决定其关键基础设施的构成”。[49]

这就是说，各国可以根据基础设施的目的、所促成的资产或服务中断的影响，或结合这两项原则，将某一项基础设施归类为关键基础设施。[50] 若干区域性组织已做出相应尝试，以具体说明关键基础设施的范围，并可为各国提供指导。例如，《上海合作组织成员国保障国际信息安全政府间合作协定》中将关键基础设施定义为“国家的设施、系统和机构，并且其受到的影响可能会直接影响国家安全，包括个人、社会和国家的安全”。[51] 其他国际和区域性框架也对这一概念做出了类似的一般性定义，例如，美洲国家组织的《保护关键基础设施免受新兴威胁宣言》[52] 和非洲联盟的《网络安全和个人数据保护公约》。[53]

46 例如，请参见美洲国家组织反恐委员会（2015年，第 9 段）

47 经济合作与发展组织（2008b）；Suter（2007）。

48 联合国反恐怖主义委员会执行局与联合国反恐怖主义办公室（2018年）。

49 联合国安全理事会（2017年，2）。某些区域框架，如非洲联盟，已经采用了国家特权（2014年，第 24 条）。例如，另见国际电信联盟（2010年）。

50 联合国反恐怖主义委员会执行局与联合国反恐怖主义办公室（2018年，58）。

51 上海合作组织（2009年，10）。

52 美洲国家组织反恐委员会（2015年，第 11 段）。

53 非洲联盟（2014年，第 1 条）。

2.2 指定相关类别和子类别

确定定义后，**各国应指定被视为关键国家基础设施的合格部门（可能的话，还有分部门）**。尽管各国针对关键基础设施的定义可能会存在一定的一致性，但被认定为关键部门的名单无疑将会有所不同。

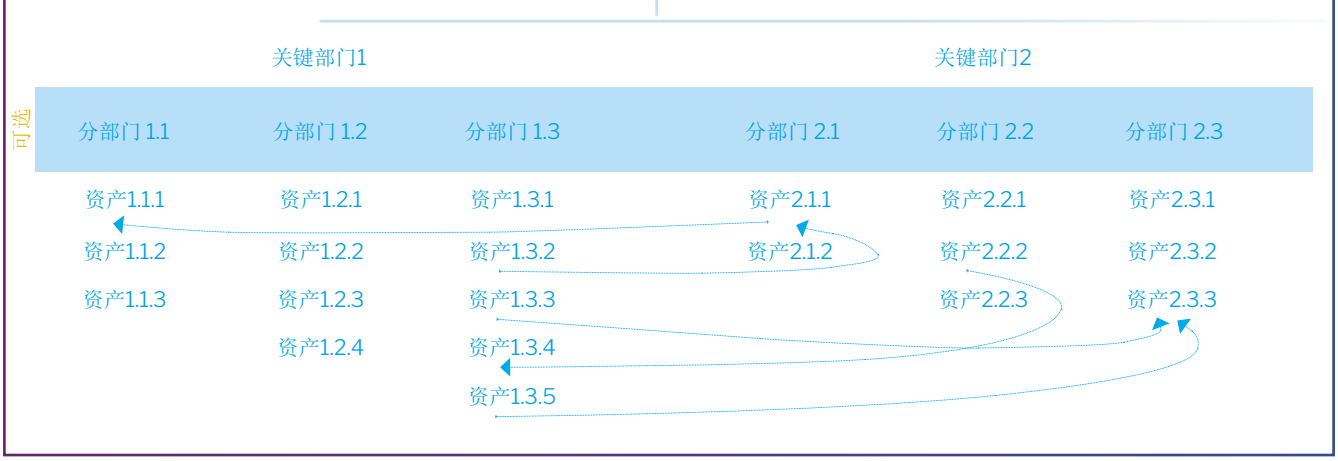
认定的关键部门往往是那些一旦中断就可能会造成人员伤害、广泛的物资损失以及经济和社会不稳定的部门。基于这一背景，大多数国家可能会将能源、金融、水资源和粮食供应、运输、信息和通信技术与政府等部门视为关键部门。[54] 但是，对于旅游业等部门，只有部分经济严重依赖这些行业的国家才有可能将其作为关键部门。[55]

2.3 汇编并维护关键资产清单

各国应汇编并维护关键资产清单。该清单应包括能够让前述确定的关键（分）部门发挥作用的具体实体或资产。考虑到此类清单可能给国家安全造成的敏感影响，各国应确保与包括资产所有者或管理者在内的相关各方进行适当沟通和信息共享。此外，国家还应根据资产的脆弱性和该项资产故障所造成影响的严重性，将清单分成不同的优先级组。清单中还可以包括符合国际关键基础设施条件的资产，这些资产可能不属于某一特定国家的管辖范围，但仍被视为对该国社会运转至关重要。各国须定期审查其关键资产清单以及优先级组分配，以便适应不断变化的国情以及不断演变的网络威胁形势。[56]

图 2：

国家关键基础设施（部门、分部门、资产）的理论结构
结构，体现其相互依赖关系

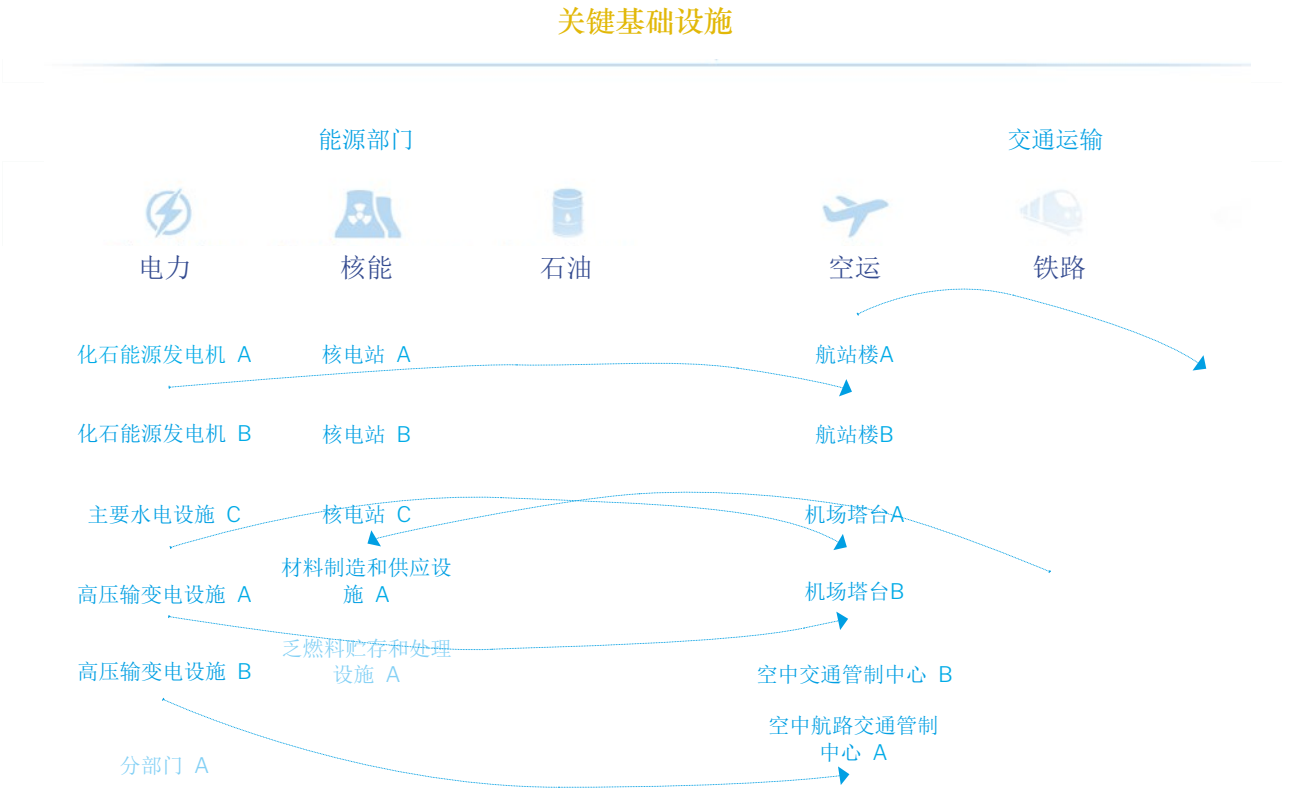


54 例如见Federal Office for Civil Protection, Switzerland (2020)。
55 例如见Republic of Mauritius (2014, 11)。
56 Global Cyber Security Capacity Centre (2016).

某些资产之间可能存在相互依赖关系。例如，如果一次网络行动破坏了某一个高压电力转换设施，那么在缺乏适当冗余设施的情况下，其他部门的资产也很可能会受到严重影响，甚至可能出现瘫痪。

图 3：

国家关键基础设施的结构示例，体现部门、资产和相互依赖关系



技术的内在进步和随之而来的成本上涨，以及2019冠状病毒病大流行驱动的快速数字化进程，这些因素不断提高可视为关键资产的数量，进而扩大关键基础设施的范围。但是，各国应避免将关键国家基础设施的概念扩大到其限度之外，这是因为：关键基础设施的界定范围越广，政府以及关键基础设施运营者保护该基础设施所需的战略投资就越广泛。[57] 因此，各国应考虑将关键基础设施的概念限制在对社会福利真正至关重要的资产和部门。

57 该报告中未讨论有关建议各国投资保护其关键基础设施的规范的实施问题。但有许多试图概述对关键基础设施保护的尝试。例如，参阅Federal Ministry of the Interior, Germany (2009)；经济合作与发展组织（2008a）。

2.4 建立国内危机解决网络

除了界定关键基础设施的概念，各国还应**考虑在相关国内行为者之间建立多边利益攸关方危机解决网络**。这类网络应具有包容性，包括国家实体单位和私营部门的代表，特别是关键基础设施运营者、私营计算机应急响应团队，以及其他愿意并有能力为成功解决影响国内外关键基础设施的网络事件做出贡献的合格行为者。此外，这类网络还能为预防工作做出贡献。

除了已建立的沟通渠道外，为了有效发出国际援助或缓解请求，各国有必要制定有案可查的精简国内协议和程序，以便迅速将信息从关键基础设施运营者或国家主管机构（例如，计算机应急响应小组）传送至国家级联络点。如同国际协作实体一样，国内利益攸关方也应该熟悉议定的协议和流程。[58]

3. 呼吁国际社会参与实施

除了在内部建立国内危机解决网络外，通过国际合作应对针对关键基础设施的恶意信息和通信技术行为的效率、有效性和及时性都将从区域和国际层面的下述行动中获益：

- 增强关键基础设施相关的透明度和信息共享，包括定义和范围
- 在明确的联络点之间建立专门的沟通渠道
- 制定协议和程序，以支持通过各国和国际通信渠道实现信息传送
- 定期进行区域和国际层面演习，以测试联络点网络、协议和程序是否正常运行

3.1 透明度和信息共享

各国应提高透明度，促进在关键基础设施的国家概念化方面定期交流信息。为此，2015年政府专家组敦促国家采取“各国就本国自认为关键的基础设施类别及国家为保护这些基础设施所作的努力自愿提供看法，包括提供信息说明关于保护数据和靠信通技术带动的基础设施的国家法律和政策”的有关措施。[59] 在关键基础设施因恶意网络行动而中断的情况下，信息共享是推动国际合作、援助和缓解的关键要素之一。它不仅支持各国在面临危机时更好地传达其需求，而且还有助于接收援助（或缓解）请求的国家能够更好地评估所需采取的应对措施。

目前有许多区域和国际资源库可以促进这种信息交流。其中一个项目是裁研所的网络政策门户[60]，这是联合国会员国、区域政府间组织和多边框架中国家网络安全政策格局的数字存储库。另一个例子是由国际电信联盟维护的国家网络安全战略库。[61]

59 联合国大会（2015b，第 IV(d) 段）。
60 www.cyberpolicyportal.org
61 国际电信联盟（2020年）。

3.2 单一联络点

在国际社会有关成员之间建立起制度化的沟通渠道，有助于确保在某一行为体关键基础设施遭到破坏时能够有效且迅速地传播信息。**国际社会应致力于建立国家主管实体内单一联络点的全球网络，授权在需要时与其国际对口单位联系**。[62] 这类网络的一个例子是由欧盟《网络与信息安全指令》[63]建立的单一联络点清单，该清单定期更新并可在线免费获取。[64]

2015年政府专家组报告建议各国考虑“在政策和技术层面”建立联络点目录。[65] 在2020年2月从国际安全角度看信息和电信发展不限成员名额工作组辩论中，多个代表团[66] 发言赞成建立全球联络点清单，但没有对本目录中实体的性质或权限达成统一立场。一些代表团主张设立政治联络点；另一些则倾向于建立一份包含代表计算机应急响应实体、执法部门和其他利益攸关方的多个联络点的清单。[67] 工作组最后的实质性报告中建议各国建立一个全球联络点目录。[68]

援助和缓解可以包括多种其他非技术形式。[69] 然而，为了减少危机时期出现混乱和不确定性的风险，建议今后制定的任何联络点清单只包括经正式批准、具有充分技术水平和业务知识、能够请求或协助国际援助和缓解工作的国家实体。

---

62 《关于实施网络规范：关键基础设施保护的多方利益攸关方对话会议纪要》2020 年 7 月 3 日[由作者保存备案]。这一观点也在 2015 年政府专家组报告中得到了推进：参见联合国大会（2015b，IV (a)）。

63 欧洲联盟（2016年，第 8 条）。

64 欧盟委员会（2020年）。另请参见 G2019）7-）；欧洲安全与合作组织常设理事会（2013年，第 8 条）。《网络犯罪公约》也要求各国指定国家联络点，以便打击网络犯罪，尽管略有不同，且范围较窄。参见专家委员会（2004年，第 35 条）。

65 联合国大会（2015b，第 16(a) 段）。

66 阿根廷、澳大利亚、巴西、加拿大、智利、哥伦比亚、厄瓜多尔、爱沙尼亚、法国、加纳、马拉维、马来西亚、墨西哥、新西兰、俄罗斯联邦、斯洛文尼亚、瑞士和阿拉伯叙利亚共和国（Gavrilović，2020）。

67 Gavrilović (2020).

68 不限成员名额工作组（2021年，第 51 段）。

69 参见第 4.3 节。

3.3 开展国家（和国际）网络安全演习

成功的国际合作取决于有效的危机解决网络以及有效的协议和沟通渠道。因此，建议各国**定期开展国家和国际网络安全演习**，测试其沟通或响应援助和缓解请求的能力。

国家网络安全演习将评估和强化国内危机解决方案网络的准备情况，及其向他国传达适当的援助和缓解请求的能力。此外，此类演习还将加强协助他国应对针对关键基础设施的网络行动的能力。[70]

国际网络安全演习还有助于建立各国有效沟通援助或缓解请求的能力，特别是强化各联络点之间的沟通渠道以及所使用的国际协议和程序。此外，国际网络安全演习还有助于各国之间建立信任。例如，国际电信联盟会定期协助各国开展区域网络安全演习。[71]

70 例如，美洲国家组织（2021年）和欧洲安全与合作组织（2018年）支持各国开展国家网络安全演习。

71 国际电信联盟（2021年）。


NEW YORK
SYDNEY

4. 在规范框架内应对网络事件

目前，呼吁开展国际合作以制止针对关键基础设施恶意网络行动的政府专家组规范，尚未明确要求国际社会开展尽职调查，也未要求国际社会主动与受影响的国家进行沟通。根据该规范，关键基础设施受到网络攻击的国家有义务发出适当的援助或缓解请求。

在此背景下，为确保该规范的可操作性，必须确定哪些请求属于“他国关键基础设施受到恶意信息和通信技术行为影响时所提出的适当的援助[或缓解]请求。”[72]

4.1 通过最佳实践指导国际交流

各联络点在交流中应遵循普遍认可的协议和流程。鉴于制定普遍的通信协议和程序时将面临的挑战，**各国应在相关国际和国内背景下，遵循关于事件报告的现有最佳做法**。这将允许有关各方之间开展最佳沟通，从而促进事件的有效解决。

欧盟网络安全局的《事件报告良好做法指南》[73] 和美国计算机应急准备小组的《联邦事件通知指南》[74] 作为事件报告框架的案例，可用于此目的。可用于相同背景的技术协议示例包括《信息交换策略2.0》和《交通灯协议》，这两个方案均由事件响应与安全小组论坛发布。[75]

此外，一份适当的援助和缓解请求中不仅要包括相关事件信息，还应包括接收请求的国家应采取的具体行动建议。

4.2 采取包容性、面向多个利益攸关方的应对方法

参与合作应对针对关键基础设施的恶意网络行动的所有国家都应**使用上述国内多方利益攸关方危机解决网络，并依靠国家及非国家行为者提供的专业缓解技能**。私营部门掌握丰富的网络安全专业知识，并通常控制着关键基础设施的相关技术。因此，任何没有私营部门参与的解决危机的尝试，都可能无法取得理想的结果。[76] 同样，各国必须致力于创建国家协作和危机解决网络，建立明确的沟通渠道，并明确网络成员的分工和责任。

72 联合国大会（2015b，III：第 13 (h) 段）。
73 欧洲网络与信息安全局（2009年）。
74 US-CERT (2015).
75 事件响应与安全小组论坛（2019年）。
76 例如见国际电信联盟等（2018年，44）。

4.3 援助与缓解的区别

根据有关规范的规定，各国应回应“适当的援助请求”或“针对他国关键基础设施的恶意信息和通信技术活动的适当缓解请求”。[77] 收到援助或缓解请求的国家不需要超出其能力范围采取行动；它们只应在当前现有资源下，尽最大努力提供援助。那么，援助与缓解之间有什么区别？

首先，当网络行动的来源无法确定时，或当网络行动是从接收请求国之外的国家的基础设施发出时，**接收援助请求的国家应在其能力范围内提供帮助或支持，以最大限度地减少针对关键基础设施的恶意网络行动所带来的不良后果**。各国还可以提供相关协助，以结束网络行动或强化受影响的关键基础设施的计算机网络系统。援助可以包括各种形式，不仅限于技术援助。例如，如果某一网络行动妨碍了特定国家的电力生产，该国可请求以增加供电的方式提供援助。请求援助时，应由受网络行动影响的国家负责明确需求或指定请求，包括援助的范围和方法。相互交流和合作的各国应在国际主权法原则和由此产生的义务的框架内真诚地开展沟通和行动。

其次，如果向恶意网络行动的来源国（即行动发出的所在国）提交请求，则该国应以尝试缓解网络行动本身作为回应。比援助相比，缓解似乎是一个更狭义的概念，是指限制[78]针对关键基础设施的网络行动的相关措施。因此，缓解很大程度上仅限于技术性质的行动，并与网络行动本身有关。**在这种情况下，应要求行动发出所在国采取合理的措施，终止或尽量减少潜在恶意代码的传播**。尽管其范围小于援助，但缓解指出了行动发出所在国在限制网络行动的传播及其造成的破坏方面可发挥的重要作用。缓解和援助并不相互排斥；被要求缓解来自其领土范围内的网络行动的国家也可以提供援助。

虽说如此，该规范却没有考虑到过境国的作用。过境国的基础设施可能是恶意行动链中的一个重要的有利环节。因此，过境国也可能有能力缓解针对他国关键基础设施的网络行动。国际社会继续在多边论坛上推动关于负责任的国家行为规范的讨论时，可以进一步分析过境国的作用。

---

77 联合国大会（2015b，第 13 (h) 段）。

78 国际法院（1997年，第 80 段）。

最后，关于援助和缓解工作的讨论不应集中在技术归责问题上。在针对关键基础设施的网络行动的即时响应中，只有在可限制正在进行的网络行动的破坏程度情况下，才能开展旨在找寻罪魁祸首的活动。这并不意味着参与这一合作应对的行为者应忽略事件解决阶段发现的任何数字化证据：此类证据在后续阶段可能会有所用处，并将支持相关行为体根据国内刑法或国际法在国家责任范围内采取措施。然而，归责绝不应成为合作各方的核心方向，因为这可能会偏离合作的首要目标，即阻止网络行动的传播，并最大限度地减少其带来的不良后果。

结论

为了最大限度地减少针对关键基础设施的威胁所带来的影响，国际社会力求通过在网络空间领域制定自愿遵循的负责任国家行为规范，以促进和平与安全。2015年，联合国大会通过了由政府专家组制定的一套规范，特别用于促进各国在打击针对关键基础设施的破坏性网络行动方面开展合作，指出各国应响应适当的援助请求，或者某些情况下，为关键基础设施受到恶意信息和通信技术行为的国家采取缓解措施。

为了促进并支持各国实施该规范，本报告中详细阐述了该规范的范围和内容，阐明了规范预期、国家实践以及与该规范相关的新兴良好实践。特别是，该报告建议各国：

- 定义关键基础设施，包括（分）部门和符合条件的资产数据库
- 建立国内多方利益攸关方危机解决方案网络
- 与国际社会分享关键基础设施概念化的信息
- 旨在建立一个全球性的联络点网络
- 定期开展国家（和国际）网络安全演习
- 在提交或响应援助或缓解请求时，遵循相关沟通最佳做法
- 尽最大努力向受影响国家提供所需任何形式的援助，并且在被确认为恶意网络行动发起的所在国时，尽其所能缓解恶意行动本身

但该准则还有几个方面有待于国际社会作进一步详细阐述。因此，各国应继续阐述其对落实该规范的观点，或通过分享实施该规范的良好做法和经验来提供额外的认识。

此外，国际社会应考虑探讨过境国在落实现行规范框架时的作用，特别要重视过境国在发生针对关键基础设施的网络行动时发挥缓解作用的潜力。

国际社会还应考虑确定国际或跨国关键基础设施的概念，明确对不同国家开展打击针对此类基础设施的恶意网络行动的行为期望。

最后，国际社会应考虑如何充分利用当前和未来的能力建设工作[79]，以加强各国的国家能力，使其能够保护自己的基础设施，并帮助缓解针对他国关键基础设施的恶意网络行动或协助有需要的国家。

---

79 联合国大会会议（2015b，第 23 段）。

参考文献

非洲联盟。2014 年。《网络安全和个人数据保护公约》，6 月 27 日。

Anderson, Brooke G., & Michelle L. Bell. 2012. 'Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY.' Epidemiology 23 (2): 189–193. 截至2020年10月24日：https://journals.lww.com/epidem/Fulltext/2012/03000/ Lights_Out_ Impact_of_the_ August_2003_Power.3.aspx

Axelrod, Robert. 1984. The Evolution of Cooperation. New York: Basic Books.

Baker, Thar, Muhammad Asim, Áine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi & Mohammad Hammoudeh. 2020. 'A Secure Fog - Based Platform for SCADA - Based IoT Critical Infrastructure.' Special Issue: Software Tools and Techniques for Fog and Edge Computing 50 (5): 503. 截至2020年10月21日 https://onlinelibrary.wiley.com/doi/ abs/10.1002/spe.2688

BBC. 2017. 'NHS "Could Have Prevented" WannaCry Ransomware Attack.' BBC News, 27 October. 截至2020年10月25日： https://www.bbc.com/news/technology-41753022

Bhunia, Swarup, & Mark Tehranipoor. 2019. Hardware Security: A Hands-on Learning Approach. Cambridge: Elsevier.

Burgstaller, Markus. 2005. Theories of Compliance with International Law. Leiden: Brill Academic.

Cimpanu, Catalin. 2020. 'Two More Cyber-Attacks Hit Israel's Water System.' ZDNet, 20 July. 截至2020年10月21日： https://www.zdnet.com/article/ two-more-cyber-attacks-hit-israels-water-system

欧洲联盟理事会(CoE)。2004年。《网络犯罪公约》，欧洲电信标准第 185 条。

欧洲联盟理事会，2008 年。欧洲联盟理事会 2008 年 12 月 8 日关于确定和指定欧洲关键基础设施以及评估改善其保护需求的第2008/114/EC号指令。

———. 2017年。《执法信息交流手册》。6261/17,，7月4日。截至2021年3月6日：https://data.consilium.europa.eu/doc/document/ST-6261-2017-INIT/en/pdf

Downs, George W., & Michael A. Jones. 2002. 'Reputation, Compliance, and International Law.' Journal of Legal Studies 31 (S1): S96.

Edison Electric Institute. 2018. 'Electric Distribution System Cybersecurity Is Critical in Today's Interconnected Society.' April. 截至2020年10月25日：https://www.eei.org/issuesandpolicy/ Documents/EEI_Cybersecurity_Considerations_Distribution.pdf

欧盟委员会 (EC)。2020 年。"SPOCS 清单和主管当局——NIS 指令"。截至 2020 年 10 月 21 日：http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53682

欧洲联盟 (EU)。2016 年。欧洲议会和欧洲理事会 2016年 7 月 6 日关于提高欧盟网络和信息系统的通用安全水平的第(EU) 2016/1148号指令。

欧盟网络安全局 (ENISA)。2009 年。“报告安全事故的良好实践”。12 月。截至 2020 年 12月 21 日：https://www.enisa.europa.eu/publications/ good-practice-guide-on-incident-reporting-1/at_download/fullReport

——— 。2019年。《2018 年 ENISA 威胁格局报告》。雅典：ENISA。截至 2020 年 10 月 21 日：https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

——— 。2020a。“关键基础设施和服务”。截至 2020 年 10 月 21 日：https://www. enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=publications

——— 。2020b。《部门/专题威胁分析：ENISA 威胁格局》。雅典：ENISA。截至 2020 年 10 月 21 日：https://www.enisa.europa.eu/publications/ sectoral-thematic-threat-analysis

——— 。2020c。《年度回顾：ENISA 威胁格局》。雅典：ENISA。截至 10 月 24 日：https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

Federal Ministry of the Interior, Germany. 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin: Government of Germany. 截至10月 25日： https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html

Federal Office for Civil Protection, Switzerland. 2020. ‘Critical Infrastructures.’ 截至2020年10月 21日：https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html

Forum of Incident Response and Security Teams (FIRST). 2019. ‘Information Exchange Policy 2.0 Framework Definition.’ 截至2020年10月 21日：https://www.first.org/iep/ iep_framework_2_0

———. 2020. ‘Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance – Version 1.0.’ 截至2020年10月 21日：https://www.first.org/tlp

G-20. 2017. ‘Communiqué – G20 Finance Ministers and Central Bank Governors Meeting.’ Baden-Baden, Germany, 17–18 March 2017.

G-7. 2019. ‘Cyber Norm Initiative Synthesis of Lessons Learned and Best Practices.’ 26 August. 截至2020年10月 21日：https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf

Gallagher, Ryan. 2020. ‘Hackers “Without Conscience” Demand Ransom from Dozens of Hospitals and Labs Working on Coronavirus.’ *Fortune*, 1 April. 截至10月 21日：https://fortune. com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus

Gavrilović, Andrijana. 2020. ‘Confidence-Building Measures.’ Geneva Internet Platform, February 2020. 截至2020年10月 21日：https://dig.watch/sessions/confidence-building-measures

Ghafur, Saira S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin. 2019. ‘A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.’ *NPJ Digital Medicine* 98 (2).

Gisel, Laurent, & Lukasz Olejnik. 2019. *The Potential Human Cost of Cyber Operations*.

日内瓦：国际红十字委员会。截至 2020 年 10 月 21 日：https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf

全球网络空间稳定委员会。 2019年。《推进网络稳定》。最终报告，11月。截至2020年10月21日： https://cyberstability.org/wp-content/ uploads/2020/02/GCSC-Advancing-Cyberstability.pdf

Global Cyber Security Capacity Centre. 2016. *Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition.* Oxford: University of Oxford. 截至2020年10月21日： https:// gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

Government of Australia. 2019. 'Australian Implementation of Norms of Responsible State Behaviour in Cyberspace.' 截至2020年10月21日：https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf

Government of Canada. 2019. 'Canada's Implementation of the 2015 GGE Norms.' 截至2020年10月21日： https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf

Government of the Netherlands. 2017. 'Building Digital Bridges: International Cyber Strategy.' 2 February. 截至2020年10月21日：https://www.government.nl/documents/ parliamentary-documents/2017/02/12/international-cyber-strategy

———. 2020. 'The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behav- ior in cyberspace in the context of international security."' February. 截至2020年10月21日：https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg- kingdom-of-the-netherlands.pdf

Gusev, Alexey. 2020. 'New Cyberattacks Vectors of Russian Critical Infrastructure Enterprises: Domestic Private Banking Sector View within AI Protection Methods.' *Procedia Computer Science* 169: 314. 截至2020年10月21日：https://www.sciencedirect.com/science/article/pii/S1877050920303124

Guzman, Andrew T. 2002. 'A Compliance Based Theory of International Law.' *California Law Review* 90(6): 1823. 截至2020年10月21日：https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1216&context=gjicl

Herzog, Stephen. 2011. 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.' *Journal of Strategic Security* 4(2): 49.

IBM X-Force Incident Response and Intelligence Services. 2020. 'X-Force Threat Intelligence Index 2020'. February. 截至2020年10月21日：https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map

Ilves, Toomas Hendrik. 2007. 'Address by Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly (25 September 2007)'. 截至2021年1月17日：https://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

美洲反对恐怖主义委员会 (CICTE) 。2015 年。《宣言：保护关键基础设施免遭新出现的威胁》。CICTE 文件 CICTE/doc.1/15，2015年3月23日。截至 2020 年 10 月 21 日：https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20 DECLARATION%20CICTE00955E04.pdf

国际法院 (ICJ) 。1997 年。 *Gabčíkovo-Nagymaros* 项目案（匈牙利/斯洛伐克）判决，《1997 年国际法院案例汇编》，第 7 页。

国际电信联盟 (ITU)。2010 年。《问题 22-1：保护信息和通信网络：发展网络安全文化的最佳实践》（最终报告）。日内瓦：ITU。截至 2020 年 10 月 25日：https://www.itu.int/pub/D-STG-SG01.22-2010

———。2020 年。“国家网络安全战略库”。截至 2020 年 12 月 17 日：https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

———。2021 年。“网络演练”。截至 2021 年 2 月 11 日：https://www.itu.int/en/ITU-D/Cybersecurity/ Pages/cyberdrills.aspx

国际电信联盟、世界银行、英联邦秘书处、英联邦电信组织、北约卓越网络防御合作中心。2018 年。《制定国家网络安全战略指南：网络安全的战略性参与》。日内瓦：ITU。

国际刑事警察组织。2020年。“预防犯罪和保护警察：国际刑警组织对COVID-19全球威胁的评估。” 4月6日。截至2020年10月21日： https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

Kaspersky ICS CERT. 2020a. ‘Cyberthreats for ICS in Energy in Europe. Q1 2020.’ 截至2020年10月21日：https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-2020Q1-Threats- to-energy-industry-in-Europe.pdf

———. 2020b. ‘Threat landscape for industrial automation systems H1 2020’. September 24. 截至2020年10月21日：https://ics-cert.kaspersky.com/media/ KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

———. 2021. ‘Threat landscape for industrial automation systems. Statis- tics for H2 2020’. March 25. 截至2021年3月28日：https://securelist.com/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/101299

———. Forthcoming. ‘Threat Landscape for ICS in Water Management Industry.’

Khalili, Joel. 2020. ‘Coronavirus Hospital Suspends Activity over Cyberattack.’ *Techradar.Pro*, 16 March. 截至2020年10月21日：https://www.techradar.com/news/ coronavirus-hospital-suspends-activity-over-cyberattack

Lauber, Jurg. 2019. ‘Chair’s Summary: Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.’ 5–6 December. 截至2020年10月21日：https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf

Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' SANS & E-ISAC, 18 March. 截至2020年10月21日：https://ics.sans.org/ media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Maglaras, Leandros A., Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras & Tiago J. Cruz. 2018. 'Cyber Security of Critical Infrastructures.' *ICT Express* 4: 42–45.

Microsoft. 2020. 'Microsoft Digital Defense Report' September. 截至2020年10月21日：https://www.microsoft.com/en-us/download/details.aspx?id=101738

Ministry of Europe and Foreign Affairs, France. 2018. 'Paris Call for Trust & Security in Cyberspace.' 11 December. 截至2020年10月21日：https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Morse, Amyas. 2017. *Investigation: WannaCry Cyber Attack and the NHS*. London: National Audit Office. 截至2020年10月21日：https://www.nao.org.uk/report/ investigation-wannacry-cyber-attack-and-the-nhs

Muthuppalaniappan, Menaka, & Kerrie Stevenson. 2020. 'Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.' *International Journal for Quality in Health Care* 33 (1). 截至2020年10月25日： https://academic.oup.com/intqhc/advance-article/doi/10.1093/intqhc/mzaa117/5912483

Nebenzia, Vassily. 2020. 'Statement by Vassily Nebenzia, Permanent Representative of the Russian Federation to the United Nations, at the "Arria-formula" VTC of the UNSC Members on Cyber-Attacks against Critical Infrastructure.' Permanent Mission of the Russian Federation to the United Nations, 26 August. 截至2020年10月21日：https://russiaun.ru/en/news/ arria_260820

从国际安全角度看信息和电信领域发展的不限成员名额工作组(OEWG)。2020 年。"从国际安全角度看信息和电信领域发展的不限成员名额工作组报告的第二份 '初稿'"。 5 月 27 日。截至 2020 年 10 月 21 日：https://front.un-arm.org/wp-content/ uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

———。2021 年。2021 年 3 月 10 日，"最终实质性报告"。联合国文件 A/AC.290/2021/ CRP.2。截至 2021 年 3 月 12 日：https://front.un-arm.org/wp-content/uploads/2021/03/ Final-report-A-AC.290-2021-CRP.2.pdf

经济合作与发展组织 (OECD)。2008a。"'关键基础设施'的保护和与国家安全相关投资政策的作用"。5 月。截至 2020 年 10 月 21 日：https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

———。2008b。《OECD 关于保护关键信息基础设施理事会的建议》。OECD文件C(2008)35。巴黎：OECD。截至 2020 年 10 月 21 日：http://www.oecd.org/sti/40825404.pdf

欧洲安全与合作组织 (OSCE) 常设理事会。2013 年。"第1106 号决议：OSCE 为减少使用信息和通信技术造成的冲突风险而采取的一套初步建立信任措施。"OSCE 文件 PC.DEC/1106，2013 年 12 月 3 日。

———。2018年。“OSCE 在哈萨克斯坦举行关于保护关键能源基础设施免受网络恐怖袭击的国家层最高演习。”11 月 29 日。截至 2021 年 2 月 10 日：https://www.osce.org/programme-office-in-astana/404594

美洲国家组织 (OAS)。2021 年。“网络安全计划”。截至 2021 年 2 月 10 日：http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Permanent Mission of the Republic of Indonesia to the United Nations, New York. 2020. ‘Statement by H.E. Ambassador Dian Triansyah Djani Permanent Representative of the Republic of Indonesia: United Nations Security Council Arria-formula Meeting “Cyber Stability, Conflict Prevention, and Capacity Building.”’ New York, 22 May. 截至2020年10月21日：https://kemlu.go.id/newyork-un/en/read/united-nations-security-council-arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building/3645/ etc-menu

President’s National Infrastructure Advisory Council (NIAC). 2017. ‘Security Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.’ August. 截至2020年10月21日：https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf p2

Republic of Mauritius. 2014. ‘National Cyber Security Strategy 2014 – 2019.’ 截至2020年10月21日：https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

Schmidthaler, Michael, & Johannes Reichl. 2016. ‘Assessing the Socio-Economic Effects of Power Outages Ad Hoc.’ *Computer Science – Research and Development* 31: 157–61. 截至2020年10月21日： https://link.springer.com/article/10.1007/s00450-014-0281-9

Security Magazine. 2020. ‘Critical Infrastructure Cyberattacks a Greater Concern Than Enterprise Data Breaches.’ Security Magazine, 26 March. 截至2020年10月25日：https://www. securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches

上海合作组织。2009 年。“上海合作组织成员国关于加强国际信息安全合作的协定”。 6 月 16 日。截至 2020 年 10 月 21 日：http://eng.sectsco.org/load/207508

Shea, Dana A. 2004. ‘Critical Infrastructure: Control Systems and the Terrorist Threat.’ CRS Report for Congress, RL31534, 20 January. 截至 2020 年 10 月 21 日：https://apps.dtic.mil/sti/ pdfs/ADA467307.pdf

Shuaia, Mao, Wang Chengzhib, Yu Shiwena, Gen Haoa, Yu Jufanga & Hou Hui. 2018. ‘Review on Economic Loss Assessment of Power Outages.’ *Procedia Computer Science* 130: 1158–63. 截至 2020 年 10 月 25 日：https://www.sciencedirect.com/science/article/pii/S1877050918305131

Siemens Gas & Power. 2019. *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* Houston: Siemens. 截至 2020 年 10 月 21 日：https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

Smith, Scott, Fabiola Sanchez & Christopher Torchia. 2019. 'Venezuela Buckles under Massive Power, Communications Outage.' *Associated Press*, 9 March. 截至 2020 年 10 月 21 日：https:// apnews.com/6ba2f69b77e2457da64593a7b8eced16

Statt, Nick. 2021. 'Hackers Tampered with a Water Treatment Facility in Florida by Changing Chemical Levels.' The Verge, 8 February. 截至 2021年 2 月 8 日： https://www.theverge.com/2021/2/8/22273170/hackers-water-treatment-facility-florida-hacked-chemical-levels-changed

Steffen, Sarah. 2016. 'Hackers Hold German Hospital Data Hostage.' DW, February 25. 截至 2020 年 10 月 21 日：https://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

Suter, Manuel. 2007. *A Generic National Framework for Critical Information Infrastructure Protection (CIIP).* Zurich: Center for Security Studies. 截至 2020 年 10 月 25 日：https://www.itu.int/ ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

联合国国际组织会议。1945年。《联合国宪章及国际法院规约》。旧金山，6月26日。

联合国反恐怖主义委员会执行局(UNCTED) 和联合国反恐怖主义办公室 (UNOCT)。2018年。《保护重要基础设施免遭恐怖袭击：良好做法简编》。6月。截至 2020 年 10 月 21 日：https://www.un.org/sc/ ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_ june_2018_optimized.pdf

联合国大会 (UNGA)。1970年。《关于各国依联合国宪章建立友好关系及合作之国际法原则之宣言》，UN 文件A/PV.1883，1970年10月24日 。

———。1999年。《审查大会第十届特别会议通过的建议和决定的执行情况：裁军审议委员会的报告》，UN文件A/51/182/Rev.11999年6月9日。截至 2020 年 10 月 21 日：https://www.un.org/disar- mament/wp-content/uploads/2019/09/A-51-182-Rev.1-E.pdf page=53

———。2001年。《国家对国际不法行为的责任》，UN文件A/ RES/56/83，2001年1月28日。

———。2010年。《从国际安全角度看信息和电信领域发展政府专家组报告》，UN文件A/65/201，2010年7月10日。

———。2015a。《从国际安全角度看信息和电信领域发展》，UN文件A/RES/70/237，2015年12月23日。

———。2015b。《从国际安全角度看信息和电信领域发展政府专家组报告》，UN文件A/70/174，2015年7月22日。

联合国安全理事会 (UNSC)。2017年。UN文件S/RES/2341 （2017年），2017年2月13日。

United States Computer Emergency Readiness Team (US-CERT). 2015. 'US-CERT Federal Incident Notification Guidelines.' 截至2021年3月6日：https://us-cert.cisa.gov/sites/default/files/ publications/Federal_Incident_Notification_Guidelines_2015.pdf

United States Cybersecurity and Infrastructure Security Agency (CISA). 2020a. 'Alert (AA20-049A) Ransomware Impacting Pipeline Operations.' Department of Homeland Security, 18 February. 截至2020年10月21日：https://us-cert.cisa.gov/ncas/alerts/aa20-049a

———. 2020b. 'Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response.' Version 4.0, 18 August. 截至2021年2月11日：https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essen- tial_Critical_Infrastructure_Workers_Final3_508_0.pdf

United States Department of Energy (DOE). 2019. *Evaluation Report.* DOE-OIG-20-12, 19 No- vember. Washington, DC: US DOE. 截至2020年10月25日：https://www.energy.gov/sites/prod/ files/2019/11/f68/DOE-OIG-20-12.pdf

United States Department of Homeland Security. 2020. 'National Infrastructure Protection Plan International Issues for CI/KR Protection.' 截至2020年10月25日：https://www.dhs.gov/xlibrary/assets/nipp_international.pdf

United States National Institute of Standards and Technology (NIST). 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61, Revision 2. Gaithersburg: US NIST. 截至2020年10月25日：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Van der Vleuten, Erik, & Vincent Lagendijk. 2010. 'Transnational infrastructure vulnerability: The historical shaping of the 2006 European "Blackout."' *Energy Policy* 38 (4): 2042–2052.

Vidyarthi, Apratim, & Anastasiya Kazakova. 2020. 'What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance,' background paper, *IGF 2020 Best Practice Forum on Cybersecurity*, September 2020.

通过国际合作减少针对关键基础设施的网络行动

规范性预期及新兴良好实践

恶意网络行动将对关键基础设施构成威胁，进而危及社会福祉。重大事件可能会影响国家稳定并危及国际和平与安全。针对关键基础设施的网络威胁的复杂性和有效性日益激增。对此，国际社会通过各国在网络空间的预期行为规范来促进合作。本报告分析了敦促各国在发生针对关键基础设施的恶意网络行动时响应他国援助或缓解请求的相关规范。该规范由联合国从国际安全角度看信息和电信领域发展的政府专家组于2015年提出。

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH