新冠肺炎疫情期间针对全球医疗卫生系统的网络攻击：问题及应对

甘肃政法大学法学院副教授

崔　岩

一、问题缘起

新冠肺炎疫情期间，捷克共和国、英国、美国、法国、西班牙、澳大利亚、泰国等许多国家的医疗机构遭到网络攻击。最令人担忧的是针对处于抗击新冠肺炎疫情第一线的医疗机构和人员的网络攻击，包括世界卫生组织等国际组织以及世界各地的医院和医学研究机构（包括牛津大学的机构）。网络攻击者进行网络行动以窃取新冠肺炎疫情期间疫苗研究并干扰疫苗开发、生产和推广。这些网络攻击削弱了关键医疗机构的运作能力，减缓了基本医疗物资和信息的分发，扰乱了对患者的护理甚至危及人类生命。新冠肺炎疫情期间保护医疗服务或医疗设施免受任何形式的网络攻击的问题凸显其重要性。

二、医疗卫生系统遭受网络攻击的国际法问题

（一）国际法层面：

《牛津声明》

2020年5月21日和7月31日，牛津大学道德、法律与武装冲突研究所率头发布两份关于新冠疫情期间医疗网络受国际法保护的《第一份牛津声明》和《第二份牛津声明》，获得了众多国际法学者的签名支持，并产生了相当大的影响力。**两份声明保护医疗设施免受恶意网络行动有关的国际法原则和规则，再次确认了国际法适用于网络空间，指出国际法的适用包括医疗部门与重要医用设施的网络运营。**

《第二份牛津声明》详细指出："与疫苗研究、试验、制造和分发相关的设施，与治疗方法、预防措施有关的其它研究路径，及其技术、网络和数据，尤其是临床试验结果"都属于其中的医用设施，受国际法保护。

两份声明均指出国际法禁止国家实施对他国基本医疗服务造成严重不利影响的网络行动。根据网络行动侵犯程度的不同，可能违反主权原则、不干涉内政原则与不使用武力原则。声明指出国家在国际法下负有积极保障义务和审慎义务，指出国家需采取一切可行措施，以防止、制止和减轻针对其已知或应当知道来自其领土或管辖范围内的恶意网络行动。

二、医疗卫生系统遭受网络攻击的国际法问题

（二）国际刑法层面：个人刑事责任

在个人层面，法律通过将相关行为定为刑事犯罪来保护医院或者更普遍的医疗保健部门免受网络攻击，在国内刑法将危及公共健康和安全的行为定为刑事犯罪。

在国际刑法层面，《布达佩斯网络犯罪公约》缔约国明确同意，对维护公共健康和安全至关重要的计算机系统的攻击包含在公约现有条款中。将特定的网络活动定为刑事犯罪，例如非法访问、数据干扰和系统干扰。依国际刑法的规定，针对医疗设施的某些特别严重的网络攻击可能构成国际罪行，例如战争罪或危害人类罪。根据国际刑事法院罗马规约规定的指挥攻击医疗设施的战争罪，包括使用网络手段攻击。

二、医疗卫生系统遭受网络攻击的国际法问题

（三）国际人道法

当武装冲突和流行病相互交织时，这些保护比以往任何时候都更加重要。在武装冲突期间保护医疗设施是国际人道法的核心问题，国际人道法禁止在武装冲突期间阻碍医疗保健设施运作的恶意网络行动。《日内瓦公约》规定：医疗设施及其工作人员必须受到尊重和保护。国际人道法基本规则也适用于网络空间，必须得到尊重，交战方不得通过网络操作损害医疗基础设施，必须非常谨慎，避免此类操作造成附带损害。在武装冲突期间，国际人道法为医疗服务和设施提供强有力的保护。《联合国宪章》、《塔林手册》网络行动可能构成使用武力。因此，国际卫生组织禁止在武装冲突期间阻碍保健设施运作的恶意网络行动。

二、医疗卫生系统遭受网络攻击的国际法问题

（四）国际人权法

国际人权法要求各国尊重并确保管辖范围内所有人的生命权和健康权。（《经济、社会和文化权利国际公约》（ICESCR）第12条规定的健康权或《公民权利和政治权利国际公约》（ICCPR）第6条规定的生命权。）

联合国经济、社会和文化权利委员会认为“缔约国必须尊重其他国家对健康权的享受”。国家尊重和确保这一权利的义务扩展到“位于国家有效控制的任何领土之外，但其生命权受到其军事或以直接和合理可预见的方式进行的其他活动。”

三、医疗卫生系统遭受网络攻击的国内法问题

（五）各国国内立法：

各国通过网络安全立法和关键信息基础设施保护法、国家安全立法等对医疗卫生系统进行保护。

美国国家标准技术研究院《提升关键基础设施网络安全的框架》、欧盟《网络与信息安全指令》等规定关键信息基础设施：遭到破坏会使国家网络安全、国家经济安全、国家公共卫生受到影响的基础设施。许多国家明确了关键国家基础设施”涉及通信、国防、能源、医疗、教育、金融、交通、水利、环境保护等十几类关键基础设施，指定相应政府机构负责保护。

三、医疗卫生系统遭受网络攻击的国内法问题

（五）我国国内立法：

2021年8月17日，我国《关键信息基础设施保护条例》9月1日正式实施。作为我国在关键信息基础设施安全方面的首部行政法规，条例在推进关键信息基础设施保障、完善我国网络安全体系、保障国家安全、国计民生与公共利益等诸多方面都有着十分重要的作用。

条例从关键信息基础设施的认定、完善监督管理体系、运营者责任义务、保障和促进措施与法律责任等多个方面提出总体监管要求，在关键信息基础设施保护法律体系建设中起到提纲挈领的作用。

《关键信息基础设施保护条例》与我国颁布的相关法律法规呈现出有效衔接、相互补充的关系，体现了国家顶层设计的通盘考虑。

以《网络安全法》为法律基础，《关键信息基础设施保护条例》对其中的“关键信息基础设施的运行安全”部分进行了落实、细化和完善。

在网络安全审查方面，《关键信息基础设施保护条例》要求对负责人和关键岗位人员进行安全背景审查，对网络产品和服务采购进行安全审查与《网络安全法》和《网络安全审查办法》的精神和内容保持了一致。

在漏洞管理方面，《条例》特别强调了未经授权不得对关键信息基础设施实施漏洞探测和渗透性测试活动，对基础电信网络实施漏洞探测、渗透测试等活动应当事先向国务院电信主管部门报告。这些规定与《网络产品漏洞管理规定》对从事网络产品安全漏洞发现、收集的组织和个人的相关规定，在内容上是互相补充。

在数据出境方面，《条例》没有特别规定，但是有《数据安全法》作为《网络安全法》的配套和衔接，关键信息基础设施的数据出境问题可依照相关规定执行。

三、医疗卫生系统遭受网络攻击的国内法问题

2018年9月13日，国家卫生健康委发布《国家健康医疗大数据标准、安全和服务管理办法（试行）》，明确责任单位应当落实网络安全等级保护制度要求，对健康医疗大数据中心、相关信息系统开展定级、备案、测评等工作。

2019年12月，我国颁布卫生健康领域第一部基础性、综合性法律《中华人民共和国基本医疗卫生与健康促进法》，明确国家采取措施推进医疗卫生机构建立健全信息安全制度，保护公民个人健康信息安全，对医疗信息安全制度、保障措施不健全，导致医疗信息泄露和非法损害公民个人健康信息的行为进行处罚。

2020年2月28日，国家医疗保障局、国家卫生健康委员会发布《关于推进新冠肺炎疫情防控期间开展“互联网+”医保服务的指导意见》，要求不断提升信息化水平，同步做好互联网医保服务有关数据的网络安全工作，防止数据泄露。

从陆续出台的政策法规可以看出，国家对医疗行业网络安全高度重视，无论从医院、基层医疗机构信息化建设，还是当前发展火热的“互联网+医疗健康”、“医疗大数据”，到一些基本惠民便民的传统医疗信息系统建设，以及国家出台的第一部卫生健康领域基础性、综合性法律，无不强调落实做好网络安全工作。

结语

新冠肺炎疫情期间针对全球医疗卫生系统的网络攻击问题，在国际法层面，受到国际法、国际人道法、国际人权法、国际刑法等法律规制，在国内法层面，受到网络安全法、卫生健康法、刑法等法律规制。医疗设施作为我国关键信息基础设施的法律保护问题尤为重要，在医疗卫生系统的网络安全保护中，有必要跟进中国和国际最新的网络安全法的立法动态，形成全球网络安全法律规制的合力，保护医疗保健部门免受网络攻击。

感谢聆听！