

中国互联网网络安全威胁治理联盟章程

第一条 本联盟的中文全称为中国互联网网络安全威胁治理联盟(下称“联盟”),英文名称为 China Cyber Threat Governance Alliance (缩写“CCTGA”)。

第二条 本联盟由国家计算机网络应急技术处理协调中心(下称“CNCERT”)与中国互联网协会网络与信息安全工作委员会联合发起成立,由在中国境内从事互联网网络安全威胁治理工作的成员单位自愿组成,接受中国互联网协会的业务指导和监督管理。

第三条 本联盟通过行业自律机制,充分发挥联盟成员单位作用,开展对互联网网络安全威胁情报共享,并对互联网黑产密切相关的各类威胁进行整治,有效净化网络安全环境,树立我国负责任网络大国的良好形象。

第四条 本联盟成员单位应符合下列条件:

- (一) 在中国境内依据中国法律成立的独立法人单位。
- (二) 热衷于推动中国互联网网络安全威胁治理工作的开展。
- (三) 严格遵守国家相关法律法规,承认本联盟章程,履行成员单位义务。

第五条 本联盟负有以下职责：

（一）广泛接收社会及联盟成员单位对拒绝服务攻击、网页篡改、网站后门、网络钓鱼、隐私窃取、恶意程序、域名安全等各类网络安全威胁的投诉举报。

（二）组织开展互联网网络安全威胁整治，推动互联网网络安全威胁治理体系建设。

（三）组织开展互联网网络安全威胁情报共享。

（四）定期公开发布互联网网络安全威胁数据和治理报告。

（五）积极参与互联网网络安全威胁治理的相关立法、新技术新应用、标准等研究制定工作，为联盟成员单位提供相关业务和政策咨询服务，为政府部门提供决策支撑。

（六）开展互联网网络安全威胁治理宣传教育工作，提升网民网络安全意识。

第六条 中国互联网网络安全威胁治理联盟由联盟专家委员会、联盟秘书处和联盟成员单位组成。

（一）联盟专家委员会依托于中国互联网协会网络与信息安全工作委员会，主要负责对联盟运行相关工作提供技术支持和专家意见。

（二）联盟下设秘书处，主要负责联盟的日常运行工作。联盟秘书处设在 CNCERT，并设秘书长。

（三）联盟成员单位按照联盟章程规定的程序加入本联盟，主要负责网络安全威胁的举报、共享和处置。

第七条 由联盟成员单位派出的代表组成联盟成员会议，指导联盟开展工作，决定联盟的重大事项。联盟成员会议每年召开一至三次，其职责是：

- （一）批准联盟章程的修改。
- （二）审议批准秘书处提交的决议事项。
- （三）决定本联盟的其他重大事项。

第八条 联盟加入程序

- （一）提交书面的代表人选推荐表。
- （二）经联盟秘书处审核通过，并在联盟的信息平台上予以公布。

第九条 联盟退出机制

- （一）提交退出的书面申请，说明退出理由；或因违反联盟有关规定，被联盟除名。
- （二）在联盟的信息平台上予以公布。

第十条 联盟成员单位享有下列权利：

- （一）享有向联盟举报各类网络安全威胁的权利。
- （二）享有使用联盟提供的各种信息服务的权利。
- （三）享有联盟威胁情报共享的权利。
- （四）参加本联盟组织安排的交流研讨活动。

第十一条 联盟成员单位应履行下列义务：

（一）对于联盟下发涉及本单位的网络安全威胁进行清理和处置，并反馈处置结果。

（二）在法律允许的范围内，基于自愿的原则，向联盟共享本单位面对的各类网络安全威胁，并提供相关数据、线索和证据。

（三）维护联盟和联盟成员单位的合法权益。

（四）积极参加联盟组织的工作会议和各项活动。

（五）积极宣传联盟。

第十二条 本章程自联盟成立之日起生效，由联盟秘书处负责解释。

中国互联网网络安全威胁治理联盟运作机制（拟）

一、背景目的

2015 年 7 月 31 日，CNCERT 会同中国互联网协会网络与信息安全工作委员会联合国内 54 家企事业单位通过行业自律方式，启动了互联网网络安全威胁治理专项行动，对拒绝服务攻击、网页暗链篡改等与互联网黑产密切相关的事件进行了重点处置。经过努力，截至 2016 年 1 月 31 日，DDoS 攻击事件日均次数由行动前的 1491 起下降到 265 起，下降了 82.2%，境内被篡改网站月均数量下降 21.4%，被篡改政府网站月均数量下降 56.2%。为持续开展互联网网络安全威胁治理工作，通过成立中国互联网网络安全威胁治理联盟，构建威胁治理联盟体系，加强威胁情报共享和威胁协同处理，有效净化网络安全环境，树立我国负责任网络大国形象。

二、联盟机构

互联网网络安全威胁治理联盟由联盟专家委员会、联盟秘书处和联盟成员单位组成。

联盟专家委员会由互联网行业相关专家组成，主要负责对联盟运行相关工作提供技术支持和专家意见。

联盟秘书处设在 CNCERT，主要负责联盟的日常运行。设秘书长。

联盟成员单位主要负责日常网络安全威胁的举报、共享和处置。

三、工作内容

在联盟框架下，开展对拒绝服务攻击、网页篡改、网站后门、网络钓鱼、隐私窃取、恶意程序、域名安全等网络安全威胁的情报共享和事件协同处置。

四、工作流程

（一） 投诉举报

联盟秘书处设置电话、邮件、在线等多种举报方式，广泛接收社会及联盟成员单位对各类网络安全威胁的投诉举报。

（二） 情报共享

联盟秘书处负责整理通过多种渠道获得的可共享的网络安全威胁情报数据；联盟成员单位可以通过数据接口，获得情报共享。

联盟成员单位可以向联盟秘书处共享自主获得的网络安全威胁情报数据；联盟秘书处对联盟成员单位允许共享他人的网络安全威胁情报进行统一共享。

（三） 威胁认定

联盟秘书处负责对一般网络安全威胁进行直接分析和认定；对于影响范围较大的网络安全威胁，由联盟秘书处提交联盟专家委员会进行研判后认定。

（四） 协同处置

联盟秘书处负责协调联盟成员单位开展对确定要处置的网络安全威胁事件进行处置；联盟成员单位负责对联盟秘书处下发的网络安全威胁处置指令进行处置，并反馈处置结果。处置方式包括但不限于：（1）对网络攻击行为进行记录、分析、溯源；（2）对网络攻击相关的 IP 地址、域名、URL、APP、电子邮箱账号、其它通讯账号等进行积极处置；（3）在终端对恶意 IP 地址、恶意网址、恶意 APP、恶意电话号码等进行拦截或提示；（4）屏蔽网络攻击服务或工具的售卖和推广渠道。

联盟秘书处负责接收申诉者的申诉请求；对一般网络安全威胁处置的申诉请求由联盟秘书处进行直接处理；对于影响范围较大的网络安全威胁处置的申诉请求由联盟秘书处提交联盟专家委员会进行研判，提出处理意见，由联盟秘书处进行具体实施。

（五） 信息发布

联盟秘书处负责定期对网络安全威胁情报、整治情况等进行分析，并以报表、报告、地图等多种方式公开发布。