欧盟网络安全战略解析*

周秋君

内容提要:欧盟网络安全战略始于20世纪90年代,历经三个阶段的发展演变,已成为欧盟安全治理格局中日益重要的内容。它以2013年出台的《欧盟网络安全战略》为标志,包含网络安全管控机构、战略文件与法律法规、信息技术保障、安全合作实践以及网络安全文化建设五大保障机制,构成了一个立体的战略框架体系。欧盟的战略是偏重于治理层面的网络安全战略,有别于军事层面的美国网络安全战略。虽然整体形制日趋完善,但鉴于日益严峻的全球网络安全形势和日趋复杂的网络政治生态,以及在统筹成员国网络安全管控资源、协调并整合内部政策与行动等方面障碍重重,欧盟网络安全战略的实施显得步履维艰。因此,若要实现其战略目标,在全球网络空间发挥规则引领和价值观导向的作用,并在全球网络管理过程中争取更大的话语权和影响力,欧盟依然面临诸多挑战。

关键词:欧盟　网络安全战略　保障机制　挑战

随着信息技术的疾速发展,网络空间①(cyberspace)已成为与物理世界平行的人类活动场域。由于网络治理并无先例可循,因此各国在应对日益复杂的网络安全②(cybersecurity)挑战时,大多沿用了各自在治理物理世界时的思路和做法,形成了具有本国特色的网络安全战略。需要说明的是,本文将"战略"定义为一种治理语境下的综合范畴,因此,欧盟网络安全战略是一个在网络空间中对欧盟安全利益产生实际影

* 本文受"上海政法学院创新性学科团队支持计划"资助,感谢《欧洲研究》杂志匿名评审专家对本文提出的宝贵意见和建议。文中疏漏之处由笔者负责。

① 国际电信联盟(International Telecommunication Union, ITU)对"网络空间"的定义是:"由以下所有或部分要素创建或组成的物理或非物理领域,这些要素包括计算机、计算机系统、网络及其软件支持、计算机数据、内容数据、流量数据以及用户。"参见"ITU Toolkit for Cybercrime Legislation", February 2010, p.12, http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf, last accessed on 24 May 2015。

② 欧盟对"网络安全"的定义是:"可在民事和军事领域内保护网络空间的各种保障措施和行动,使网络空间免受各种与之相关的或可能损害与之相依存的网络和信息基础设施的威胁。"参见 European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, last accessed on 24 May 2015。

响的所有因素构成的有机体,包括指导理念、行动逻辑及具体措施。基于此,本文试图解读的是欧盟网络安全的整体战略,包括以《欧盟网络安全战略》为标志的政策体系、组织机构、技术保障、合作实践以及文化建设五大内容。它们涉及欧盟网络安全治理的各个方面,彼此协调,相互渗透,以确保欧盟在网络空间的根本利益。

与美国直接服务于其全球霸权的网络安全战略不同,欧盟的网络安全战略实质是用法治精神和欧洲价值观改造网络世界,从而能够在一个符合欧盟善治理想的网络政治生态中保护自身的数据隐私和信息安全,尤其是对公民个人数据隐私以及商业隐私的保护。因此,这是一种更偏重于治理层面的网络安全战略,有别于军事层面的美国网络安全战略。然而,受制于内部的诸多不利因素,欧盟为网络世界设计的制度规则能否最终演变为国际社会普遍接受的世界规则;它所做的内外协调努力又能否促成一个让自己在其中发挥领导作用的网络"利益共同体",都还是未知数。

一 欧盟网络安全战略的出台背景

由于网络安全国际立法的缺失,加上本身所具有的开放性和匿名性特征,网络空间成了一个易攻难守之地。信息技术越先进、对网络越依赖的国家也往往越容易使自己暴露于网络威胁之中,遭受猝不及防的攻击。欧盟正是这样一个一手执技术之矛、一手执风险之盾的网络行为体,因而其网络安全战略的目的是在抗衡网络安全风险的同时,利用自身的技术资源助推欧洲社会的整体进步,为欧盟赢得更广阔的发展空间和更重要的国际影响力。具体而言,就是为了应对严峻的网络安全挑战;保障欧洲智慧型增长模式的发展;改善欧盟内部网络安全管控资源碎片化的局面;竞争网络国际规则的话语权。

(一)应对严峻的网络安全挑战

欧盟是全球互联网体系最发达的地区,信息通信技术(Information Communication Technology,ICT)创造的产值在其 GDP 中占有可观的比重;固网、移动网络和卫星技术已覆盖到全部人口的 99.9%,①并支配着人们的日常生活方式。② 正是对网络服务的

① "欧盟发布 2013 年数字化议程评估报告(上)",中国经济网,http://intl.ce.cn/specials/zxgjzh/201311/21/t20131121_1788486.shtml,2015 年 5 月 24 日访问。

② 欧洲晴雨表调查显示,超过半数(54%)的欧洲人每天上网至少一次;半数左右的欧洲网民使用社交网站(53%)、网购服务(50%)或网银业务(48%)等网络服务。参见 European Commission, Special Eurobarometer 404, "Cyber Security", November 2013, http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf, last accessed on 24 May 2015.

高度依赖令欧洲人对于网络安全问题十分敏感。据估计,全球每秒约有 15 万个计算机病毒在互联网中流通,而这个数字也差不多是每天被病毒感染的计算机的数量。① 根据 Hackmageddon 网站统计,欧盟仅在 2012 年 10 月到 2013 年 5 月间就发生了 65 起网络攻击事件,最多的一个月(2012 年 11 月)达到 19 起;②而这只是"冰山一角"。欧洲晴雨表 2013 年的调查显示,欧盟网民中有 10%经历过网络诈骗,6%网上身份被盗,12%因网络攻击而被中断在线服务,12%被黑客攻击过社交媒体或邮件账户,另有 7%是网银诈骗的受害者。③ 如此大量的安全事件引发了民众对网络的信任危机,绝大多数人担心网站不能保护个人信息,并认为自己在过去一年里成为网络犯罪受害者的风险提高了。④ 2013 年的美国"棱镜门"事件⑤更加深了这种担忧。因此,提高网络风险抵御能力,树立民众对网络的信心就成为欧盟网络治理的首要任务。

(二)实现欧盟智慧型发展

2008 年全球金融危机发生后,欧洲经济增长停滞,暴露出欧洲经济的结构性缺陷。为重振经济、抱团取暖、提升整体竞争力,欧盟委员会在 2010 年 3 月公布了《欧洲 2020 战略》,⑥提出未来发展的三大方向:基于知识与创新的智慧型增长(smart growth),以有效利用资源和绿色环保为主的可持续增长(sustainable growth),以及提高就业率和增强社会凝聚力的包容性增长(inclusive growth)。作为智慧型增长的旗舰计划(flagship initiatives)之一,"欧洲数字议程"(A Digital Agenda for Europe, DAE)备受瞩目。DAE 从欧盟层面统一政策入手,把建设数字单一市场(Digital Single Market,DSM)和网络安全作为发挥欧洲 ICT 产业巨大潜力的重要保障。⑦ 在此基础上,欧盟于 2013 年 3 月正式推出了《欧洲网络安全战略》,为实现欧洲的智慧型发展目标保驾护航。

---

① Briefing of European Parliamentary Research Service, "Cyber Security in the European Union", 12/11/2013, http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf, last accessed on 24 May 2015.

② Neil Robinson et al., "Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts", pp.31-34, http://www.europarl.europa.eu/delegations/fr/studiesdownload.html? languageDocument=EN&file=96230, last accessed on 24 May 2015.

③ European Commission, Special Eurobarometer 404, "Cyber Security".

④ Ibid..

⑤ "棱镜门"是美国国家安全局和联邦调查局自 2007 年开始实施的一项代号为"棱镜"(PRISM)的全球电子监听计划,2013 年因前美国中央情报局雇员斯诺登泄密而被曝光。

⑥ "Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth", Brussels, 2010-03-03, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=COM:2010:2020:FIN:EN:PDF, last accessed on 24 May 2015.

⑦ DAE 共设七大目标 101 项行动措施。七大目标都是着眼于困扰欧洲 ICT 发展的主要问题,包括:建设数字单一市场;提升信息技术标准和兼容性;互联网信任与安全;提高宽带覆盖率;增加研发投资;提高全民数字素养;使用 ICT 技术应对气候变化等问题。参见 DAE 网站:http://ec.europa.eu/digital-agenda/en/our-goals,2015 年 5 月 24 日访问。

(三)整合内部网络安全管控资源

欧盟虽然不乏网络技术资源和庞大的 ICT 产业链,但未能合理配置各种资源,导致网络管控资源在联盟层面上交叉重叠,在成员国层面上又各行其道。在欧盟层面上,各个政策领域都有自己的网络管控部门,比如商业和政府部门的安全由欧洲网络和信息安全局(European Network Information Security Agency,ENISA)与欧盟委员会通讯网络、网络数据与技术总司(Directorate-General Communication Network Content and Technology,DG CNCT)负责;网络犯罪则由欧洲刑警组织(Europol)和欧盟对内事务总司(Directorate-General,DG HOME)负责;跨国网络安全和防御事务又是由欧洲对外行动署(European External Action Service,EEAS)和欧洲防务局(European Defence Agency,EDA)负责。这些部门存在明显的职责重叠现象,不仅容易造成多头管理,导致取证困难,而且容易造成资源浪费,影响欧盟处理突发事件时的针对性和有效性;而在成员国层面,各国 ICT 发展速度不均、网络管控资源分散的状况也很严重。比如德国从 1999 年起就开始规划网络安全战略及行动纲领,2001 年成立了反黑客预警系统,2010 年启动"数字德国 2015"战略;法国除了有国家级权限的"网络与信息安全局",还拥有自己的网络战部队;英国也早就有秘密的黑客部队,2009 年公布了它的《网络安全战略》并成立"网络安全办公室"和"网络安全行动中心"配合战略实施,2011 年再度出台新战略,还为此后四年的行动方案拨了 6.5 亿英镑的专项资金。相比之下,很多成员国却还缺乏相应的网络管控部门及打击网络有组织犯罪的必要工具,与发达成员国的差距非常大。① 以法律基础为例,欧盟 28 国中仅 19 国出台了网络安全战略,有 8 国(保加利亚、克罗地亚、丹麦、希腊、爱尔兰、马耳他、斯洛文尼亚和瑞典)连基本的法律框架都没有。即便是已有战略文件的国家,文件质量也参差不齐,许多只是高层的模糊表态而缺乏明确的实施计划。此外,仅少数国家更新过最初的战略,大部分国家都未对战略进行过修订和完善;同样,也只有少数国家为战略配套了相应的立法和政策工具以满足有关安全、信息分类义务和关键基础设施保护的要求。② 类似的差异还表现在网络安全管控主体、公私伙伴关系、网络安全教育等诸多领域。这些问题若解决不好,必然会成为欧盟网络治理中的一笔负资产,正如微软线上服务部门合作伙伴架构师马克·戴维斯(Marc Davis)所说:"如果铁路不具备交互性,那么火车就难以一

① 参见笔者接受中国社会科学院欧洲研究所关于欧盟网络安全的专访,2013 年 12 月 2 日,http://ies.cass.cn/Article/bwzf/201312/7805.asp,2015 年 5 月 24 日访问。

② BSA Report, "EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace", http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf, last accessed on 24 May 2015.

路畅通地行驶”。① 所以欧盟需要从整体上对资源进行统筹管理和优化布局,以克服网络安全战略执行过程中的内部阻力。

(四)竞争网络国际规则话语权

网络国际立法的缺失是传统国际法遇到的新挑战。从个体上讲,没有法律规则,网络犯罪和网络攻击就会失去底线,出现诸如网上租赁黑客服务的现象。这种服务根据买家希望实施的黑客行动进行收费,花 130 美元便可以黑掉某人的 Facebook 账户。② 从全球来看,国际法在网络空间里的“留白”也成为国家间无序竞争的温床。美国在当今互联网根服务器、域名及 IP 地址管理上握有重大发言权,③理论上可以对任何国家进行数据监控、信息窃取和网络攻击;而事实上也确实发生过利比亚的“.ly”域名、伊拉克的“.iq”域名、塔利班阿富汗的“.af”域名被美国随意屏蔽或处置的先例。美国利用这一优势争夺全球“制网权”以辅助其全球霸权战略。从近年来不断上涨的网络战预算和日益完善的网络战体系来看,美国正试图改变传统的作战工具和战争方式,从过去十多年依靠武力介入的地区中抽身出来,转而进入一个“虚拟战场”。从 2003 年伊拉克战争中的打印机病毒植入到 2010 年伊朗布什尔核电站离心机的“震网”(Stuxnet)攻击,再到 2014 年底朝鲜网络服务中断,美国的网络战已从最初附属于常规战转为“虚实结合”作战和单独作战。据全球最大的网络安全公司赛门铁克的报告,全球网路攻击源的数量美国位居第一,攻击量占世界总量的 25%;位于美国的僵尸控制服务器占到 33%;“钓鱼网站”占到 43%。④ 从 2010 年美军网络司令部正式运行至今,美国不仅突破常规扩军备战,而且先后制定了指导网络战争的《塔林手册》(2013 年)和《网络空间联合作战条令》(2014 年),从各个方面做足了网络战准备,使全球网络空间升起新一轮军备竞赛的硝烟。因此,尽早填补网络法律空白,出台规范网络行为体的国际公约具有相当的紧迫性。对欧盟而言,必须第一时间参与到国际规则的制定中去,将欧洲的话语体系纳入网络空间的游戏规则,让网络立法体现欧洲的价值观和行为准则,进而获得网络法治进程的主动权和话语权。

① http://www3.weforum.org/docs/WEF_GAC_Outlook_2013_CN.pdf, last accessed on 24 May 2015.

② http://europa.eu/rapid/press-release_SPEECH-13-105_en.htm, last accessed on 24 May 2015.

③ 目前全世界管理互联网主目录的根服务器共有 13 台,其中主根服务器放置在美国弗吉尼亚州的杜勒斯,其余 12 台辅根服务器中的 9 台也放置在美国,且所有的根服务器都受到由美国授权的互联网名称与数字地址分配机构 ICANN 的管理。

④ 秦安:“美国已完成发动网络战准备,各国招数”,中国军网,2014 年 4 月 17 日,http://www.mod.gov.cn/opinion/2015-04/17/content_4580616.htm,2015 年 5 月 24 日访问。

二 欧盟网络安全战略的演变

欧盟曾是与美国同处于第一梯队的信息技术开拓者,甚至可以说,没有欧洲人的早期贡献,恐怕就没有今天被称之为"Internet"的互联网。早在20世纪70年代初,法国软件工程师路易·普赞(Louis Pouzin)在自己领衔的Cyclades网络项目中发明了数据报(datagram),这种技术通过分拆数据包进行多路径传输,再整合还原初始信息,是最早的分组交换技术。可惜,这一得到蓬皮杜总统支持的科技项目在继任的德斯坦总统那里受到冷遇,不仅研究重点发生了变化,而且实验室经费也被中断,本可引领互联网技术的欧洲力量就此没落;而捡起了欧洲人技术的两名美国人罗伯特·卡恩(Robert Kahn)和温顿·瑟夫(Vinton Cerf)在此基础上建立了互联网的通用规则TCP/IP协议,成就了美国在互联网世界的领袖地位。①

除了错失在互联网世界的"领头羊"地位,欧盟的网络安全意识也是姗姗来迟。尽管高度依赖互联网,但直到2007年爱沙尼亚网络攻击事件②发生后,欧盟才真正将网络安全作为其安全治理的重要内容之一,而且战略的建设进程也比较缓慢,加之内部协调整合与外部竞争都困难重重,因而时至今日,欧盟已无法与美国比肩。

美国除了科技创新力强劲,还从克林顿政府开始就高度重视网络安全战略,将其作为国家安全战略的重要组成部分,而且明确将"制网权"作为网络安全战略的理论基础和目标导向,始终为打造并护持其网络空间霸权构筑技术与规则壁垒,形成了从关键基础设施防御、先发制人的网络攻击,到鼓吹"全球公域"(global commons)以谋取全球制网权的发展脉络。③ 来自美国制网权之争的压力因而成为欧盟在发展其网络安全战略时的一大动因。另外,自上世纪60年代以来,随着ICT产业的蓬勃发展,与该技术共生的网络和信息安全(Network and Information Security, NIS)事故也日益频繁,对欧盟及其成员国的数字经济和社会管理都造成了极大的困扰。于是,为了解

① Eric Albert, "Louis Pouzin, pionnier de l'Internet", *Le Monde Science et Techno*, 2013-02-07, http://www.lemonde.fr/technologies/article/2013/07/01/louis-pouzin-pionnier-de-l-internet_3439915_651865.html? xtmc=louis_pouzin&xtcr=2, last accessed on 24 May 2015.

② 2007年4月27日,爱沙尼亚政府将首都塔林市中心的一尊苏联红军纪念碑"青铜战士"拆除并移至塔林军人公墓,引发了占全国人口近25%的俄罗斯族人的不满,当日该国多个网站就受到疑似黑客利用僵尸网站发动的分散式拒绝服务攻击,一些网站的首页被换上俄国宣传口号及伪造的道歉声明,大量网站被迫关闭,其中包括总统的网站。由于爱沙尼亚近年来网络办公系统发展迅猛,国家生活已经极度依赖互联网,因此这场突如其来的网络攻击对该国造成了灾难性的打击。http://scholarcommons.usf.edu/cgi/viewcontent.cgi? article=1105&context=jss, last accessed on 24 May 2015.

③ 有关美国网络安全战略的发展脉络,参见程群:"美国网络安全战略分析",《太平洋学报》2010年第7期;沈逸:《美国国家网络安全战略》,北京:时事出版社2013年版。

决现实的和潜在的网络安全问题,整合欧盟内部的网络安全管控资源,确保数字经济的安全运行,实现未来“智慧型”发展目标,进而争取网络国际规制权和话语权,欧盟遂于上世纪末开始发展自己的网络安全战略。

从欧盟网络安全战略的发展历程来看,大体上经历了三个阶段:第一阶段是机制起步阶段(1993-2000 年)。1993 年,欧盟发布《德洛尔白皮书》①,首次将促进 ICT 产业的发展纳入其面向 21 世纪的宏观发展战略之中,决心改变发展模式,将建设信息社会作为欧盟 21 世纪的发展重心并为此配套完善的法制环境,以“保护数据和隐私”,“解决信息和通信系统的安全问题”;②第二阶段是机制升级阶段(2001-2009 年)。进入 21 世纪后,非传统安全问题日益严重, 2007 年的爱沙尼亚网络事件更是让欧盟体会到了网络攻击的切肤之痛,促使其开始真正重视网络安全,并以建章立制的方式推动网络安全战略向法制化和国际化的方向迈进。欧盟委员会在 2001 年的《网络和信息安全提案》③中首次提到了网络信息安全的重要性,2004 年创建了欧洲网络和信息安全局(ENISA),作为提高欧盟网络安全水平和促进成员国间信息交换、经验分享的重要抓手。在此基础上,2006 年的《确保信息社会安全的战略》进一步提出了要在欧洲范围内营造人人参与的网络安全文化。④ 2009 年 3 月,欧盟委员会又出台了关于《关键信息基础设施保护》(Critical Information Infrastructure Protection, CIIP)的通讯,⑤表明欧盟在经历重大网络安全事故后对待互联网的思路正由原来的“重技术研创,轻安全管控”向“一手抓技术、一手抓安全”转变,不再专注于个人数据与商业隐私保护,而开始筹划从成员国层面和联盟层面双管齐下,提升欧盟网络的整体抗风险能

① Commission of the European Communities, “Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century”, 5 December 1993. 这份白皮书旨在为欧洲经济的可持续发展奠定政策基础,从而使其能够应对国际竞争,同时创造成千上万个欧共体所需的工作机会。http://europa.eu/documentation/official-docs/white-papers/pdf/growth_wp_com_93_700_parts_a_b.pdf, last accessed on 24 May 2015.

② Council Decision of 31 March 1992 in the Field of Security of Information Systems (92/242/EEC), p.98, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:31992D0242&from=EN, last accessed on 24 May 2015.

③ European Commission, “Network and Information Security: Proposal for A European Policy Approach”, COM (2001) 298.

④ Communication from the Commission of 31 May 2006, “A Strategy for a Secure Information Society-Dialogue, Partnership and Empowerment”, COM(2006) 251 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:52006DC0251&from=EN, last accessed on 24 May 2015.

⑤ 该通讯包含了以下几个重点措施:准备和预知、监督和响应、减少损失和灾后重建、欧盟在世界范围内的合作、ICT 部门的准则。欧盟希望通过以上措施,将自身打造成一个在网络安全技术、管理、政策、法律等领域具有突出优势的新型联盟体。Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, “Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience”, SEC(2009) 399, SEC(2009) 400, COM(2009) 0149 final, http://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX:52009DC0149, last accessed on 24 May 2015.

力,保护欧洲免受大规模网络攻击和网络中断的风险;第三阶段是机制形成阶段(2010 年至今)。2010 年 5 月,欧盟发布了“欧洲数字议程”(DAE)五年计划,作为落实《欧洲 2020 战略》的“旗舰计划”之一;紧接着又于 2013 年 2 月 7 日正式推出了网络安全领域的首份战略文件——《欧盟网络安全战略:公开、可靠和安全的网络空间》(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)。文件指出,欧盟重点关注的对象是网络犯罪和关键性基础设施的安全,并在制度上设计了一张纵贯“成员国→欧盟→国际层面”的联动合作网络。这份战略文件的出台标志着欧盟在网络安全治理上正显示出独立、主动的姿态。尽管有些政策先行的味道,执行力也备受质疑,①但欧盟网络安全战略体系的整体架构至此已基本成型。

从总体上看,欧洲的网络安全战略还是以信息安全尤其是个人数据和商业隐私保护为主线,经历了从信息安全到数据安全再到网络空间安全的发展历程。与美国不同的是,欧盟对网络安全的治理更倾向于一种广泛而全面的社会治理模式,突出对公民个人权益的保护,把网络空间视为民主法治之地而非军备竞赛场所。

三 欧盟网络安全战略的保障机制

在缓解网络风险和整体发展压力的双重需求下,欧盟为自己的网络安全战略构建了一套涉及多层次、多主体、多向度的保障机制:

(一) 建立网络安全组织体系

与单个国家相比,欧盟的网络安全组织架构不仅极其复杂,而且在如何组织以及如何执行上也缺乏共识。这一方面是由于网络的开放性特征本身导致了一旦有安全风险,往往就会牵扯到政府、企业和消费者等多方利益,需要由公共部门和私营部门在一个跨学科的路径中采取协调一致的行动;另一方面也与以往欧盟层面上那些指定的问责(accountability)与责任(responsibility)的机构授权不无关系。②

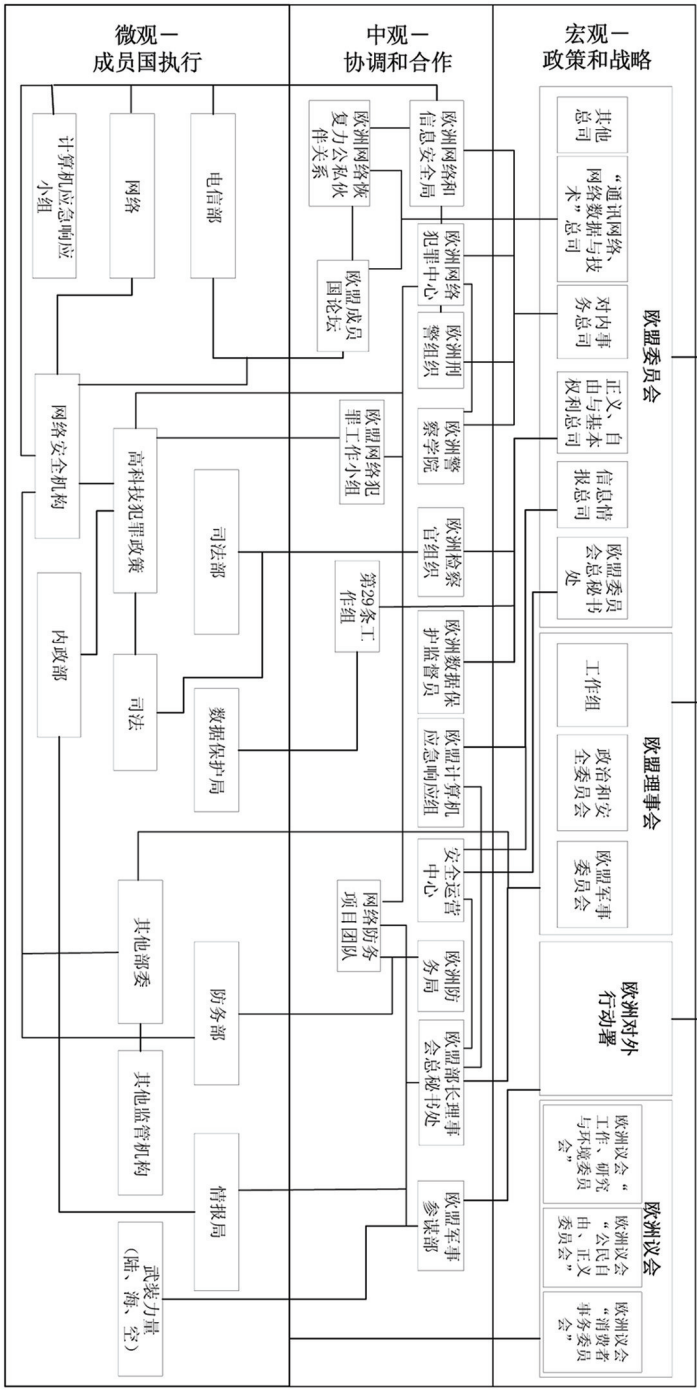
目前欧盟的网络安全管控机构大致可分为两类:一类是欧盟层面的核心机构,包括堪称欧洲网络“稳压器”和“领跑者”的 ENISA;③ 刚起步的欧洲网络犯罪中心 EC3

① Claudia Cencetti and Alessandro Marrone, “EU and Cyber Security: What's Next?”, http://www.european-globalstrategy.eu/nyheter/opinions/eu-and-cyber-security-whats-next, last accessed on 24 May 2015.

② Neil Robinson et al., “Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts”.

③ ENISA 成立于 2004 年,其作用是统筹协调欧盟机构、成员国和企业界的网络安全合作,具体工作包括:收集和分析网络安全威胁并向各方提供分析结果;提供相关咨询和帮助;协助欧盟开展国际合作等,以此提升欧盟网络与信息安全的整体水准。参见 ENISA 网站, http://www.enisa.europa.eu/, 2015 年 5 月 24 日访问。

图 1 欧盟网络安全管控组织系统



资料来源：Neil Robinson et al., “Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts”, p.81.

(The European Cybercrime Centre);①欧盟计算机应急响应小组(Computer Emergency Response Team-EU,CERT-EU);主要服务于政府部门的欧洲成员国论坛(The European Forum for Member States,EFMS)以及与之对应的负责私营部门的欧洲网络弹性公私伙伴关系(The European Public-Private Partnership for Resilience,EP3R)等。

另一类是与核心机构有密切关系的次要机构,扮演着辅助性的角色:或是支持网络性能或是处理突发事件的后果,如欧洲警察学院(The Collège Européen de Police,CEPOL)、欧洲数据保护监督机关(The European Data Protection Supervisor,EDPS)、欧盟隐私监管机构数据保护工作组(The Article 29 Working Party)、欧洲数字生活信任的公私伙伴关系(The European Public-Private Partnership for Trust in Digital Life,EP-TDL)、高级网络防御中心(The Advanced Cyber Defence Centre,ACDC)、事件响应小组网络(Networks of incident response teams)和反钓鱼工作小组(The Anti-Phishing Working Group,APWG)等。②

这两类机构在欧盟层面上进行复杂的互动,构成了欧盟网络安全治理的组织框架(见图1),其优点是机构范围广且针对性强,既有面向公共部门的,也有面向私营部门的;既有战略性的指导中心,也不乏直接解决突发事件的事故响应小组;但其缺点也很明显,主要就是前文述及的机构交叉与重叠,使不同组织间出现复杂授权和角色模糊现象,一旦发生网络安全事故,需要多方协调,这无疑会妨碍欧盟应对危机事件的效率。

(二) 建构、完善法律政策体系

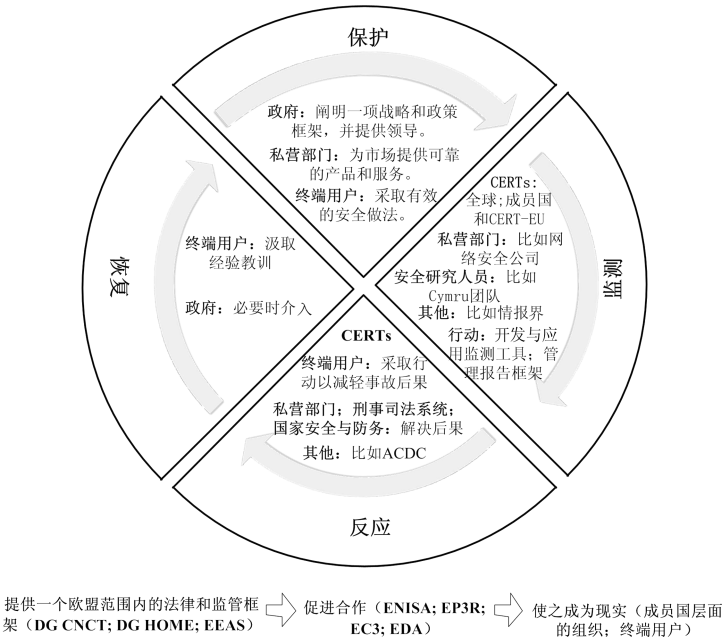
欧盟的网络法制建设并不与其ICT的持续发展保持同步,一项法律或政策的出台往往是为了解决实践中出现的某个具体问题,因此立法与政策不仅带有被动性和滞后性,而且"相关的立法与政策框架也是支离破碎",③这种情况直到2010年的《欧洲2020战略》出台后才有所改善;尽管如此,我们还是可以从中梳理出两条贯穿始终的脉络:一条是提高欧盟网络的弹性和事故反应能力;另一条是打击网络犯罪和网络恐怖主义。由这两条脉络串起的政策框架支撑着欧盟网络危机事件处理系统的运转(见图2)。

① EC3成立于2013年1月1日,隶属欧洲刑警组织,其使命是对付三方面的网络犯罪:(1)犯罪数额巨大的有组织犯罪,如网络诈骗;(2)对受害人造成严重伤害的网络犯罪,如网络儿童性虐待;(3)影响欧盟范围内关键基础设施和信息系统的网络犯罪。参见EC3网站,https://www.europol.europa.eu/ec3,2015年5月24日访问。

② Neil Robinson et al., "Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts".

③ Piotr Bąkowski, "Cyber Security in the European Union", Briefing of European Parliamentary Research Service 12/11/2013, http://www.europarl.europa.eu/eplibrary/Cyber-security-in-the-European%20Union.pdf, last accessed on 24 May 2015.

图 2 欧盟政策框架与网络危机事件处理系统



资料来源：Neil Robinson et al., "Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts", p.82.

首先，三份欧盟层面的战略文件与网络安全直接相关：第一份是 2010 年的《欧盟内部安全战略》(Internal Security Strategy，ISS)，该文件提出了保障欧盟安全的五大战略目标，①其中之一为"提高公民和企业在网络空间的安全级别"。文件呼吁成员国在欧盟层面上集中执法和司法力量，到 2013 年建立 EC3 并使之成为欧洲打击网络犯罪的中坚力量；加强各行各业利益相关者之间的接触与互动，优化信息共享与危机管理机制；要求成员国与欧盟机构到 2012 年时都拥有一套良好的计算机安全应急响应机制，与执法机关在危机预防和响应上加强合作，提高网络攻击处理能力。总体上，该战略强调 ENISA 在欧盟网络安全管理上的领导角色，认为该机构可以通过提升欧洲计算机应急响应小组(CERT)的标准来支持欧盟网络安全行动的落实，并支持开发一套

① ISS 列出的五大战略目标分别是：捣毁国际犯罪网络；预防恐怖主义和应对激进化与招募；提高公民和企业在网络空间的安全级别；通过边境管理加强安全；提高欧洲应对危机和灾难的能力。每个目标由少量可衡量的具体行动支持。参见 European Commission, "The EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe", COM(2010) 673 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=COM:2010:0673:FIN:EN:PDF#page=2, last accessed on 24 May 2015.

欧洲信息共享和预警系统(European Information Sharing and Alert System,EISAS)。第二份战略文件是2010年作为《欧洲2020战略》旗舰计划的"数字欧洲议程",该文件旨在建设欧洲数字社会的信任与安全,强调扩大欧盟CERT网络,为欧盟层面的机构设立CERT。第三份文件是2013年的《欧盟网络安全战略》,明确指出要为欧盟建成世界上最安全的上网环境,与之配套的还有确保促成欧盟范围内高度统一的网络和信息安全的指令草案,以及对这份指令草案影响评估的执行摘要等。《欧盟网络安全战略》作为欧盟在网络安全领域内的第一份政策性文件,对于完善欧盟网络治理的法律政策框架意义重大。

其次,提高网络弹性和事故响应能力的文件可分为两类:一类涉及网络和信息安全;另一类涉及关键基础设施保护。前者主要包括将网络安全纳入整体经济议程的《安全和信息社会战略》系列文件;①对ENISA重新授权的基本规章,以及为监督成员国在欧盟范围内进行有效的信息分享和高度统一的网络信息安全合作而建立机制的立法提案。② 后者主要包括2004年首次在打击恐怖主义问题中讨论关键基础设施保护(CIP)的委员会通讯;③强调CIP主要是成员国和基础设施所有者及运营者责任的理事会第2008/114/EC号指令,④以及受爱沙尼亚网络攻击事件刺激而提出由欧盟协调构建一个欧洲多主体共治框架的关键信息基础设施保护(CIIP)的通讯文件等。

最后,打击网络犯罪和网络恐怖主义的文件也可分为两类:一类涉及信息系统的保护,如2013年的指令文件对攻击信息系统的刑事犯罪定义及刑罚规则进行了基本规定;⑤另一类是与EC3有关的法律文件,由于该组织隶属于欧洲刑警组织(Europol),因此EC3的法律法规和执法网络很大程度上与Europol重合。

(三)信息技术保障

网络安全说到底,首先是个技术(以及对技术至关重要的标准)问题,然后才是政

① 包括2006年欧盟委员会通讯《安全的信息社会战略》(http://ec.europa.eu/information_society/doc/com2006251.pdf)及2007年的理事会决议《安全的信息社会战略——对话、伙伴关系和授权》(http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf),2015年5月24日访问。

② Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union, COM(2013) 048 final, http://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX:52013PC0048, last accessed on 24 May 2015.

③ Communication from the Commission to the Council and the European Parliament, "Critical Infrastructure Protection in the Fight against Terrorism", COM(2004) 0702 final, http://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX:52004DC0702, last accessed on 24 May 2015.

④ Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, http://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX:32008L0114, last accessed on 24 May 2015.

⑤ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, http://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX:32013L0040, last accessed on 24 May 2015.

治问题。欧洲曾开发出全球移动通信标准 GSM,在 ICT 领域具有雄厚的研发实力,但其成果整体转化率并不高,大多数提供信息和通信产品与服务的全球性大公司都在美国;而美国以其技术优势谋取网络空间的霸权,对欧盟的网络生存空间造成了一定的挤压。欧盟要想维护自身网络安全并争取国际网络规则的话语权,需要在以下两个方面努力:一是加大科技投资与创新力度,提高成果转化率;二是整合政策资源,搭建一个统一的欧盟技术政策框架。后者既是对前者的保障,也为前者指明方向,对于欧盟可持续地发展网络安全技术可谓意义重大。

欧盟的信息技术创新一直是整个网络安全体系建设的核心,欧盟通过多项科研资助计划鼓励本土团队为网络安全治理、个人数据保护、未来新技术开发等提供对策和产品。

欧债危机后,欧盟确定了以科技创新促经济增长的战略目标。在此目标下,欧盟推出了具有里程碑性质的 FP8——"地平线 2020"(Horizon 2020),仅 2014 年就有超过 10 亿欧元投入其中。欧盟希望通过重点资助 ICT 的创新研究来打造一个更具创业精神的 ICT 生态系统,一方面利用 ICT 创业实验室(ICT Entrepreneurship Labs)将创业者、学生、科研人员和公司联系起来,鼓励 ICT 创业;另一方面培育校内的 ICT 创业精神和创业技能,打造一批新生代的年轻创业者。① 在"地平线 2020"中,网络安全新技术的开发是重点优先课题,支持的研发创新项目经济社会效益明显,尤其是在网络安全保障、个人隐私权保护、风险预防应急和可靠信息自由获取等新技术开发方面表现突出。目前,欧盟层面正在实施的研发创新项目主要包括:维护网络安全与个人数据保护相辅相成的技术开发;互联网数字道德研究;创新型数字加密与识别技术开发;网络风险预测、分析、应急技术及工具开发;新型计算机网络攻击防护技术开发,以及基于光学技术的国防与网络安全技术研制等,②这些项目对欧盟网络安全战略的可持续发展意义深远。

(四) 安全合作实践

欧盟的网络安全合作对内表现为欧盟层面与成员国层面的双向合作,对外表现为与其他国家的双边合作以及在国际组织中的多边合作。这些合作形式旨在增强欧盟内部凝聚力,提高其在国际网络空间中的可见度和规则影响力。

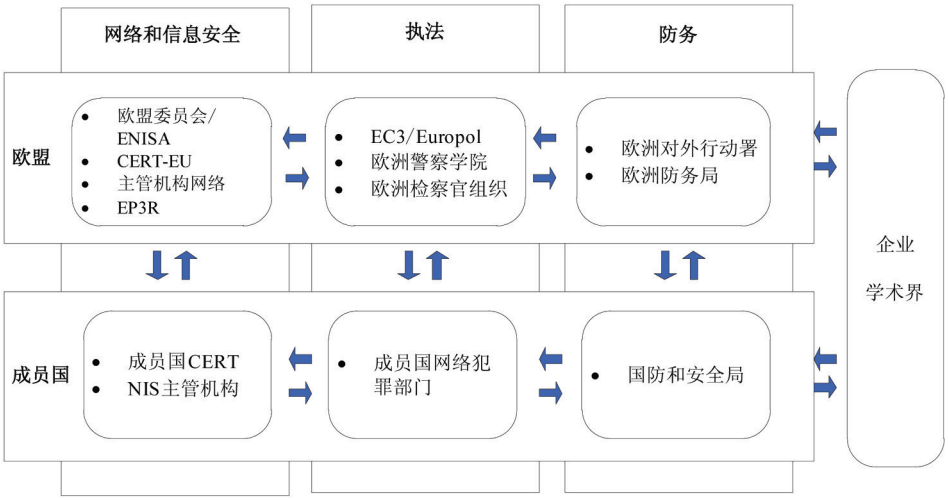
在内部合作方面,主要由 ENISA 负责欧盟机构、成员国和私营部门之间的信息沟

① ICT Innovation in Horizon 2020, http://ec.europa.eu/digital-agenda/en/ict-innovation-horizon-2020, last accessed on 24 May 2015.

② "欧盟网络安全保护五大指导原则",中国驻欧盟使团网站,2015 年 2 月 9 日, http://www.chinamission.be/chn/kjhz/t1235676.htm, 2015 年 5 月 24 日访问。

通与安全合作,形成联盟内部多利益主体共同参与的横向合作机制;与之相对的纵向合作则是在欧盟与成员国之间展开,欧盟通过为网络安全的三种主要形态——网络事故、网络犯罪和网络战争——配置三大解决部门(亦称“三大支柱”),即网络安全部门、执法部门和防务部门,来明确不同主体在各个问题领域内的角色和责任(见图 3),从而使成员国在治理网络安全问题上的政策和法律框架尽快与欧盟对接,优化资源配置,真正实现超越国家层面的网络安全合作。

图 3　欧盟-成员国网络安全双向合作机制



资料来源:European Commission, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, p.17。

在内部横纵联合的合作框架下,ENISA 与欧盟委员会内部研究机构“联合研究中心”(Joint Research Centre, JRC)在 2010 年发起了一项旨在测试泛欧洲国家网络弹性的实战演习计划——“网络欧洲”(Cyber Europe)。该计划从 2010 年开始,每两年演习一次,参加国须在位于欧洲某地的演习控制中心内按照“仲裁”系统的统一指示,对大量“植入”的网络攻击展开防御行动。以“欧洲网络 2012”为例,共有来自 339 个组织的 571 人参加了演习。这些组织主要来自于 25 个参演国和欧盟相关机构的网络安全机构、相关部门、电子政府服务所有者(the e-government service owners)、金融机构和网络服务供应商(ISPs),以及电信服务运营商等。① ENISA 根据演习情况总结出国

① ENISA, “Cyber Europe 2012: Key Findings and Recommendations”, p.5, http://fe-ddis.dk/cfcs/CFCSDocuments/Cyber%20Europe%202012%20-%20Key%20Findings%20Report-2.pdf, last accessed on 24 May 2015.

家合作、国际合作和网络演习本身的实际效果,并提出建议。

欧盟的对外合作渠道首先存在于国际组织中。目前联合国的专门机构——国际电信联盟(ITU)是讨论并制定网络技术标准、行为准则与安全措施的重要论坛;国际标准化组织(ISO)和国际信息系统审计和控制协会(ISACA)是重要的信息安全评价组织;经合组织(OECD)、欧安组织(OSCE)、信息社会世界峰会(WSIS)、互联网治理论坛(IGF)和网络空间会议(Conference on Cyberspace)等多边论坛都为欧盟寻求国际合作平台提供了选择。欧盟对外合作的另一个向度是双边合作,其中又以欧美合作为核心。北约网络防御卓越中心合作组织(CCDCOE)每年举办一次代号为"锁定盾牌"(Locked Shields)的多国演习,成为欧美合作的固定平台。2011 年 11 月 3 日,欧美借双边峰会的契机,在布鲁塞尔成功进行了"大西洋网络 2011"的联合演习。① 除美国外,欧盟也与中、俄、日、韩等其他国家就不同的安全议题开展双边或多边合作和演习。欧盟与中国在网络安全领域有很大的合作空间,双方在全球互联网管理的理念上有一些共同点,双方的 ICT 行业优势互补,且双方业已存在一些高水平的专家合作,比如由中国科技大学的潘建伟和维也纳大学的安东·蔡林格(Anton Zeilinger)分别领衔的科学家团队已在合作研发第一条连接亚洲和欧洲的量子网络,如获成功,那么他们将创造出一种超级安全的全球通信网络。② 未来的云技术、移动技术、5G 标准等也都是欧中合作的方向,特别是在 5G 标准制定上,由于 3G 时代专利技术被美国垄断,欧中没有话语权;4G 时代,欧中合作制定出了 LTE 标准,开始削弱美国企业在通信技术上的专利地位;对于即将到来的 5G 时代,欧中都希望能够增强自己的主动权和话语权。目前双方在 5G 标准的制定上看法一致,都倾向于在蜂窝网的基础上发展,而美国则希望在 Wifi 技术的基础上发展,如果欧中联手成功,那么美国将失去 5G 时代的领导权,③这对于要求改变以美国为中心的互联网管理现状的欧中双方来说,都是乐见其成的。④

(五) 建设网络安全文化

欧盟注重发动社会力量,动员一切网络利益相关者参与网络安全的文化建设工程,既加强同私营企业的合作关系,又注重发挥科研机构的创新优势,还重视培养欧洲

① EU-US Summit Joint Statement, Washington, November 28, 2011 (MEMO/11/842).

② Zeeya Merali, "Data Teleportation: The Quantum Space Race", *Nature*, 2012-12-05, http://www.nature.com/news/data-teleportation-the-quantum-space-race-1.11958, last accessed on 24 May 2015.

③ 青筠:"中欧化解贸易争端,联手电信 5G 标准",经略网,2014 年 11 月 17 日,http://www.jingluecn.com/spdp/1/2014-11-17/1105.html, 2015 年 5 月 24 日访问。

④ 刘长安:"保卫网络空间安全,各国施展锦囊妙计",C114 中国通信网,http://www.c114.net/news/16/a833692.html, 2015 年 5 月 24 日访问。

公民的网络安全意识,提高他们维护数据隐私和数据安全的自觉性和能动性。

自 2000 年起,联合国陆续通过了一系列涉及网络安全问题的决议案,①其中部分针对网络安全文化,比如 2003 年 1 月的联大第 57/239 号决议“培育全球网络安全文化”②和 2004 年 1 月的联大第 58/199 号决议“培育全球网络安全文化和保护关键信息基础设施”。③ 为落实决议精神,欧盟在 2003 年 2 月通过了“关于建立欧洲网络信息安全文化”的决议,明确了所有利益相关者在网络安全治理中的责任,并鼓励政府、企业和民众进行相互交流与合作。

就具体措施而言,虽然欧盟大规模的网络治理行动发生在 2007 年以后,但其内部很早就启动了网络安全文化的建设,“从娃娃抓起”,为青少年营造绿色网络环境。1999 年欧盟委员会推出“更加安全的互联网计划”(the Safer Internet Programme),旨在为儿童和青少年使用互联网保驾护航,使其免受网上非法和有害内容的侵袭。在该计划框架之下,欧盟参与资助的非营利性机构 Insafe 发挥了领航作用,它通过与行业、学校和家庭的紧密互动来唤起政府、教育者、家长和媒体等所有社会相关者的网络安全责任意识,为青少年弥合家庭和学校以及世代之间的数字鸿沟,最终达到保障公民权利和需求的终极目标。Insafe 除了监测网络趋势并提供研究报告外,还在欧洲内外的 30 余国建立了有关网络安全的认知教育中心(awareness center)、求助热线及青年论坛;它还从 2004 年起将每年 2 月的第二个星期二设立为“互联网安全日”(Safer Internet Day,SID),号召全民参与网络安全事业,创造一个更好的互联网环境。

通过上述行动,欧盟希望让所有利益相关者认识到网络安全所面临的严峻挑战,以及个体在整个“安全链”中的地位,营造一种“人人为我,我为人人”的合作防范意识,为联盟整体的网络安全文化建设铺路。继网络安全日活动获得成功后,再设立一个“欧洲网络安全月”(European cyber-security month,ECSM)的想法也更易于推行了。历经两年酝酿之后,欧盟最终将 2013 年 10 月设定为“欧洲网络安全月”,甫一推出即得到了多个欧盟成员国的积极响应。“欧洲网络安全月”的目标是推动欧洲民众的网络安全水平,改变民众对于网络威胁的认知,并通过教育和共享好经验等措施为其提供最新的安全信息。④

① 比如关于建立法律基础以打击滥用信息技术犯罪的联合国大会第 55/63 号决议(2000 年)和第 56/121 号决议(2001 年);关于在国际安全背景下发展信息技术的联合国大会第 53/70 号决议(1998 年)、第 54/49 号决议(1999 年)、第 55/28 号决议(2000 年)、第 56/19 号决议(2001 年)和第 57/53 号决议(2002 年)。

② http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf, last accessed on 24 May 2015.

③ http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf, last accessed on 24 May 2015.

④ http://www.cepolicy.org/publications/cyber-security-raising-awareness-understanding-it, last accessed on 24 May 2015.

四 欧盟网络安全战略面临的挑战

欧盟发展网络安全战略的动因和目的既是在技术层面上应对网络攻击和网络犯罪,也是在政治和法律层面上争取更具独立性的制网权。尽管美国是它迄今为止关系最密切的合作伙伴,但在网络安全方面,两者无论在战略理念还是运作实效上,都表现得大不相同。就现实的政治生态来看,欧盟的网络安全治理恐怕不仅在具体落实上存在较大的难度,而且远期表现也不容乐观。

欧盟与美国在网络安全战略上的本质区别在于理念。美国遵循军事进攻型的网络安全自助法则,将"制网权"作为网络安全战略的理论基础和目标导向,用"假想敌+先发制人"的手段主动出击,突出了网络安全的威慑性和惩罚性,说明美国对待网络生态的理解是和物理世界如出一辙的丛林法则;这从它发动的各类网站战到"斯诺登事件"和"棱镜门"丑闻中早已一览无遗。与此相反,欧盟更倾向于一种自我保护型的网络安全战略,在该战略的设计与实施过程中,规则意识、价值认同和合作文化占据主导地位,欧盟希望将网络变成自己实践善治理念的又一个试验场,在其中推广欧洲价值观与法治经验,以此保障欧洲公民在网络世界里的权利和利益,并为网络国际规则建设提供经验。欧美的这种理念分歧在 2013 年的"棱镜门"事件中得到放大。事实上,引起欧洲大陆政治地震的不是美国情报机构的情报搜集工作,也并非被监听领导人的个人情感,而是美国的窃听行为触犯了欧盟对于网络治理的基本理念,即无节制、低成本地搜集情报打乱了网络运行的秩序规则;监听欧洲公民违背了欧盟对个人数据隐私和公民权益的价值认同;对欧洲盟友的监听又破坏了盟友间的政治信任。因此,尽管内部意见存在分化,但德国总理默克尔的愤怒仍然具有相当普遍的代表性。默克尔甚至高调提议建立欧洲自己的数据网,以取代美国主导的互联网基础设施。① 不管这一建议的可行性有多大,"棱镜门"事件至少加速了欧盟数据立法的进程,欧洲议会公民自由、司法与内政事务委员会(LIBE)在当年的 10 月就通过了新版《欧盟数据保护法》,增加了更为严格的反外国情报监视内容,成为首部真正意义上保护 5 亿欧盟公民数据资料及隐私权的重要法律。② 欧盟还计划在 2015 年内完成一部欧洲大陆通用的数据保护法规(General Data Protection Regulation),推动数据保护的改革进程,使

① "默克尔支持建立'欧洲版'互联网",FT 中文网,2014-02-17,http://www.ftchinese.com/story/001054853,2015 年 5 月 24 日访问。

② "欧洲议会司法内政委员会通过新版数据保护法,欧盟数据保护立法取得重大进展",法制网,http://www.legaldaily.com.cn/international/content/2013-10/29/content_4969345.htm,2015 年 5 月 24 日访问。

“欧盟持有个人数据保护的全球黄金标准”,[①]这似乎也是欧盟竞争网络国际话语权的武器之一。然而,短期内美国在关键基础设施、域名及 IP 地址管理上仍具有垄断地位,欧盟内部因为持续的经济困难而导致的信任危机和一体化发展的瓶颈也制约着欧盟网络战略的发展,“欧洲方式”多少有些过于理想化。

当然,欧盟网络安全的战略框架有其特色:一是法律规范与执行机构相配套。欧盟建立了一套与物理世界一脉相承的网络法律规范体系,以此方式输出制度经验,有望在个人数据保护等领域的国际立法中获取较大的话语权。与立法相配套的是一系列专门机构的建设,特别是欧洲网络和信息安全局 ENISA 和欧盟打击网络犯罪中心组织 EC3 正在网络治理中发挥越来越重要的作用,这有助于欧盟改善内部管控机制分布不均且资源重叠的现象,形成欧盟自己的管控核心及由此向外辐射的调控网络;二是内部多元多级联动治理。欧盟 2009 年提出的“多主体治理路径”强调政府、企业和个人都是网络治理的利益攸关方,并针对不同主体制定了不同的行动方案。这种多元共管、多级共治的方式有助于最大限度地调动社会力量,让社会成员分摊网络安全责任,共同推动建设进程。在当前外部网络空间权力格局尚未明朗,至少美国是否真正会放权给“全球多利益攸关方”[②]还未可知的情况下,努力打造一个团结的“内部多利益攸关体”不啻为务实之举;三是重视网络安全的文化顶层设计。在营造网络安全文化方面,欧盟善于动员社会力量,向民众普及网络安全防范意识,这也有助于保障官方网络安全战略的实现。

尽管如此,欧盟网络安全战略的执行效果还存在诸多不确定因素。短期内,欧盟必须面对不少积重难返的矛盾:从内部看,一方面是网络安全管控资源的统筹协调尚需时日,在未解决资源散乱的局面以前,势必会遭遇效率低下的情况;另一方面是提升欧洲民众对网络安全的信任度也非易事,特别是经历了“棱镜门”事件后,民众对于个人数据和隐私的保护意识更高,甚至对安装智能电表之类的公共服务所产生的数据共享也感到担忧,这显然不利于欧盟正在积极推动的数字单一市场和全民参与的网络安全战略建设。从外部看,欧盟也面临两个主要问题:一方面是与美国竞争网络治理的发言权和话语权;另一方面是与北约竞争网络安全管控资源。美国不仅在网络核心技术领域占尽先机,而且对网络价值的认知和国家意识的觉醒也都先于欧盟,它早在

① SC Magazine News, “New EU Data Protection Law to Arrive in 2015”, http://www.scmagazineuk.com/new-eu-data-protection-law-to-arrive-in-2015/article/395142/, last accessed on 24 May 2015.

② ICANN Press Briefing, “Administrator of Domain Name System Launches Global Multistakeholder Accountability Process”, 14 March 2014, https://www.icann.org/resources/press-material/release-2014-03-14-en, last accessed on 24 May 2015.

1991 年的海湾战争期间就提出了“信息战”概念,在过去的 20 年里也一直致力于将网络打造成为继陆、海、空、天之后美国推行全球霸权的空间依托,最近几年又开始拼命鼓吹“全球公域”概念,实际上也是打着维护网络开放与稳定的旗号为自己的制网权“造法”。相比之下,欧盟不仅缺乏硬实力,更缺乏危机意识,假若以 2007 年爱沙尼亚网络攻击事件后欧盟的真正觉醒为起点,它也比美国足足晚了 16 年。如果说欧盟找到了某种与美国错位竞争的路径,那么它的制度建设还有可能会使其享有一定程度的规则引领作用和示范价值;否则,欧盟将不仅在 ICT 行业的全球竞争中失去优势,而且数据流入美国手中,还将丧失自己的网络行动力和战斗力。因此,欧盟如何利用自己的优势与美国展开数字产业与网络安全竞争是其必须面对的一大课题。此外,与北约的资源竞争,说到底还是绕不开与美国的关系。以美国为首的北约拥有自己的网络防御基础设施,包括指挥、控制、通信、计算机和信息系统,且已经可以实现超国家的网络防御方案。尽管受制于其成员国之间技术水平的差异,以及“棱镜门”事件所造成的欧洲盟国与美国之间的隔阂,北约的一体化建设似乎并不那么顺利,但这并不妨碍美国在北约网络管控系统中的领导地位,各项措施也都服务于美国的国家利益。相比之下,国别差异同样严重的欧盟内部由于缺少一个绝对权威,在集体安全防卫上一直举步维艰,“共同防御”之名往往流于形式,最终的责任还是落在各个成员国的身上。北约目前 28 个成员国中大部分是欧盟国家,如果欧盟自己的网络安全体系发展不起来,那么资源很容易流向北约,为美国做了“嫁衣裳”,致使欧盟在网络安全管控方面仍然受制于人,不利于其网络安全战略的长远发展。

(**作者简介**:周秋君,上海政法学院国际事务与公共管理学院讲师;**责任编辑**:张海洋)