引用本文：马雷. 反思与借鉴：美国网络安全信息共享规制研究[J]. 河海大学学报(哲学社会科学版)，2019，21(5)：76-81.
DOI：10.3876/j.issn.1671-4970.2019.05.011

反思与借鉴：美国网络安全信息共享规制研究

马　雷

(南京大学法学院，江苏南京　210093)

摘　要：随着网络日益成为人类信息交流的主要载体，网络安全信息的合理共享便成为各国政府不可回避的议题。作为先行者，美国对网络安全信息共享机制进行的全方位研究可谓意义深远。以“共享”为主线，通过剖析共享范围/类型、共享主体与程序、私主体信息共享责任的豁免、共享权力限制等4个方面，力图准确把握美国于2015年通过的《网络安全信息共享法案》的要旨。为此，我国应通过合理界定网络安全信息共享的范围，构建特有的信息共享行政机制，赋予私主体责任豁免，确立利益平衡的基本原则，最终保障共享信息的合理使用。

关键词：网络安全信息共享；《网络安全信息共享法》；本土化建构；信息共享规制

中图分类号：D920.4　　**文献标志码**：A　　**文章编号**：1671-4970(2019)05-0076-06

一、问题的缘起

文字被创造之日起，它的表达方式就始终未能脱离经济和科技的影响。作为信息的载体，文字传播形式的变化势必会带来信息流动过程的剧变[1]。因特网的出现使得人类社会越来越依赖网络传递信息，而这一现象在拥有几亿网民的中国被放大。伴随着网络的迅猛发展，网络攻击和威胁事件也如影随形，在全球化融合态势下，网络安全信息共享已获得各国政府的广泛重视。基于此，世界各国积极制定关于网络安全的法律规范，其一致认为，应对网络安全威胁最为便捷和有效的方案就是使安全信息最大限度内的共享，而美国当仁不让地成为了该领域的法治先驱者。2015年12月18日，作为综合预算法案之附加内容的《网络安全信息共享法案》(简称CISA)获得美国国会通过，总统奥巴马随后签署了该法案，这标志着网络安全信息共享以及整合迈出了重要一步。

与美国一样，我国政府对网络安全也高度重视。政策导向上，我国进行了一系列设计，例如《国家网络空间安全战略》《网络空间国际合作战略》等规范性文件都积极探索网络安全信息共享模式。毋庸置疑，这些法律规范为我国网络安全信息的保护建构起了初步框架，但较之美国的立法现状，我国仍有许多问题有待明确。在此语境下，立足于对美国网络安全信息共享的立法研究，希冀在比较分析之后发掘我国网络安全信息共享立法方面的着力点。

收稿日期：2019-07-06

作者简介：马雷(1987—)，男，安徽滁州人，博士研究生，从事信息法学研究。

二、美国网络安全信息共享的价值选择及立法历史沿革

网络安全信息共享是指与网络信息系统及其储存传输信息安全有关的一系列信息的交换①。从广义上来看,网络安全中的"信息"并不仅仅是指在服务器或者客户端中的代码,还包括系统风险、程序漏洞、网络威胁及网络安全的良好实践等[2]。网络安全信息共享的聚合点在于通过联结重要信息体提升对于潜在威胁的高度认知,进而保障信息或策略的安全传播[3]。本部分就美国网络安全信息共享的价值选择和立法进程进行具体分析,这是理解 CISA 的前提和基础。

1. 价值定位——安全抑或隐私

CISA 在公布之后便招致了来自学界和社会团体组织较大的争议,如华盛顿大学法学院的 Kerr 教授尖锐地指出,基于法律语词的不确定性以及该法在法律适用上绝对有限等多种原因,CISA 将以正当化的方式赋予网络运营者更多的权力监控网络用户,这无疑将在公民隐私权上撕开一道口子[4]。美国民权组织联盟也指出,尽管信息的共享对网络尤为重要,但是 CISA 对于"网络威胁指征"(简称 CTI)和"防御措施"(简称 DM)做广义的界定势必有损公民的合法权益[5]。

从以上的质疑声中不难发现,反对者认为该法的出台选择了保护国家安全这一五维空间而摒弃了普适的公民隐私权价值观。笔者认为,实际上这是对 CISA 价值定位的误解,应当说,从本法的制定内容和过程来看,其已经最大限度地实现了国家安全与个人隐私的兼顾。理由如下:其一,在国家安全和公民隐私之间,需要根据法益的重要程度作出一定的让步。不可否认,隐私权是公民的重要权利,但当国家网络安全这一法益的完整性受损时,隐私权势必受到牵连,因为前者是后者的基础和保障。其二,国家安全和公民隐私权并非完全对立,二者存在叠合的一面,当国家安全得以维护的情境下,绝大部分公民的隐私权是有保证的。因而,CISA 在保护国家安全的同时也维系了公民个人隐私。

2. 美国网络安全信息共享法立法的基本进程

在过去的数十年,美国政府已经制定和颁布了一系列国家战略、行动计划、行政指令以及多部法律,旨在通过制度化安排以妥善处理并应对网络空间安全和网络信息安全。与此同时,信息共享并不是 CISA 的产物,早在克林顿执政时期通过的《第 63 号总统决策指令》就创建了信息共享与分析中心(简称 ISAC)。该机构的主要任务是负责收集、分析和共享其成员之间的安全事件信息和应对措施,进而促成政府和私营行业的信息交流[6]。

在遭遇"9·11 恐怖袭击事件"之后,美国政府更加意识到情报信息收集与共享的重要性。此种背景下,美国国会于 2002 年通过了《国土安全法》并成立了著名的国土安全部,该机构研发了国土安全信息网络(简称 HSIN)以用于联邦政府和地方政府的执法信息交流[7]。之后,HSIN 运营范围在不断扩张,逐渐将美国各个关键基础设施行业纳入其涵摄领域。奥巴马上台以后,对于网络安全信息的保护力度并未消减,继续致力于推进网络安全的综合性立法,由于美国政治体制的原因,总统转向于推进国会立法并取得了一系列的成果。在 20 多年的网络安全保护历程中,信息共享实践一直存续。应当说,CISA 的颁布仅仅是更为完善地、在更加广泛地范围内进一步确认并发展网络安全信息共享。

三、域外网络安全信息共享的立法设计——以美国为样本

围绕着信息安全与隐私保护两大主题,理论界和学术界尚未达成共识,但是就 CISA 的文本内容来看,"共享"并非是没有限度的信息融合,而是具有一整套共享规则约束的信息分享机制。笔者从共享范围/类型、共享主体与程序、私主体信息共享责任的豁免、共享权力限制等 4 个方面解读 CISA,以期揭开美国信息共享的法律面纱进而为我国相关的制度设计提供参考。

1. 共享范围/类型的诠释

2015 年,美国人事管理局数据库遭到黑客攻击,超过两千万条个人信息被盗用,这其中包括了地址、家庭成员信息、银行卡信息、职业信息等[8],据此不难发现,网络安全信息需要在立法层面予以关切,否则任何不当的运用或者泄露都可能造成不可挽回的损失。在此种语境下,网络安全信息共享就

①也有文章中将网络安全信息(Cybersecurity Information)界定为网络威胁信息或网络威胁情报,本文不做以上区分,视为同一概念。

要对其内容作出清晰的界定。CISA 将共享的内容分为两类:网络威胁指征及防御措施。所谓网络威胁指征主要是指识别或者描述网络恶意侦查、安全漏洞等必要信息;防御措施则主要是指应用于信息系统,或系统中储存、处理、传输的信息,以检测、预防或者减轻已知或疑似之网络安全威胁或网络安全漏洞的行为。

2. 共享主体与程序

(1)联邦实体的网络安全信息共享

CISA 规定,针对已经解密的网络安全威胁指征、防御措施及其他关联性信息,联邦政府允许以非机密形式与其他主体共享。由于所涉的网络安全信息已经解密,所以其共享的对象范围较广,包括联邦实体、非联邦实体以及适当的民众。对于涉及机密的国家网络安全信息,仅限于具有安全资质的主体。除此之外,该法还要求联邦政府在对有关信息的持续分析基础之上,通过出版物及针对性地推广,定期共享网络安全最佳实践。

为了配合网络安全信息共享流程的通畅、安全以及高效,CISA 还设置了一系列程序性条件,具体包括 4 个方面:其一,要求联邦政府对网络安全信息做技术性处理。一方面保证机密信息不外泄,另一方面又要完成在恰当主体之间的共享。其二,统一职责。目前,关于网络安全信息共享责任承担与主体属性相关,为了实现信息共享的体系化和规范化,应当最大限度地合并联邦实体与非联邦实体责任。其三,通知义务。无论是联邦实体抑或是非联邦实体,在得知所接收的信息为错误或违规时应当及时予以通知。其四,设置“控制阀”,从而避免未经授权访问或者获取该网络威胁指征或防御措施的相关要求。需要说明的是,这里的联邦实体包括美国联邦的各部门、机构以及组成部分,例如商务部、国防部、财政部、国家情报总监办公室等。

(2)非联邦实体的网络安全信息共享

非联邦实体的网络安全信息共享是指共享的一方为非联邦实体,如此一来便存在两种情形:联邦实体与非联邦实体间的信息共享、非联邦实体之间的信息共享。例如,2016 年包括摩根大通、通用等在内的公司达成了企业间网络安全信息共享的共识,以此来应对破坏性的网络攻击[9]。

该法同时对非联邦实体网络安全信息共享的流程进行规制:其一,事前审查机制。对于非联邦实体共享的网络安全威胁指征及时审查,以确定不属于特定个人的公民信息。其二,事中移除机制。在共享过程中,一旦发现上述包含特定个体信息时需及时移除。为了保证网络安全信息的共享得以高效完成,立法者将问题解决的重点置于如何获取信息的路径上。基于此种理念,CISA 规定通过自动化的方式来进行网络安全信息的全天候响应,诸如电子邮件、自动共享程序等。如此观之,该规定是虚拟空间内信息离散化与一体化的内在需求。

3. 共享责任的豁免

众所周知,网络安全的治理必然会面临信息安全与个人隐私的内在冲突,正如有学者所言:“在信息化高速发展的今天,信息共享在抗制风险的过程中会引发隐私权的纷争[10]。”从既存的法律文本来看,CISA 对二者做了最大限度的调和,并给予私主体共享信息过程中责任豁免的照顾。

其一,维持有关特权或保护资格。主要包括两个方面:监控授权、防御措施运行授权。所谓监控授权是指私主体可以基于网络安全目的监控该私实体的信息系统、经另一非联邦实体授权且书面同意的该实体信息系统及其他重要信息等内容;防御措施运行授权意味着私实体可以将防御措施应用于特定信息系统中用于保护其权利或财产。其二,反对摊派任务。本法规定的网络安全信息共享是以自愿为前提,不允许联邦实体强迫某一非联邦实体向其他主体提供信息。其三,法律责任的豁免。以上保护形式在一定程度上打消了网络安全信息持有者(这里主要指非联邦实体)的后顾之忧,促进其积极加入共享联盟。

4. 共享权力限制

法谚有云:“任何不经控制的权力都将成为噬人的恶魔”,这在信息膨胀的时代显得极具合理性[11]。在 CISA 所建构的网络安全信息共享关系中,毫无疑问,联邦实体以其掌握的权力资源在共享主体的格局中居于优势地位,因此,该法对政府活动也施加一定的限制。

其一,借助于共享目的的设置,限制国家的网络安全信息共享行为。CISA 对于“安全目的”进行界定在一定程度上为共享划定了界域。其二,力图通过保护公民隐私与自由,间接约束公权力的行使。此阶段包括两方面内容:一是发布指南并定期审查,二是确定隐私的内容。根据该法可知,司法部和国

土安全部为发布临时指南和最终指南的主要部门，它们所发布的指南应当对于联邦实体接收、保存、使用以及传播其获得与授权活动有关的网络威胁指征做出相应规定。与此同时，该法还要求定期对于指南的内容予以审查（每两年不少于一次）。为了最大限度地保护公民隐私，该法也做了努力，如建立相应机制，及时销毁与已知授权不相关的信息，且对网络威胁指征的储存期也施加限制。除此之外，该法对违规操作予以制裁，上述规定对确保共享关系的有序建立以及共享的持续进行都极具意义。

四、网络安全信息共享机制的本土化建构

深度剖析 CISA 可知，美国已经建立了趋于成熟的网络安全信息共享机制，并且正在为美国政府和国民提供优质服务，而这对于初步创建网络安全法，并且积极改善配套法律规范的中国而言，无疑值得借鉴和学习。当今，互联网成为科技强国决战和角力的竞技场，网络安全信息共享机制的完整性自然显得尤为重要。基于此，笔者认为应该先准确认识我国网络安全信息共享概况，再着手构建具有中国特色的新型互联网安全信息共享机制。

1. 建构的前提：我国网络安全信息共享的现状

当前，我国的网络安全信息共享制度尚处于初级阶段，存在诸多问题：其一，共享的主体受限。从理论上讲，网络安全信息由零散向体系的蜕变过程需要更多的主体参与其中，然而我国目前的共享主体集中在政府机构之间以及公共部门与少数私主体之间。其二，共享路径单一。长期以来，我国习惯于采用信息通报制度，这种信息流通方式拘泥于单向抑或者双向的分享，缺乏立体性思考，因而难以适应当前的网络安全危机。其三，立法体系分散。不可否认，2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》已经为互联网的展开提供了指南，但是具体的政策和法规依旧欠缺，在网络安全信息共享的对象、责任划分等方面尚未有明确的规定。

2. 合理界定网络安全信息共享的范围

网络安全信息共享的范围影响共享制度的定位，然而其自身又与信息共享的类型、主体以及用途相关联，因此可以考虑从以下 3 个方面切入。

第一，网络安全信息共享的类型。对于共享信息类型的定义，美国不同部门的规定也不尽相同。有立法采用“概括规定+具体列举”的方式从广义层面予以界定，如 CTSA 将其分为网络威胁指征和防御措施两类，并具体罗列了包括恶意侦查、安全漏洞、恶意的网络指挥控制等在内的各种类型。美国国家标准技术研究院将网络威胁信息类型化界定为指征、策略、技术和程序、安全警报等，而美国参议院主张将网络安全信息限定在一定空间中，因而在 2015 年《网络威胁共享法案》（CTSA）中直接回避了网络安全策略的共享主体。笔者认为，我国应该采用网络威胁指征和防御措施的分类，并在后续的立法过程中逐渐明确和细化。

第二，网络安全信息共享的主体。关于网络安全信息的共享主体，存在两种不同的模式：一是授权私主体可以自愿与任何其他主体进行网络安全信息的共享，例如 CTSA 便做了此类规定[12]。二是作出了限制，例如 CTSA 主张私主体只能与特定的主体共享信息，信息共享组织和国家网络安全和通信整合中心（NICC）[13]。笔者认为，立足于我国的网络安全现状，应该允许私主体可以与政府或其他私主体共享信息，助力网络安全信息共享的体系建设。

第三，网络安全信息共享的后续限制。网络安全信息共享进行后续限制是为了更好地实现共享，几乎所有的立法者都对其做出了限定。美国《网络情报共享与保护法案》规定，基于网络安全目的可进行情报共享，且共享者可以做任何限制。CISA 也设置了基于网络安全目的的前置性条件，但对于政府的后续使用并未全面限制。我国在立法过程中也应当设置基于网络安全目的的原则，并对政府使用私主体共享的信息作出必要的限制性规定。

3. 构建我国特有的信息共享行政机制

为了实现网络安全信息在政府部门之间以及政府部门与私主体之间的共享，势必要求有强有力的行政机制做后盾。CISA 形成了由高效统一领导、多部门广泛协同的共享模式，即由美国国土安全部领导，国家情报总监、国防部等共同参与网络安全信息共享程序的制定[14]。美国起先通过立法强化了国家网络安全和通信整合中心的职能，指出由其负责部门间信息共享的整合，之后，在国家情报总监之下又成立了网络威胁情报整合中心（CTIIC）进一步配合国家网络安全与通信整合中心以及其他部门的工作[15]。

网络安全信息共享的关键在于共享，即实现信息的流通。面对庞大的数据流，若想实现这一目的，

应该建立行政保障机制。其一,构建公(政府)私(企业)合作机制。在既存的政府部门分工基础之上,鼓励指引各个行业根据自身特点成立行业协同委员会。如此一来,政府各职能部门便可以和行业协同委员会建立合作关系。公私合作关系建立的意义在于尽快制定信息共享和交换相应的技术参数以及行业标准等,不定期发布和更新行业指引。其二,适时成立专门性的机构。尽管我国之前也陆续设置了若干与网络安全信息相关的机构,例如国家网络与信息安全通报中心,但并未明确彼此间的关系,这直接导致机构繁多、力量不集中,且与企业以及行业组织也都缺乏深度交流[16]。国家网络安全信息共享中心的建立可以为中小企业的网络安全信息共享提供服务,当信息共享较为平稳之后,再逐级扩展,进而形成覆盖全国的、不同层级的合作体系。需要指出的是,在公私合作的过程中,政府可以给予参加网络安全信息共享的企业一定的资金或技术支持,调动私实体的积极性以便迅速构建信息共享机制。

4. 赋予私主体责任豁免,促进信息共享的畅通无阻

如何促使私主体将其掌握的信息与政府分享是当前信息共享环节的前提性问题。政府在配给义务的同时也要给予私营主体一定的权利,如此方可真正实现"心往一处想,力往一处使"。

权利和义务的关系表明,任何一方的缺席都会使整个利益生态系统失衡[17],这对于网络信息安全共享机制的构建同样适用,如果一味向私实体增加义务,最终只会适得其反。笔者认为,应该立法规定私实体在遵守法定标准和行业准则的情况下,出现信息大规模泄露时予以免责。有学者认为,对于此种情形可以考虑适用补偿性赔偿责任以减轻私主体的负担[18]。应当说,这种做法并不适合我国,至少现阶段并不可取。与以美国为代表的发达国家不同,我国的网络安全信息维护能力正处于上升期,由于体量巨大,此时工作的重点就是信息共享主体的强化和扩容,而不是对于参与者的责任强化。

与此同时,为了提升私主体发现网络安全漏洞的能力并消除因共享信息而受到法律惩处的疑虑,我国政府在未来的立法过程中可以考虑授权私主体对所负责运营的网络信息系统等予以监视且不承担法律责任,两个或者两个以上私主体在网络安全信息共享过程中的相互协助不构成垄断。除此之外,国家也可以在税收、政府采购、技术指导、人员培训等方面给予适当帮助。

5. 确立利益平衡的基本原则,保障共享信息合理使用

在网络安全信息共享的整个流程中,政府部门处于优势地位,因而公众对于其如何适用这些信息心存疑虑,这显然成为立法者不可回避的问题[19]。具体而言,政府部门对所获得信息的不慎使用可能使商业秘密公开、侵害主体的隐私权以及个人权益等。鉴于此,笔者认为我国立法工作可以针对以下两个方面进行规定。

第一,构建网络安全生态关系圈,注意协调网络安全与保护私人权利的关系。笔者认为,应该借鉴美国 CISA 的经验,规定政府或其他主体在使用或者共享网络安全信息时必须充分保障含有可识别的个人信息未经授权不得予以披露。当然这也并非所涉信息不可共享,共享主体可以采用匿名或者除名的形式适用。而对于个人信息无法移除的,则应该做好保密工作,防止泄露和滥用。一旦含有个人信息的网络安全信息被泄露,共享主体应尽到及时通知的义务,将个人利益损失降到最低。

第二,网络安全信息的附条件使用,并促成定期报告制度。《中华人民共和国网络安全法》规定,政府履行网络安全保护职责所获取的信息应该以维护网络安全为使用原则。应当说,该原则同样适用于网络安全信息共享,并且可以进一步细化,这一点可以借鉴美国的立法。基于网络安全为目的之考量,政府机关所获取的信息披露或者使用仅限于以下情形:识别网络安全漏洞;避免或减轻对国民生命或财产造成重大损失;应对与恐怖主义、未成年人保护、网络诈骗、国家安全等相关严重犯罪行为其他情形。除此之外,为了实现对于网络安全信息共享的监督,我国政府部门应该定期向全国人大常委会进行汇报,汇报的内容应该主要围绕共享的标准、数据、个人隐私保护措施等。

五、结　语

在整个社会都向网络时代迈进的同时,原本在现实空间存在的问题也顺势过渡到虚拟世界中,网络安全信息共享便是如此。网络安全信息的共享与协作不仅关系单一主体的安全与秩序,更维系整个国家时代命运。因此,此种背景下只有确立本土的

“共享”规则,才可能建构具有中国特色的新型互联网安全信息共享机制。现阶段,合理界定网络安全信息共享的范围、构建我国特有的信息共享行政机制、赋予私主体责任豁免以及确立利益平衡的基本原则应该成为理论界和实务界努力的方向。唯有首先解决宏观上的制度设计,后续关于网络安全信息共享的具体构建才有可能顺利开展。

参考文献:

[1] 韩元凤. 互联网时代图书文字编辑工作的转型升级探讨[J]. 传播与版权,2019(6):28-29.

[2] 刘金瑞. 我国网络安全信息共享立法的基本思路和制度构建[J]. 暨南学报(哲学社会科学版),2017(5):14-23.

[3] NATHAN A S. Regulating cyber-security [J]. Northwestern Law Review,2013,107(4):1503-1568.

[4] NOJEIM G T. Cybersecurity and freedom on the Internet [J]. Journal of National Security Law & Policy,2010(4):119-137.

[5] 方婷,李欲晓. 安全与隐私:美国网络安全信息共享的立法博弈[J]. 西安交通大学学报(社会科学版),2016,36(1):69-76.

[6] 刘金瑞. 美国网络安全信息共享立法及对我国的启示[J]. 财经法学,2017(2):22-30.

[7] 蔡士林. 美国国土安全事务中的情报融合[J]. 情报杂志,2019(1):8-12.

[8] 李恒阳. 美国网络安全面临的新挑战及应对策略[J]. 美国研究,2016(4):101-110.

[9] 杨沛安,武杨,苏莉娅,等. 网络空间威胁情报共享技术综述[J]. 计算机科学,2018,45(6):9-18.

[10] KELLY B B. Investing in a centralized cybersecurity infrastructure: why “hacktivism” can and should influence cybersecurity reform[J]. Boston University Law Review,2012(92):1163-1711.

[11] 宋国涛. 试析美国《网络安全信息共享法案》[J]. 保密科学技术,2016(6):28-31.

[12] JEREMY J B. Building on executive order 13636 to encourage formation sharing for cyber security purpose [J]. Harvard Journal of Law & Public Policy,2014,37(2):674-690.

[13] 蔡士林. 被遗忘权在刑事领域中的展开[J]. 华侨大学学报(哲学社会科学版),2018(4):75-85.

[14] 赵志云,崔海默. 美国网络安全新近立法及对我国的启示[J]. 学术交流,2017(6):136-141.

[15] 张臻. 美国网络威胁情报工作体系及启示[J]. 保密科学技术,2017(9):48-52.

[16] 黄道丽. 网络安全漏洞披露规则及其体系设计[J]. 暨南学报(哲学社会科学版),2018(1):94-106.

[17] 童之伟. 法权中心主义要点及其法学应用[J]. 东方法学,2011(1):3-15.

[18] BURSTEIN A J. Amemding the ECPA to enable a culture of cyber security research [J]. Harvard Journal of Law & Technology, 2008,22(1):167-182.

[19] 刘金瑞. 我国网络关键基础设施立法的基本思路和制度建构[J]. 环球法律评论,2016(5):110-129.

(责任编辑:高　虹)