“斯诺登事件”后美国网络情报政策的调整*

汪晓风

[内容提要] “斯诺登事件”后,美国政府通过加强网络情报监管,推动立法和行政措施规范网络情报搜集、存储、应用和共享流程,纠正一些侵犯公民个人隐私和有违公司商业利益的做法,以化解内外压力。同时加大投入,应对网络空间发展和大数据、人工智能等新技术应用带来的机遇和挑战。美国政府将会更加重视网络情报活动,也会更加谨慎地令网络情报项目隐秘地运行。而在较长时期内,国际社会难以维持持续外部压力和建立有效约束机制,使美国大规模监控全球互联网的活动对网络空间和国际关系的威胁依然存在。

[关键词] 美国 “斯诺登事件” “棱镜计划” 网络情报

[作者介绍] 汪晓风,复旦大学美国研究中心副研究员,主要从事美国政治与外交、网络安全与网络外交研究。

2013 年 6 月,爱德华·斯诺登(Edward Snowden)曝光美国国家安全局“棱镜计划”等多个大规模网络监控和情报搜集项目,这些网络情报项目监控范围之广、情报搜集能力之强令人瞠目,美国国内公众和国际社会纷纷要求美国政府限制网络监控活动、规制网络情报行为和保护个人隐私数据。迄今,“斯诺登事件”已过去五年,而美国依然在对全球网络空间进行监控,其范围和力度还在不断扩大,外界对该计划的关注和压力则逐渐消退。那么,美国政府为何执意继续进行网络情报活动?又是如何化解各方压力?其未来进一步走向如何?本文拟梳理“斯诺登事件”后美国网络情报政策的调整,分析其变与不变的主要理由,并简要评析其影响。

一

“棱镜计划”等网络情报项目曝光后,美国政府面临很大压力,美国国内公众抗议情报机构的网络监控侵犯个人隐私,国际社会则指责美国政府滥用技术和资源优势,即便是盟友伙伴也因遭受秘密监控而表示愤慨,参与“棱镜计划”的主要互联网企业也力图与国家情报项目撇清关系或保持距离。在此种形势下,美国政府需要安抚社会公众、稳住合作企业、劝服盟友伙伴,同时加强网络情报监管,使其“合法合规”运行。为此,“斯诺登事件”后美国政府对相关政策讨论持开放态度,甚至主动设置和引导议题,及时充分的政策讨论一定程度上纾缓了激愤情绪,也有助于了解各方的重点关切和对于政策调整的可能反应。总体而言,相关政策辩论主要围绕以下三方面展开:

第一,关于网络情报活动的合法性。政策辩论首先触及到监控的法律依据,国家安全局通过“棱镜计划”进行网络监控和情报搜集是否合法?引发质疑是因为项目设立缺乏相应法律支持,还是项目执行超越了法律授权?美国家安全局称,“棱镜计划”搜集的是电信通话和网络会话的“元数据”,[①]并非通话或会话内容,因而不需要事先取得单独授权。

* 本文是国家社科一般项目“美国棱镜计划的系统分析与综合应对”(项目号:15BGJ049)的阶段性成果。

① “元数据”是结构化数据的数据,用于描述数据的属性(名称、大小、数据类型等)、结构(长度、字段、数据列)、归属(位于何处、如何联系、拥有者)等基本信息。“棱镜计划”搜集的数据主要针对元数据,包含互联网会话的客户端和服务器端 IP 地址、电信通话的双方号码、会话或通话的起讫时间等基本信息,但不包含会话和通话的内容。

质疑者援引美国宪法第四修正案，认为无论何种搜查，都应针对特定嫌犯，且应具备合理依据和司法授权。网络监控侵入目标系统或窃取储存数据，类同于住所或人身被搜查，根据这一理解，国家安全局和联邦调查局等情报和执法部门是在未获得单独授权的情况下，对大量未被列为恐怖嫌犯、也没有实施犯罪行为的对象进行搜查。民权组织“美国公民自由联盟”（American Civil Liberties Union）据此向纽约南区地区法院提起诉讼，指控国家安全局大范围搜集用户数据，涉嫌违宪，请求联邦法院下令终止这一监控项目，清除收集到的记录。①

时任总统奥巴马则认为，这一监控项目经国会授权，已运行多年，②其合法性不容质疑。时任国家情报总监詹姆斯·克拉珀（James Clapper）援引 2008 年《外国情报监视法案》修订案第 702 条款为“棱镜计划”辩护，该条款规定，司法部长和国家情报总监可以授权情报机构对非美国居民的通信或会话进行监控，时间最长可达一年。针对一些互联网企业为“棱镜计划”提供数据访问接口涉嫌违法，则以《爱国者法案》第 215 条款辩解。该条款规定，为外国情报搜集和国际恐怖主义调查获取商业记录，可请求外国情报监视法庭传票，要求从运营商获取服务器日志，并对“善意披露”给予豁免。③ 这意味着运营企业按照法庭指令，为情报机构提供包含公民个人信息及隐私的内容，可免予起诉。这就为网络内容服务提供商与情报机构合作，提供用户信息和元数据消除了法律上的后顾之忧。可见立法者早知进行网络监控可能遭遇公众质疑和法律风险，已经预先为参与各方设置了免责条款。

另一与合法性相关的争议是通过网络窃取商业机密的问题。美国惯常指责外国政府通过网络窃取美国企业的商业机密和科研机构的技术专利，严重削弱美国经济和科技竞争力。但美国各情报机构也非常重视这一蕴含重要经济和政治情报的信息来源，并特意将自身从事系统入侵的行为合法化。奥巴马宣称，“如果这些情报有益于美国的国家安全，或者其盟友伙伴的安全，那么美国情报部门仍然可以搜集这些信息。”为了与美国惯常指责的窃取商业机密活动区别开来，奥巴马还强调情报机构未从网络情报搜集中获取商业利益，称美国政府“没有授权对外情报或反情报机构基于为美国公司或商业部门谋取竞争优势的目的搜集上述信息。”④从而将判断合法性的重点转向是否具有谋取商业利益的意图上。为了最大限度维持网络情报的合法性，美国政府构建了一种奇怪的逻辑：当手段受到质疑时，则强调目标合法性，当目标受到质疑时，则强调意图的特殊性。

第二，关于网络情报的有效性。质疑者主要关注网络情报的巨大投入究竟在什么程度上有助于反恐目标。“9·11 事件”后，反恐成为美国情报界⑤的工作重心，而恐怖主义组织也在积极利用互联网的便利，进行宣传、招募、联络、筹资等活动。受网络情报化的趋势和网络恐怖主义的双重影响，网络情报越来越受重视，搜集和监控范围不断扩大，数据存储和处理中心越建越大，财政预算也不断增加。美国的情报预算长期以来秘而不宣，在奥巴马“开放政府”理念指导下，2010 年联邦政府首次公布情报预算，情报界共获财政拨款 801 亿美元，其中国家情报项目 531 亿，军事情报项目 270 亿，且增幅大大超过联邦预算的平均增幅。⑥ 由于网络情报对人员、技术和硬件有很高要求，因而一些项目耗资尤其巨大，“9·11”后仅破解加密数据的项目就耗费了数十亿美元，如一个专攻密码分析和破解的“布尔朗”

① Ellen Nakashima and Scott Wilson, “ACLU Sues over NSA Surveillance Program,” *The Washington Post*, June 11, 2013, https://www.washingtonpost.com/politics/aclu-sues-over-nsa-surveillance-program/2013/06/11/fef71e2e-d2ab-11e2-a73e-826d299ff459_story.html.（上网时间：2018 年 5 月 22 日）

② “棱镜计划”为绝密项目，2013 年 6 月，媒体根据斯诺登曝光的项目代码推测出该计划的启动时间为 2008 年，可与此形成印证的是，2008 年 7 月美国国会通过《外国情报监视法案》修正案，国家安全局获得执行电信和网络监控的新授权。

③ U.S. Public Law 107-56, “Uniting and Strengthening America by Providing Appropriate Tools Required Intercept and Obstruct Terrorism (USA PATRIOT Act of 2001),” https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.（上网时间：2018 年 5 月 22 日）

④ White House, “PPD-28: Signals Intelligence Activities,” https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.（上网时间：2018 年 5 月 22 日）

⑤ “情报界”（intelligence community），美国联邦层级各情报机构的统称，当前美国情报界由国家情报总监办公室和 16 个分属国家安全委员会和联邦各部的独立情报机构组成，亦译作“情报系统”。

⑥ Paul R. Pillar, “Think Again: Intelligence,” *Foreign Policy*, Vol. 191, January/February, 2012, p.52.

(Bullrun)项目 2013 年预算就达 2.5 亿美元。

一些观点认为,“棱镜计划”获取很多生活细节或个人隐私,并不有助于国家安全和外交决策,为此投入庞大资金和人力,是滥用政府预算。对此,情报界力图证明网络情报的高额投入是物有所值的,时任联邦调查局局长罗伯特·穆勒(Robert Mueller)表示,“棱镜计划”帮助政府在全球范围内挫败 50 多起潜在的恐怖袭击计划,包括一起试图用炸弹袭击纽约交易所所的计划。时任国家安全局局长基斯·亚历山大(Keith Alexander)在众议院情报委员会作证时,也确认“棱镜计划”获取的情报帮助美国避免了 54 起恐怖袭击,而且预谋的恐怖袭击 90%以上都是被“棱镜计划”击破的。然而,时任国家安全局副局长克里斯·英格利斯(Chris Inglis)被追问时承认其中仅 11 或 12 起与美国本土有关,而明确针对美国人恐怖图谋的实例其实仅有一起。①

第三,关于安全与隐私的平衡。相关讨论的核心是国家安全和反恐目标究竟可以在多大程度上以个人权利为代价,抑或执法和情报机构应当如何把握两者之间的平衡。“斯诺登事件”中,除“棱镜计划”外,还有多个网络情报项目陆续曝光,如从光纤主干网收集数据的“上游”(UpStream)项目、监控互联网重要节点的“关键得分”(X-Keyscore)项目等,监控对象从各国政要到普通公众无所不包,盟友伙伴和敌对国家概莫能外。这些网络监控项目搜集的数据汇总到统一的存储和分析平台,即便获取的数据仅为元数据,根据数据之间的相关性,也可挖掘出大量个人隐私。这就引发了国内关于公民隐私和国际上对于网络空间主权管辖的各种讨论。

国会议员出现分歧。参议院多数党领袖米奇·麦康奈尔(Mitch McConnel)希望保留 2001 年《美国爱国者法案》赋予情报机构的所有监控能力。参议院情报委员会主席戴安娜·范斯坦(Dianne Feinstein)认为有必要为网络监控提供法律支持,她提议允许情报机构继续进行无证搜索,只要它们保留侵入系统的记录并可供各机构审查。② 众参两院司法委员会的两位主席众议员詹姆斯·森森布雷纳(James Sensenbrenner)和参议员帕特里克·莱希(Patrick Leahy)则主张限制国家安全局拉网式的网络监控活动,禁止无理由收集美国公民的电话和上网记录,森森布雷纳认为应回到以往目标明确的监控模式,“情报机构应该按图索骥,而不是在我们的私人数据中大海捞针”。③

奥巴马曾经承诺结束小布什政府过度强调国家安全但忽视个人隐私的做法,要在两者之间达成更好的平衡,但政策辩论也显示奥巴马政府的天平仍然向安全目标倾斜。奥巴马辩称“棱镜计划”并不针对美国公民或境内的外国人,“你可以武断地抱怨这是‘老大哥’式的监控,以及这是一个错得多么离谱的秘密项目。而当你认真了解相关细节时,会同意我们已经达到了平衡”,④奥巴马所说的平衡,即是国家安全目标与现有立法所保护的个人权益之间的平衡。关于网络监控的各种辩论,重新激起了“9·11”后困扰美国社会的一个未决之难题,多数公众都承认恐怖主义的现实威胁,认可通过加强监控及时获悉恐怖情报,但美国公众又很难在恐怖袭击威胁和个人隐私伤害之间作出非此即彼的选择。

二

基于“斯诺登事件”后的政策辩论,以及为了确保国家安全和外交决策继续获得网络情报支持,美国政府的网络情报政策调整主要围绕两大“主线”展开:一是确保依规合法,即着眼于化解压力和改善流程,重点明确网络情报活动的边界,理顺部门间、政企和国际伙伴的协同关系;二是确保能力提升,即紧跟网络空间环境的变化及网络技术的发展,进一步提升情报界通过互联网搜集、处理和分析情报的能力。

第一,明确网络情报活动应遵循“特定必要”原则。2014 年 1 月 17 日,奥巴马发布旨在改革信号

① [英]卢克·哈丁著,何星等译《斯诺登档案:世界头号通缉犯的内幕故事》,金城出版社,2016 年,第 234 页。

② Michelle Richardson, “Dianne Feinstein's Fake Surveillance Reform Bill,” *The Guardian*, November 8, 2013, http://www.theguardian.com/commentisfree/2013/nov/08/dianne-feinstein-nsa-intelligence-reform-bill. (上网时间:2018 年 5 月 22 日)

③ [英]卢克·哈丁著,何星等译《斯诺登档案:世界头号通缉犯的内幕故事》,第 236 页。

④ Timothy B. Lee, “Here's Everything We Know about PRISM to Date,” *The Washington Post*, June 12, 2013, https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date. (上网时间:2018 年 5 月 22 日)

情报活动的总统政策指令，明确强调信号情报必须基于“法律、行政命令、公告或其他总统指令授权，并根据宪法和相关法律、行政命令、公告和总统指令进行。”①从而限制了扩大情报搜集范围和增加情报技术手段的可能性，而这以往被视为情报活动创新和情报机构自由裁量的表现。同时，该总统行政令还要求对收集电话通话和网络会话记录等情报活动加强监管，提高情报工作审查层级、限制情报部门拦截国际通信的权限、提高联邦调查局使用国家安全密函的透明度、不再由政府保存通话记录、限制网络数据的存储和使用等等。

“斯诺登事件”激发了国会网络情报监管立法的热情，自“棱镜计划”曝光至 2013 年底，半年间参众两院已提出近 30 个与网络情报相关的单独法案，大多围绕规范网络监控活动，包括增加透明度、严格外国情报监视行动审核流程等。2015 年 6 月，国会通过《美国自由法案》(USA Freedom Act of 2015)，明确规定情报机构不能不加区分地大规模收集美国公民的通话数据，情报机构进行监控或获取数据之前，应就每一项具体行动事先向外国情报监视法庭申请，然后据此向电信或互联网公司索取特定记录和数据。如怀疑特定个人与已知或疑似恐怖分子进行接触，需要获取运营商储存的数据，必须事先取得外国情报监视法庭提供的许可文件，才能调取并审查相关数据记录。② 《美国自由法案》还赋予外国情报监视法庭更明确的监管职责和审核要求，自 2015 年开始，美国法院行政办公室(The Administrative Office of the U.S. Courts)应公布年度外国情报监视法法庭③处理监视请求的统计信息。从已公布三个年度的数据来看，被驳回或部分驳回的监视或搜查申请有明显上升，2015 至 2017 年被驳回或部分驳回的搜查申请分别是 5、35 和 76 项。④ 这与“9·11”后至“斯诺登事件”前非常宽松的审核程序形成鲜明对比。2001 年至 2012 年期间，外国情报监视法庭一共审核了 20909 份监控或搜查申请，仅仅驳回了 10 份申请。⑤ 这一定程度上表明，外国情报监视法庭执行审核和监管变得更为严谨严格，更重视程序的依规合法。

第二，改善对个人隐私权的尊重和保护。隐私权及更广泛的公民自由权利是美国的基本价值观和立国之本，“棱镜计划”等网络情报项目最令美国公众不满的是不加区分地监控。在公众舆论和公民权利组织的压力下，国会和行政部门对网络情报可能影响个人隐私的做法采取了一些具体限制和保障措施。

立法层面，《美国自由法案》禁止情报机构在无明确理由的情况下收集美国人的通话记录，不论身居何处，都禁止对其拉网式的监听和先取后查。情报机构还尽量避免侵害美国公民和身处美国的外国公民，因为这些对象可能会以美国法律起诉他们。另外情报机构获取和处理个人网络数据受到更为严格的限制。2018 年 4 月国家情报总监办公室发布了一份国家安全机构透明度报告，宣称随着一系列保障公民权利措施的实行，“美国人及境内外国人的隐私权益和政府的国家安全利益之间已经达到了合理的平衡。”⑥

尽管美国政府经常宣扬公民权利和个人自由等价值观的普适性，但在具体立法和政策中，几乎毫无

---

① The White House, “PPD-28: Signals Intelligence Activities,” https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. (上网时间:2018 年 5 月 22 日)

② U.S. Public Law 114-23, “Uniting and Strengthening America by Fulfilling Rights and Ensuring Discipline over Monitoring Act of 2015 (USAFREEDOMAct of 2015),” https://www.gpo.gov/fdsys/pkg/PLAW-114publ23/html/PLAW-114publ23.htm. (上网时间:2018 年 5 月 22 日)

③ 外国情报监视法法庭(Foreign Intelligence Surveillance Act Courts)包括外国情报监视法庭(Foreign Intelligence Surveillance Court,FISC)和外国情报监视上诉法庭(Foreign Intelligence Surveillance Court of Review, FISCR)。

④ Director of the Administrative Office of the U.S. Courts, “Director's Report on Foreign Intelligence Surveillance Courts' Activities of 2017,” http://www.uscourts.gov/statistics-reports/analysis-reports/directors-report-foreign-intelligence-surveillance-courts. (上网时间:2018 年 5 月 22 日) 其中，2015 年的数据从《美国自由法案》生效之日起开始统计。

⑤ 也有观点认为外国情报监视法法庭的数据经过了技术处理，如情报机构被驳回的申请经修改后，再次向外国情报监视法庭提出申请，如果获得了许可，则申请获准数增加，但不会减除被驳回申请数。相关分析可见 Conor Clarke, “Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?” Stanford Law Review Online, Vol.66, February 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2511653. (上网时间:2018 年 5 月 22 日)

⑥ U.S. Office of the Director of National Intelligence, “Statistical Transparency Report Regarding Use of National Security Authorities: Calendar Year 2017,” https://www.dni.gov/index.php/newsroom/press-releases/item/1867-odni-releases-annual-intelligence-community-transparency-report. (上网时间:2018 年 5 月 22 日)

例外地将需要向外国情报监视法庭申请许可的对象范围表述为“美国公民和境内外国人”，显示其他国家公民的个人隐私并不受美国政府尊重和保护，自然也不是网络情报政策调整的重点。然而“斯诺登事件”中一系列被曝光的诸如针对巴西总统、德国总理、墨西哥总统、罗马教皇等外国政要的监控，以及对法国和西班牙公众大规模的数据搜集不仅触犯个人隐私，还引发了盟友伙伴之间外交纠纷，迫于国际压力，美国政府还是作出了一些姿态，表示外国公民的个人权利也会得到适当尊重和保护。2015 年 2 月 3 日，总统国土安全及反恐事务助理发布声明，要求情报人员对数据库中涉及外国公民的记录进行甄别，5 年之内逐步删除没有情报价值的外国公民个人信息。① 但是，这一宽泛的承诺并没有相关监管程序予以保证。

第三，设法使网络情报活动回归隐秘状态。网络情报是信号情报的一部分，需要针对特定目标执行实时监控而获取数据，并进行深度挖掘，从海量数据中获取有价值的信息。网络情报的监控对象是互联网数据传输和会话，必须覆盖尽可能广泛的数据来源，进行长期的数据积累。如果将这种长期大范围的网络监控计划公之于众，必然引起广泛争议，不利于情报项目持续稳定运行。

历史经验也促使美国政府尽快使网络情报话题淡出公众视野。“9·11”恐怖袭击发生后，小布什政府迅速授权国家安全局启动一个名为“星风”(Stellar Wind)的监控项目，包括电话和互联网记录、电话和互联网元数据，重点是外国人与美国人之间以及过境美国的外国人之间的通信。该项目一直在极度保密的情况下运行，外国情报监视法庭直到项目运行后一年才获悉其已经运行，国会也只有情报委员会极少数议员知情。② 2005 年 12 月，《纽约时报》揭露该项目监控美国人电话和网络的事实，引起轩然大波。小布什政府一方面以“恐怖分子监视计划”辩解项目重要性，同时承诺促进运营商与情报部门之间合作的相关立法，另一方面引导媒体将关注焦点转向修订《外国情报监视法案》相关条款的专业讨论。不久之后，国家安全局的大规模网络监控重回秘密状态，媒体也不再关注该项目了。随着美国政府设法再次以淡化舆论来使争议边缘化，加上网络情报项目的监控对象和数据获取方式受到了一定限制，美国公众关注的隐私保护问题基本得到解决，国际社会也未能聚集足够力量持续施压美国政府，同时巩固情报联盟及伙伴关系的一些努力也取得了效果，包括承诺不再对盟友领导人进行监控，美国国内和国际压力就这样再次被消解了。

第四，增加网络情报技术和研发投入。美国情报界充分利用网络空间快速发展的机遇，加上美国的技术和资源优势，投入巨额资金，获得了这一新型空间获取数据和情报的超强能力。美国政府认为这些能力是其应对充满挑战的安全环境的主要动力，白宫的文件称，“美国必须保持并继续发展强大的技术先进的信号情报能力，以保护我们的安全以及我们的合作伙伴和盟友的安全。我们的信号情报能力必须足够灵活，以便我们能够专注于短暂的机会或新出现的危机，不仅要解决今天已经出现的问题，而且要解决无法预见的未来可能出现问题。”③

基于这样的认识，情报界的财政预算逐年稳步增长，这在奥巴马政府致力于限制联邦预算增长的背景下，其意义不言而喻。特朗普政府也继续给予情报界预算支持，这从另一个角度显示了国家安全和外交决策中网络情报的重要性。作为一种获取情报的新手段，网络情报的广泛性和时效性，自然能够成为各情报机构争取更多预算的竞争力项目。

大笔资金投向网络情报的获取、存储、加工和运用等环节的新技术研发和运用。国家安全局很早就开展了大数据研究，投资了数百个大数据初创项目，是美国大数据浪潮的强力推手之一，一些大数据项目在规模、可扩展性和安全性等方面甚至超过了谷

① The White House Office of the Press Secretary, “Update on Implementation of Signals Intelligence Reform and Issuance of PPD-28,” https://obamawhitehouse.archives.gov/the-press-office/2015/02/03/statement-assistant-president-homeland-security-and-counterterrorism-lis. (上网时间:2018 年 5 月 22 日)

② “星风”项目长期在高度保密状态运行，据称至 2007 年 1 月，国会 535 名议员中仅有 60 人有权了解该项目。[英] 卢克·哈丁著，何星等译《斯诺登档案:世界头号通缉犯的内幕故事》，第 77 页。

③ The White House, “PPD-28: Signals Intelligence Activities,” https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. (上网时间:2018 年 5 月 22 日)

歌、亚马逊等行业领先企业。2008 年启动、2014 年建成的犹他数据中心，即情报界综合国家网络安全倡议数据中心，建设费用 15 亿美元，硬件和软件费用 20 亿美元，用于设备运行每年所消耗的电量花费

美国情报系统预算(亿美元)					
财务年度	国家情报项目预算		军事情报项目预算		批准总额
	申请数	批准数	申请数	批准数	
2019	599	–	212	–	–
2018	577	–	207	–	–
2017	549	546	185	184	730
2016	539	530	179	177	707
2015	504	503	166	165	668

数据来源：美国国家情报总监办公室网站，http://www.dni.gov.(上网时间：2018 年 5 月 22 日)

达 4000 万美元。① 该数据中心的建成大大提升了整个情报界存储和处理海量数据的能力。人工智能技术和应用的快速发展，包括与网络应用的快速结合，也对网络情报提出新的挑战。2017 年月，哈佛大学贝尔弗科学和国际事务中心发布了一份题为《人工智能与国家安全》的报告，认为人工智能可用于创建和传播虚假信息，对情报搜集形成挑战，建议情报界(以国家安全局为核心)在对抗人工智能的攻防能力方面加大投资，成立人工智能安全机构，扩大与私营企业的交流与合作，研究能够识别对手利用人工智能伪造的音视频数据的技术。②

上述几个方面的政策措施，一定程度上弥补了引发美国公众和国际社会不满的政策和法律漏洞，“棱镜计划”等网络情报项目得以“合法”地继续运行。更重要的是，获得重新定位的网络情报有了更有效的保障和更持续的动力，这也决定了未来相当长一段时期内，美国政府继续强化网络情报活动的大方向将不会改变。

三

网络空间与经济社会运行密切融合，国家安全和外交决策对网络情报青睐有加，情报界在各方压力下全面反思，大国网络空间竞争态势进一步发展，这些构成了“斯诺登事件”后美国政府调整网络情报政策的基本动因。

第一，国家安全与外交决策对网络情报的依赖。冷战结束以后，美国情报界一度陷入无所适从的境地，失去了苏联这一最重要的战略对手，对外情报地位亦随之下降。“9·11”后，美国社会弥漫着对恐怖主义的恐惧，促使小布什政府将在全球范围内预防和打击恐怖主义作为国家安全的优先目标，反恐也成为情报工作的核心内容。小布什政府推出一系列情报改革政策，迅速通过《美国爱国者法案》，发展无所不在的监控能力，其宣称的目标就是加强对外情报工作，集聚一切反击恐怖主义的能力和资源。

随着网络空间的快速发展，恐怖组织开始运用互联网进行联络交流、组织培训、协调行动、舆论宣传等活动，也促使美国情报界将互联网作为情报搜集和实时监控的重点，范围和规模不断扩大，“棱镜计划”即是国家安全局实施的一系列网络监控和情报搜集项目之一。利用“棱镜计划”，国家安全局能够获取互联网用户的电子邮件、聊天记录、视频、照片等在线活动记录和存储数据，监控对象包括数家互联网公司的境外用户，与境外用户进行在线互动和信息往来的美国公民。

通过这种大范围的实时监控，既可以实现对已知恐怖嫌犯的实时跟踪，掌握被监视人与美国境内进行通话、试图进入美国或组织针对美国的恐怖图

① Bamford James, “The NSA Is Building the Country's Biggest Spy Center,” *Wired*, March 15, 2012, https://www.wired.com/2012/03/ff-nsadatacenter. (上网时间：2018 年 5 月 22 日)

② Greg Allen, Taniel Chan, “Artificial Intelligence and National Security,” Belfer Center for Science and International Affairs, Harvard Kennedy School, July, 2017, https://www.belfercenter.org/publication/artificial-intelligence-and-national-security. (上网时间：2018 年 5 月 22 日)

谋等实时信息，还可以建立被监视对象、潜在嫌疑人之间的关系链，通过大数据分析，寻找恐怖组织网络的更广泛线索。而对后一种情报来源的探索，日益成为情报界扩展影响力的重点。为了更广泛地扩充情报数据库，增加关系链条的有效性，情报机构还设法侵入各种网络系统和数据库，从目标网站下载数据。一旦具备了这种全方位监控能力，情报机构就可以随时超越初始目标，监控对象既可以是恐怖组织头目，也可以是外国政要、国际组织领导人、社会活动家，只要赋予国家利益和国家安全的目标，更新一下监控对象列表即可。“无所不在的秘密监控体系肆意扩张，已经成为美国政府最持久的遗产”。①

与网络情报价值日益重要的态势相对应的，是美国政府国家安全和外交决策日益依赖网络情报。据称呈送白宫的总统《每日简报》中，有一半以上是来自国家安全局，而其中又有很大一部分来自网络监控项目获取的最新动态。因此，美国网络情报政策的调整方向，决不是要放弃或削弱这种情报能力，而是为了进行更广泛的监控，实现更有深度的数据挖掘，获取更有价值的情报。

第二，情报界的反思与“基于需要”情报文化的回归。美国情报界的基本架构自二战后初期建立起来，经历冷战期间的不断调适，逐渐形成了一种“基于需要”而搜集的情报组织文化，其核心是情报和信息应围绕预设目标而搜集，且只有在其提供者认为必要时才能被更多部门共享。“9·11”袭击促使情报界思考这一情报文化在应对恐怖主义时的不足，“9·11”调查委员会认为，情报获取不全面、情报分析不及时、情报共享不充分是造成情报机构早已发现恐怖袭击的蛛丝马迹、但未能成功阻止灾难发生的重要原因。

小布什政府时期，决策者和情报界致力于重建“基于责任”和“充分共享”的组织文化，从而提升应对恐怖主义的情报能力。2008 年《情报界信息共享战略》指出，“‘基于需要而知道’”的组织文化应该向‘基于责任而提供’的组织文化——信息提供者主动将信息分享给其他情报机构与人员——转变，从而最大限度地利用各情报机构搜集到的信息。② 奥巴马政府基本沿续了这样一种思路。在这种情报文化的激励下，加之有了充足的预算支持，其结果就是尽其所能获取一切可能得到的数据，网络情报设定的任务和目标越来越大，远远超出了防范和反击恐怖主义袭击的初始范围。已故参议员约翰·麦凯恩（John McCain）在被问及为何德国总理默克尔也会被监听、监听外国领导人与反恐究竟有何种联系时，就直言不讳地说：“我认为，他们这么干只是因为他们有能力这么干。”③

“斯诺登事件”又促使情报界反思这种“基于责任”的情报文化隐藏的巨大风险，充分的情报共享固然可以避免遗漏重要信息，有助于部门间更紧密协作，阻止恐怖袭击再次发生，然而这既增加了情报机构的工作负担，也增加了内部机密外泄的几率。当情报机构累积了大量数据搜集、加工、存储和共享的业务，仅依靠自身的人力和技术难以完成，因而很多业务被外包给如博思艾伦咨询公司（Booz Allen Hamilton）之类承揽情报流程各环节业务的专业公司，导致斯诺登这种低级别的外部技术人员可以接触到大量高密级的文件资料。

“斯诺登事件”对美国情报文化形成了巨大冲击，其力度丝毫不亚于“9·11 事件”造成的颠覆性影响，只不过“9·11”后各情报机构都热衷于情报整合与共享，都尽其所能搜集各种数据信息，“斯诺登事件”又促使各情报机构趋向谨慎，防止内部机密泄露成为优先考虑，尽量减少情报失误造成的负面影响。至此，美国情报界的心态和行动又开始了回摆，国会和白宫采取立法和行政措施加强情报监管，很大程度上也反映了这种“基于需要”的情报文化在决策层面的回归。

第三，大国网络战略竞争和多方博弈的态势。随着社会信息化进程深入发展，网络空间已经成为大国竞争的新平台，主要大国纷纷提出网络空间的

① ［美］格伦·格林沃尔德著，米拉等译《无处可藏：斯诺登、美国国安局与全球监控》，中信出版社，2014 年，第 13 页。

② U.S. Office of the Director of National Intelligence, “U.S. Intelligence Community Information Sharing Strategy,” https://fas.org/irp/dni/iss.pdf.（上网时间：2018 年 5 月 22 日）

③ Karen McVeigh, “John McCain Says NSA chief Keith Alexander ‘Should Resign or Be Fired’,” *The Guardian*, November 10, 2013, https://www.theguardian.com/world/2013/nov/10/john-mccain-nsa-keith-alexander-snowden.（上网时间：2018 年 5 月 22 日）

国家战略，一方面促进网络空间与经济社会融合发展，维护网络空间安全，另一方面谋求国际话语权和影响力，力争掌握网络空间国际行为规则制定的主动权。

“斯诺登事件”掀起轩然大波，削弱了美国政府对网络空间治理的主导权和可信度，也促使主要国家和国际组织重新考虑网络空间国际秩序的基本架构，甚至提出探讨在美国之外构建一个更为安全和可信互联网的可能性。由于在联合国等全球性国际组织中推进国际网络空间行为规范的努力受到美国阻拦，一些主要互联网大国转向地区层面，近年来在现有区域性国际组织中推动网络空间治理合作的尝试已经取得了一些进展。

“斯诺登事件”对美国企业的国际信誉也造成了严重伤害，特别是那些参与情报搜集项目的互联网运营企业。2015 年 10 月，欧洲法院认为，欧盟公民的个人数据不能传输至非欧盟国家，除非该国能为这些数据提供有效保护，鉴于美国未能达到上述要求，从而判决 2000 年欧美之间签署的《数据安全港》协议失效，[①]美国企业不再能够以政府背书而直接使用和传输欧盟公民数据。而 2018 年 5 月生效的《通用数据保护条例》再也没有赋予美国企业任何额外权力。因此，美国政府调整网络情报政策的原因，也包括重塑国际公信力和影响力，通过展示自身行为的合法性，建立共同遵守的行为规范，将盟友伙伴重新拉回“志同道合”（like-minded）的合作阵营。而这需要相当漫长的时间，更为重要的是，需要促进网络空间共建共享的诚意。

结　语

如同海湾战争中“沙漠盾牌”、“沙漠风暴”行动展示了美军压倒性的信息化作战能力和制空优势，“斯诺登事件”也显示出美国情报界对互联网超乎想象的渗透和控制。斯诺登曾说，“国家安全局已经建立了一种基础设施，几乎可以让其截收一切数据。拥有这种能力，人类绝大部分通信都可以被自动获取”。[②] 作为首屈一指的网络强国，美国充分利用其技术和资源，获取了网络情报领域远超其他国家的领先地位。然而情报优势并不必然意味着决策能力的提升，奥巴马政府从“棱镜计划”中获取了大量情报，此间美国政府的国家安全和外交决策却未见多么富有成效。“斯诺登事件”造成了盟友和伙伴之间难以修复的猜忌与裂隙，激发了主要竞争对手的防范和反制，对美国对外关系的伤害却是长期和深刻的。

情报活动历史悠久，自从有了国家，就开始了相互刺探军事、政治、经济和社会情报的活动。同时，情报活动长期处于国际关系的灰色地带，迄今没有一项国际法规约束或规范国际间的情报活动，因而情报活动的空间取决于当事国之间的外交关系。网络情报作为一种新型情报获取方式，其合法性对内而言应基于正当国家安全利益需要，对外而言则应符合国际关系的一般准则。在缺乏持续有效外部压力的情况下，期待美国情报界及决策层主动放弃其网络空间的资源和技术优势、自我约束尽其所能获取网络情报的冲动，无异于缘木求鱼。当美国的政策调整与国际社会主流期待逆向而行时，国际社会将寻求一种与共同利益相一致的力量，这种力量应当是一种合力，不仅来自国际社会对于和平、安全、繁荣的网络空间的期待，也包括美国国内积极、理性的诉求，这正是各利益攸关方应该付诸共同努力的方向。○

（特约编辑：李艳）

① Court of Justice of the European Union, “The Court of Justice declares that the Commission's U.S. Safe Harbour Decision Is Invalid,” https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.（上网时间：2018 年 5 月 22 日）

② ［英］卢克·哈丁著，何星等译《斯诺登档案：世界头号通缉犯的内幕故事》，第 91 页。

and energy security to China's participation in the Caspian Sea cooperation.

Keywords: The Convention on the Legal Status of the Caspian Sea; demarcation of the Caspian Sea; development of Caspian energy; security of Caspian Sea

Cyber Security Dilemma and Governance Mechanism

Lu Chuanying

Abstract: The Snowden incident has accelerated national competition in the realm of cybersecurity, triggered a cyber arm race, and promoted the formation of an international security dilemma in cyberspace. The underlying reasons for this are the characteristics of cyber technology and the dual-use nature of cyber products and services, as well as the universality and importance of cyberspace for the state and society. Therefore, studying the cyber security dilemma should not only concentrate on international political competition, but also analyze from the perspectives of technology, commerce and politics and establish targeted governance mechanisms in different perspectives.

Keywords: Snowden incident; cyber security; technology nationalism

The Adjustments of US Cyber Intelligence Policy after Snowden Leaks

Wang Xiaofeng

Abstract: In order to relieve domestic and international pressures due to Snowden leaks, the US government has strengthened supervision on cyber intelligence activities, regulated the collection, storage, application and sharing of cyber intelligence through legislative and administrative measures, and suspended some infringements of personal privacy and business interests. Meanwhile, the US government has increased investment to cope with the opportunities and challenges brought by the rapid development of cyberspace and the application of new technologies such as big data and artificial intelligence. The article argues that the US government will pay more attention to cyber intelligence, and will be more cautious in making cyber intelligence projects covert operations. In the near future, global internet surveillance by the US intelligence community still poses threats on cyberspace and international relations.

Keywords: US; PRISM; Snowden leaks; cyber intelligence

(Edited By Zhang Yimeng)