第29卷 第6期 太 平 洋 学 报 Vol. 29, No. 6
2021年6月 PACIFIC JOURNAL June 2021

DOI:10.14015/j.cnki.1004-8049.2021.06.005
包霞琴、黄贝:“日本网络安全政策的现状与发展趋势”,《太平洋学报》,2021年第6期,第51-61页
BAO Xiaqin, HUANG Bei, “Japan's Cybersecurity Policy and Its Development Trends,” *Pacific Journal*, Vol. 29, No. 6, 2021, pp. 51-61.

日本网络安全政策的现状与发展趋势

包霞琴[1] 黄 贝[2]

(1.复旦大学,上海 200433;2.清华大学,北京 100084)

摘要:近年来,日本政府在国家安全战略转型的背景下积极推进网络安全政策。在国内能力建设方面,日本通过组织机构构建、网络防卫能力建设和官民网络安全合作等措施打造网络安全强国。在国际合作方面,日本将网络安全作为提升国际安全事务影响力的抓手,以国际网络对话、网络安全合作、国际网络安全规则塑造和网络安全能力建设支援为着力点,试图抢占主动权,塑造网络安全领导者角色。在信息技术革命深刻影响国际政治的当下,日本网络安全政策的发展方向值得关注和研究。

关键词:网络安全;网络治理;国际规则;发展趋势

中图分类号:D83 **文献标识码**:A **文章编号**:1004-8049(2021)06-0051-11

在安倍晋三第二次执政之后,日本的国家安全战略出现重大转型,日本正以愈发积极的防卫姿态应对多样化和复杂化的国际安全环境。2018年12月,日本政府出台了新版《防卫计划大纲》,提出构建融合宇宙、网络和电磁波等领域的“多域联合防卫力量”,并特别强调要提高网络空间等新领域的军事能力。2021年,日本防卫预算达到历史最高的5.34万亿日元,并重点加强在网络空间、外层空间和电磁波等新领域的能力建设,引起国际社会的普遍关注。①

本文梳理了日本网络安全政策的发展历程,探究日本在对内网络安全能力建设和对外网络安全外交两方面的新举措,并对日本网络安全政策的未来走向进行剖析。本文认为,日本网络安全政策已完成了从内向型和民用化向外向型和战略化的转变。日本政府不仅将网络安全政策视为应对网络攻击、保护日本国民与社会信息安全的必要手段,更将其作为国家对外战略的重要一环。日本正以构建网络安全强国为目标,采取多种举措增强网络安全治理能力,积极参与国际网络空间治理事务,试图在这

收稿日期:2020-12-22;**修订日期**:2021-05-16。
基金项目:本文系教育部哲社重大项目“战后日本政治、外交实质和未来走向研究”(14JZD033)的阶段性成果。
作者简介:包霞琴(1964—),女,上海人,复旦大学国际关系与公共事务学院教授、博士生导师,法学博士,主要研究方向:战后日本政治、外交、中日关系;黄贝(1993—),女,湖北恩施人,清华大学社会科学学院国际关系学系2020级博士研究生,主要研究方向:国际安全、日本外交。

*感谢《太平洋学报》编辑部和匿名评审专家提出的建设性修改意见,文中错漏由笔者负责。

① 『我が国の防衛と予算-令和3年度概算要求の概要』、2021年3月30日、https://www.mod.go.jp/j/yosan/yosan_gaiyo/2021/yosan_20210330.pdf。

个国际政治新领域占据一席之地。

一、政策背景:网络安全环境与网络安全观

20世纪90年代的互联网信息技术革命浪潮催生了“网络安全”这一概念,国际社会对网络安全的关注随之开始。在信息通信技术持续发展和网络安全环境日益复杂的背景下,日本政府对网络安全的重视程度也不断提升,网络安全政策的制定及实施成为日本各界频繁讨论的议题。

1.1 全球网络安全环境的发展态势

互联网技术的诞生和普及使网络攻击带来的威胁与日俱增,网络安全威胁成为各国政府亟需应对和处理的治理难题。这些威胁往往由个人、组织或国家等多类主体实施,涉及经济、社会和军事等不同领域。具体来看,全球网络安全形势的变化主要经历了两个阶段:在互联网形成发展之初,网络安全威胁主要源自窃取商业机密、实施犯罪活动、扰乱网络正常运行的黑客攻击,“网络恐怖主义”这一概念也于2000年开始出现。① 由于这一时期网络攻击发起方多为掌握网络技术的个人和民间组织,网络安全仍主要被视为非传统安全领域的议题。然而,爱沙尼亚在2007年遭到大规模网络攻击之后,全球网络安全形势转而进入第二个阶段,国家行为体成为网络攻击的发起方或目标方,网络攻击开始真实威胁到国家的生存与稳定。此后,2008年俄罗斯—格鲁吉亚战争中的网络攻击、2010年伊朗核设施遭“震网”(Stuxnet)病毒攻击等重大网络安全事件,进一步引发各国政府对网络安全的重视,国家之间围绕网络攻击展开的互动、博弈日益增多,东亚等地区面临的网络安全威胁不断扩散、深化。② 同时,近年来不断激化的中美战略竞争也从现实政治领域蔓延至网络空间,网络安全出现“过度安全化”的现象。③ 在此背景下,各国政府对网络安全的关注重心逐渐由经济目的驱动的网络攻击转向由政治、军事目的驱动的网络威胁,网络安全的军事化趋势成为影响当前全球网络空间局势的重要因素。

1.2 日本网络安全环境的变化

作为全球最发达的经济体之一,日本较早成为网络攻击的主要目标之一。2000年,日本科学技术厅、总务厅和参议院等24个政府网站主页内容相继遭到黑客篡改,一时引发舆论热议。④ 此后10年间,针对日本政府、企业网站的网络攻击虽时有发生,但该问题仍被视为纯粹的技术性问题,并未成为国家安全和危机管理重要事项。直至2011年,日本遭受的网络攻击激增,针对日本企业、研究机构和政府部门的鱼叉式网络钓鱼攻击(spear phishing)数量较2007年增加了6倍;三分之一的鱼叉式网络钓鱼和37%的高级持续性攻击(Advanced Persistent Threat,简称APT)更指向核电站、高科技产业等重大基础设施。⑤其中,日本重要军工企业三菱重工遭受攻击,负责潜水艇、核电、导弹研究及制作的11处场所可能发生信息泄露,而作为该企业采购方的日本防卫省在事件发生后则是通过媒体得知该消息,直接暴露了日本政府各部门在网络安全方面信息沟通不畅的问题。⑥

面对不断增加的网络攻击,日本国内对这一虚拟空间安全威胁的感知逐渐增强。首先,日本政界对网络攻击和网络威胁的重视程度提升,首相官邸及国会关于网络安全的探讨不断

① 郎平:“网络空间安全:一项新的全球议程”,《国际安全研究》,2013年第1期,第132页。

② 刘杨钺、杨一心:“集体安全化与东亚地区网络安全合作”,《太平洋学报》,2015年第2期,第48-50页。

③ 杨楠:“网络空间军事化及其国际政治影响”,《外交评论(外交学院学报)》,2020年第3期,第69-93页。

④ 「ハッカー暗躍、無防備日本 保安対策あぎ笑う」、『朝日新聞』、2000年2月12日。

⑤ Paul Kallender and Christopher W. Hughes, “Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace,” *Journal of Strategic Studies*, Vol. 40, No. 1-2, 2017, p. 121.

⑥ ポール・カレンダー「防衛省とサイバーセキュリティ—日本のサイバーセキュリティに関する進展と落とし穴—」、『SFC研究所日本研究プラットフォーム・ラボ ワーキングペーパーシリーズ』No.8、2013年12月、6頁。

增多。2016 年至 2020 年期间,日本首相历次国会施政演说中均提及网络犯罪与网络安全问题。同时,日本国会就网络安全议题进行的讨论明显增多。日本参众两院提及“网络安全”或“网络攻击”的会议次数从 2010 年的 7 次增加至 2020 年的 118 次,网络安全在日本政治议题中的重要性不断提升。① 其次,日本防卫省开始对网络威胁给予高度重视。日本防卫白皮书自 2010 年起将网络空间作为国际社会重大安全课题进行追踪,并于 2011 年后将“应对网络攻击”作为日本防卫政策的重要组成部分。2020 年,防卫白皮书进而将网络威胁与来自宇宙、电磁波领域的威胁一并视为需要“跨领域作战”应对的重要问题。② 最后,日本民众对网络安全所表现的担忧与日俱增。根据美国皮尤研究中心民调结果显示,2016 年日本受访者最为担忧的国家安全威胁是网络攻击,选择该选项的受访者占比达 71%,2018 年继续上升至 81%。同时,认为“本国已准备好应对一次重大网络攻击”的日本受访者仅占 41%,在 26 个调查国中排至第 18 位,日本也成为此次调查中对本国网络防卫能力最缺乏信心的亚洲国家。③

1.3　日本网络安全认知的演变

随着网络安全形势的持续变动,日本政府的网络安全认知也不断演化。具体来看,这种变化分别涉及对网络空间内安全主体、威胁来源和实现手段的认知。

第一,对安全主体的认知,从社会层面转向国家安全层面。在 20 世纪 90 年代互联网技术实现大规模商用化之后,由于遭受网络攻击的大多为民间机构,日本政府对网络安全的理解侧重于确保个人、企业及社会组织等民间主体的“信息安全”。④ 2006 年,日本政府发布首个信息安全政策年度计划,指出“利用 IT 技术威胁国民生活、社会经济安全的事态已经出现”,表示将推进“官民统一、跨领域的信息安全对策”。⑤ 2013 年,日本政府正式将“信息安全”计划改名为“网络安全”计划,并将“国家安全保障与危机管理”“国际竞争力的维护与加强”与“国民的安全与安心”一起列为日本网络安全政策的主要目标。⑥ 自此,以民间为主导的“信息安全”转向政府主导的“网络安全”。同年,日本政府出台《网络安全战略》,网络安全正式被纳入日本国家安全战略。

第二,对安全威胁来源的认知,从强调网络威胁的非政治性、个人性转向强调网络安全的政治性、国家性。近年来,随着大国间网络空间竞争态势加剧,网络安全的“国家中心化”趋势进一步加强。日本各界都深刻认识到,“网络空间作为自由共同空间的黄金时代已经过去”,网络正在成为“复杂的地缘政治竞技场”。⑦

第三,对实现安全路径的认知,从内向型转向外向型。一方面,日本政府明确了防卫省和自卫队在网络安全事务中的地位,应对网络攻击的主要力量不再限于警视厅等治安机构。外务省在 2012 年表示,“如果国际法体系可适用于网络空间,并且已知网络攻击来自外国,那么可以对网络攻击行使自卫权”。⑧ 2019 年,时任日本防卫相岩屋毅进一步表示,日本在应对网络攻击时不排除使用物理反击手段。⑨ 另一方面,由于网络

---

① 参见国会会議録検索システム, https://kokkai.ndl.go.jp/,访问时间:2021 年 6 月 4 日。

② 『令和 2 年版防衛白書』、https://www.mod.go.jp/j/publication/wp/wp2020/html/nt200000.html,访问时间:2021 年 6 月 4 日。

③ “International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security,” Pew Research Center, January 9, 2019, https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/.

④ 「情報防衛へ官民連携　警察に専門捜査班　サイバー攻撃政府が対応策」、『朝日新聞』、2000 年 11 月 27 日。

⑤ 『セキュア・ジャパン2006』、情報セキュリティ政策会議、2006 年 6 月 15 日、https://www.nisc.go.jp/active/kihon/pdf/sjf_2006.pdf。

⑥ 『サイバーセキュリティ2013』、情報セキュリティ政策会議、2013 年 6 月 27 日、https://www.nisc.go.jp/active/kihon/pdf/cs2013.pdf。

⑦ [日]川口貴久「サイバー空間における『国家中心主義』の台頭」、『国際問題』No.683(2019 年 7・8 月)、37 頁。

⑧ [日]川口貴久「昨今のサイバー安全保障政策の課題:サイバー攻撃と自衛権」、日本国際問題研究所(外務省外交・安全保障調査研究事業)平成 26 年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート、2014 年 8 月、1 頁。

⑨ 「武器反撃『排除せず』サイバー被害深刻なら 防衛相」、『朝日新聞』、2019 年 4 月 27 日。

安全和网络治理已成为全球社会面临的共同议题,日本政府加强了与盟友及伙伴国的网络安全合作,并积极推动国际网络安全规范的形成与落实。

二、网络安全的治理机制与能力建设

为了有效应对网络安全问题,日本政府采取了一系列跨部门、跨领域的能力建设措施,试图构建“强韧的网络空间”,将日本打造成世界领先的“网络安全强国”。

2.1 构建网络安全治理顶层框架

为了有效统筹并管理涉及经济、交通、科技和国家安全等多个领域的网络安全问题,日本政府在2005年设立了信息安全政策会议(ISPC)和内阁官房信息安全中心(NISC),前者负责制定日本网络安全基础战略,后者作为执行机构负责统筹落实该战略,但是政府各部门之间“各自为政”的问题依然没有解决。2009年,日本政府对这一机制进行调整,明确在内阁官房信息安全中心的领导下,警察厅、总务省、经产省和防卫省等4个部门(后加入外务省)共同参与。[①] 2012年6月,内阁官房信息安全中心设置信息安全紧急支援团队(CYMAT),负责在出现紧急事态时协调政府各部门的信息交换与合作。

2012年12月安倍晋三上台后,网络安全在国家安全事务中的重要性进一步提升。2014年,日本国会通过《网络安全基本法》。根据该法律,日本政府于2015年将原信息安全政策会议升格为以内阁官房长官为首的“网络安全战略本部”,原内阁官房信息安全中心升格为“内阁网络安全中心”,直属内阁领导。其中,“网络安全战略本部”除负责网络安全战略的制定外,还有权制定网络安全通用标准、监督各省厅和独立行政法人与网络安全相关的预算编制。内阁网络安全中心作为内阁常设机关,成为日本政府应对网络攻击的“司令塔”,其下设7个部门,分别负责基本战略、国际战略、政府机关综合对策、信息统合、东京奥运会、重要基础设施和个案应对分析。同时,内阁网络安全中心与日本国家安全保障会议之间建立了密切的合作关系,进一步从组织架构上确保网络安全政策作为日本安全战略的重要组成部分,能够更好地服务于日本整体安全利益(参见图1)。

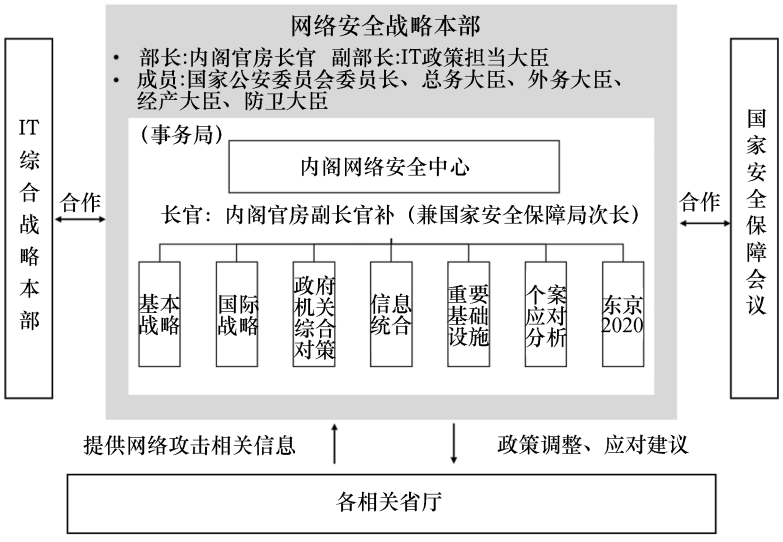

图1 日本网络安全领域政府领导机制

资料来源:笔者根据“内阁网络安全中心”网站信息整理,https://www.nisc.go.jp/index.html,访问时间:2021年6月4日。

① ボール・カレンダー「防衛省とサイバーセキュリティ―日本のサイバーセキュリティに関する進展と落とし穴―」、『SFC研究所日本研究プラットフォーム・ラボ ワーキングペーパーシリーズ』No.8、2013年12月、7頁。

2.2　打造网络安全防卫力量

2013 年之后,日本政府加快了对国家安全战略的调整与升级,《国家安全保障战略》将强化网络安全作为日本国家安全保障战略的重要手段。2018 年版防卫大纲进一步将宇宙、网络和电磁波作为“强化跨领域作战必要能力的优先事项”,并提出增强自卫队“在发生紧急事件时阻止攻击方使用网络空间的能力”。① 在此背景下,日本网络安全防卫力量获得迅速发展,并表现出三大态势。第一,网络安全防卫力量规模不断壮大(参见图 2)。2014 年 3 月,自卫队正式成立 90 人编制的“网络防卫队”,进行 24 小时监控,并向内阁网络安全中心派遣人员以强化与各部门的协调合作。② 2020 年,“网络防卫队”已扩充至 220 人,并计划于 2021 年内继续增加至约 540 人。③ 同时,自卫队海陆空三军下设的网络防卫力量继续扩充。2019 年 3 月,陆上自卫队西部方面队设立了由 50 人组成的地方网络部队,负责在“西南诸岛有事”时保护野外通信系统,防范网络攻击。④ 防卫省还将参照美国设立独立于海陆空三军的职能整合部队,以统筹宇宙、网络和电磁波等“新领域”的跨领域作战。⑤第二,网络安全防卫预算不断增加。2019 年,日本防卫省拨出 223 亿日元作为网络安全相关预算,为 2015 年网络安全防卫预算的 2.45 倍。2021 年,该预算继续增加至 301 亿日元。⑥第三,防卫省及自卫队下设教育机构,加强对网络安全技术人才的培养。日本防卫大学设立了全球网络安全中心,开设“网络战概论”等课程,并定期邀请网络安全专家举行研习班和讲座,为学员介绍网络安全最新信息及各国动态。⑦

2.3　推进网络领域“官民合作”

鉴于企业、研究机构等民间主体在信息技术研发上具有优势和灵活性,日本政府强调进行“官民合作”,最大程度利用民间力量。2015 年版日本《网络安全战略》基本原则是“多主体合作”,强调“所有网络安全利益相关方,如重要基础设施运营者、企业和个人,都必须共享其网络安全愿景,履行各自角色和职责并做出努力”。⑧ 2018 年,网络安全战略进一步从人才培养、研究开发和提高全民意识三个方面阐述了官民合作的内容。在此背景下,网络安全领域的“产学官”结合日趋紧密,民间主体也直接参与到日本网络安全能力的建设之中。

一方面,日本自卫队积极引入民间网络技术人才,扩充网络安全的人才队伍建设。2018 年,自卫队提出向社会公开招募精通信息技术的“白色黑客”作为“特定任期队员”,任期 5 年,年收入超 2 000 万日元。自卫队网络防卫队也计划将恶意软件监控和分析任务委托给民间团队。⑨ 另一方面,企业、研究机构等民间主体与日本政府在网络安全技术领域开展合作。防卫省等部门与这些民间主体积极开展网络安全技术研发及模拟演练,尤其加大了在人工智能、量子通信等尖端技术领域的合作力度。2015 年,防卫省设立“安全保障技术研究推进制度”,

---

① 『平成 31 年度以降に係る防衛計画の大綱について』、2018 年 12 月 18 日、https://www.cas.go.jp/jp/siryou/pdf/h31boueikeikaku.pdf。

② 『平成 26 年版防衛白書』、http://www.clearing.mod.go.jp/hakusho_data/2014/html/nc016000.html,访问时间:2021 年 6 月 4 日。

③ 『我が国の防衛と予算-令和 3 年度概算要求の概要』、2021 年 3 月 30 日、https://www.mod.go.jp/j/yosan/yosan_gaiyo/2021/yosan_20210330.pdf。

④ [日]山下龍一「自衛隊　地方に初のサイバー部隊　中国念頭」、朝日新聞デジタル、2019 年 6 月 11 日、https://www.asahi.com/articles/ASM67645CM67UTFK01N.html。

⑤ 「宇宙・サイバー、自衛隊初の統合部隊創設へ　防衛省検討」、産経ニュース、2019 年 1 月 28 日、https://www.sankei.com/politics/news/190128/plt1901280002-n1.html。

⑥ 『我が国の防衛と予算-平成 31 年度予算の概要-』、2019 年 3 月 27 日、https://www.mod.go.jp/j/yosan/yosan_gaiyo/2019/yosan.pdf;『我が国の防衛と予算-令和 3 年度概算要求の概要』、2021 年 3 月 30 日、https://www.mod.go.jp/j/yosan/yosan_gaiyo/2021/yosan_20210330.pdf。

⑦ 「グローバルセキュリティセンター」、防衛大学校、https://www.mod.go.jp/nda/about/center_for_global_security.html;「防衛学」、防衛大学校、https://www.mod.go.jp/nda/education/defense.html;「防大タイムズNo.184」、防衛大学校、2016 年 8 月 1 日、https://www.mod.go.jp/nda/times/no184.html。

⑧ 『サイバーセキュリティ戦略(2015)』、2015 年 9 月 4 日、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf。

⑨ 「自衛隊のサイバー防衛、『ホワイトハッカー』採用へ、民間の高度技術生かす」、『日本経済新聞』、2018 年 10 月 22 日。

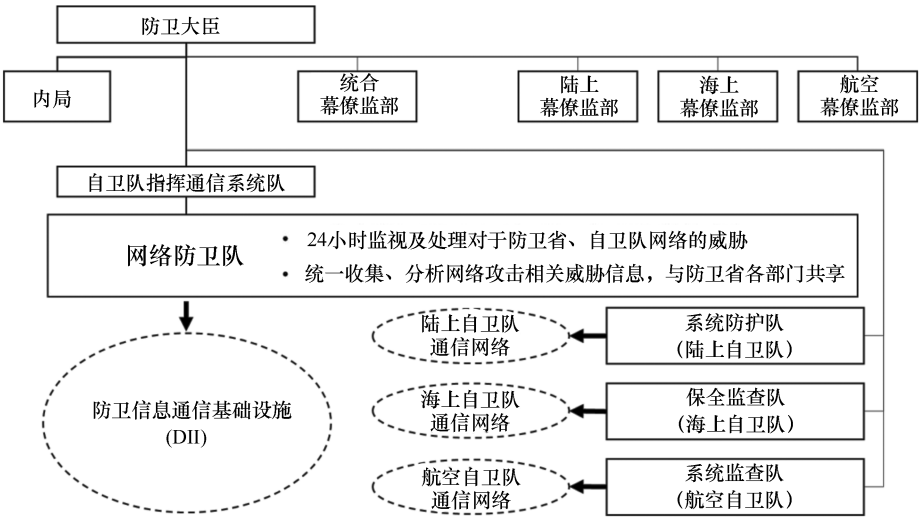

图 2 日本防卫省网络安全相关组织结构

资料来源:「防衛省のサイバーセキュリティへの取組」,https://www.nisc.go.jp/conference/seisaku/ituse/dai2/pdf/siryou0200.pdf,访问时间:2021 年 6 月 4 日。

公开招标并资助企业、研究机构进行创新性基础研究。在这一制度支持下,三菱重工等企业及研究机构关于人工智能(AI)的研究项目已开始实施。① 2019 年,防卫省发布《研究计划愿景:迈向多领域联合防卫力量》,表示将在网络安全技术领域进一步积极运用先进的民用技术。②

三、网络安全领域的国际合作

在增强本国网络安全能力的同时,日本政府积极利用国际对话机制,与伙伴国家开展外交、防务等多轨道网络安全合作,参与构建国际网络安全规则,从而提升日本在国际网络安全事务中的发言权。

3.1 网络安全国际对话

从技术上看,网络空间是一个无边界的跨国空间,因而日本政府在发展“信息安全”战略之初便强调国际交流。随着网络安全议题与国家安全战略的联系日益紧密,日本政府大力推动网络安全外交对话,积极参与国际网络空间会议,在国际网络安全交流平台上不断发声,增强日本的影响力。

日本外务省于 2012 年设立“网络政策担当大使”(由综合外交政策局审议官兼任),并于 2016 年成立网络安全政策室,日本在网络外交舞台上愈发活跃。首先,日本主动利用国际和地区多边组织参与网络空间治理。联合国是日本多边外交的主要平台,联合国在 2004 年发起政府专家组(UNGGE)以协调各国对于网络安全规则的意见,日本从 2012 年第三次会议起作为成员国参与历次会议。同时,日本在七国集团(G7)、东盟地区论坛等多边外交会议中就网络安全议题发表观点并推进合作。其次,日本大力发展与多个国家及组织的双边、三边网络对话及协商机制。截至 2021 年 5 月,日本与 11 个国家或组织建立了双边网络对话机制。另外,日本还分别与

① 「平成 30 年度『安全保障技術研究推進制度』新規採択研究課題」、防衛省・自衛隊、2018 年 12 月 26 日、https://www.mod.go.jp/atla/funding/kadai/h30kadai.pdf;「『安全保障技術研究推進制度』新規採択研究課題」、防衛省・自衛隊、https://www.mod.go.jp/atla/funding/kadai/r02kadai_b.pdf。

② 「研究開発ビジョン 多次元統合防衛力の実現とその先へ 解説資料 サイバー防衛の取組」、防衛省・自衛隊、2019 年 8 月 30 日、https://www.mod.go.jp/atla/soubiseisaku/vision/rd_vision_kaisetsuR0203_03.pdf。

中韩、美韩举行了三边网络对话会议。[①] 目前,与日本开展网络对话的国家涵盖了美国、澳大利亚和英国等盟国或安全伙伴,中国、韩国和俄罗斯等重要邻国,以及以色列、爱沙尼亚和乌克兰等网络安全技术强国。在这些网络安全沟通会议中,日本派出外务省、防卫省和内阁网络安全中心等相关人员参加,并与意见相近的伙伴国达成更为深入的网络安全合作。最后,日本积极参与由官方和民间力量共同参与的"1.5 轨"网络安全对话。2011 年开始举行的全球网络空间会议(Global Conference on Cyberspace,简称 GCCS)是目前网络空间领域最大规模的国际会议,参与方包括了相关政府机关、民间企业和民间组织等。以外务省为主导的日本代表团参加了历次会议,并将此平台作为向全球推介日本网络安全政策的重要场所。

3.2　网络安全国际合作

日本防卫省除借助双边"2+2"会议和网络空间沟通机制之外,也与美国、北约等安全伙伴直接展开安全合作。

在日本网络安全战略发展的过程中,日美网络安全合作始终贯穿其中,并体现出起点高、跨机构、机制化和功能明确等鲜明特点。[②] 2011 年,日美"2+2"会议首次将网络空间纳入共同战略目标。2013 年 5 月,日美举行网络对话,表示将通过该机制在信息交换、国际规则制定、信任构建和网络开放等领域加强合作。同年 10 月,日美两国决定设立网络防卫政策工作小组(CDPWG),提升日美网络防卫合作水平。[③] 目前,两国已基本形成以情报共享、联合训练和人员培训为主的网络安全合作常态,如 2013 年 11 月,日美在北海道举行的联合军演中首次进行了反网络攻击训练;2019 年 12 月,陆上自卫队与美军举行的"山樱"联合演习也加入了网络攻击应对训练。[④] 在人员培训方面,美国相关大学和美军教育机构为日本自卫官提供了一系列网络安全培训和交流机会。2020 年,自卫队还派遣自卫官赴美国国防大学参加网络战指挥官培训课程,日本成为"五眼联盟"之外首个参与该课程的国家。[⑤] 2019 年 4 月,日美"2+2"会议表示,针对日本的网络攻击可以被视为"武装袭击",并适用于《日美安保条约》第 5 条,这标志着日美两国在网络攻击领域开展更深层次的合作,训练整备也从"日常化"走向"战时化"。

另外,日本与北约联合演习、人员交流方面的合作也不断加速。2015 年,日本自卫队首次以观察员身份参与了北约网络防卫合作中心主办的名为"锁盾"的网络防卫演习;2019 年 3 月,防卫省向北约派遣人员,学习应对网络攻击的处理能力;12 月,自卫队以正式成员国身份参加了北约主办的网络防卫演习。[⑥] 2020 年 2 月,时任防卫大臣河野太郎与北约秘书长斯托尔滕贝格(Jens Stoltenberg)同意将进一步推进双方在网络安全方面的合作。[⑦]

3.3　塑造国际网络安全规则

为了在国际网络空间议题上占据主导权,日本积极参与国际网络安全规则的制定,并签署了相关网络空间国际条约。2001 年 11 月,欧洲委员会制定了全球首个应对网络犯罪和滥用网络的国际公约——《网络犯罪公约》(又称《布达佩斯公约》)。日本以观察员身份参与了公约制定,并于 2004 年 4 月正式通过了该公约。在 2012 年

① 「日本のサイバー分野での外交　二国間協議・対話等」、外務省、https://www.mofa.go.jp/mofaj/fp/nsp/page24_000687.html。

② 张景全、程鹏翔:"美日同盟新空域:网络及太空合作",《东北亚论坛》,2015 年第 1 期,第 87 页。

③ 「(仮訳)日米安全保障協議委員会共同発表—より力強い同盟とより大きな責任の共有に向けて」、外務省、2013 年 10 月 3 日、https://www.mofa.go.jp/mofaj/files/000016027.pdf。

④ "美日北海道联合军演首次进行反网络攻击训练",中国新闻网,2013 年 12 月 4 日,www.chinanews.com/mil/2013/12-04/5578819.shtml;「対サイバー攻撃、日米で、自衛隊と米軍、図上演習」、『日本経済新聞』、2019 年 12 月 10 日。

⑤ 「サイバー指揮官養成へ　米国防大に自衛官派遣」、『読売新聞』、2019 年 10 月 7 日。

⑥ 「NATOのサイバー演習、日本が本格参加へ 知見多く蓄積…関係進化目指す」、産経ニュース、2018 年 9 月 2 日、https://www.sankei.com/politics/news/180902/plt1809020001-n1.html;「サイバー防衛で職員派遣　防衛省、NATOに」、『日本経済新聞』、2019 年 3 月 8 日;『令和 2 年版防衛白書』、388 頁、https://www.mod.go.jp/j/publication/wp/wp2020/pdf/R02030303.pdf。

⑦ 「河野大臣によるNATO 事務総長との会談(概要)」、防衛省、2020 年 2 月 15 日、https://www.mod.go.jp/j/approach/exchange/area/2020/pdf/20200215_nato-j.pdf。

举办的全球网络空间会议上,确保《网络犯罪公约》有效性和扩大缔约国成为会议的主要议题之一,作为亚洲唯一一个缔约国的日本表示愿意发挥积极作用。①

与此同时,日本积极倡导所谓的自由、开放、法治的国际网络空间价值观。2012年,日本政府首次提出将"构建开放、可互用、安全、可靠的网络空间"作为其参与构建国际框架的基本方针。② 2015年版《网络安全战略》提出了"信息自由、法治、开放性、自律性、多主体合作"五项基本原则。③ 其中,"法治"被列为日本网络安全三大支柱之首,成为日本宣传与倡导的重点。2017年5月,七国集团在日本伊势志摩峰会联合声明中承诺,共同构建适用于现行国际法的稳定的国际网络空间。④ 此后,日本政府在全球网络空间对话平台上多次强调"国际法适用于网络空间"的基本立场。

3.4 支援网络安全能力建设

近年来,日本以"支援能力建设"为名与其他国家深化安全领域合作,不断增强本国在地区安全事务中的影响力,这一趋势也扩展至网络安全领域。目前,日本将"支援能力建设"作为网络安全外交的核心之一,试图向发展中国家提供网络安全公共产品,树立区域网络安全领导者形象。2015年版《网络安全战略》指出,日本将利用已有经验和积累,积极协助各国提高网络安全治理能力。⑤ 2016年10月,内阁网络安全中心、警察厅、总务省、法务省、外务省、经产省与防卫省共同发布"关于在网络安全领域支援发展中国家能力建设的基本方针",并明确了三大支援内容:事件反应能力、应对网络犯罪、制定网络空间的国际性规则及构建信任措施。⑥

在这一系列文件的指导下,日本政府采取了诸多措施,而东盟国家则成为重点支援对象。首先,在事件反应能力方面,日本政府部门及国际协力机构(JICA)等组织向东盟国家提供提升网络安全技术水平的人力及财力援助,如日本总务省、经产省和内阁网络安全中心向印尼、越南定期派遣网络安全专家,进行技术合作;日本国际协力机构提供资金,援助缅甸通信网络改善项目;与东盟国家举行相关短期培训、研讨会和联合演习。⑦ 2017年12月,日本防卫省对越南军队进行了信息处理技术、信息安全等方面的培训。⑧ 2018年9月,日本—东盟网络安全能力建设中心在曼谷成立,该中心由日本提供500万美元资金及培训人员,通过培养东盟国家学员,帮助东盟国家提升网络安全能力。⑨ 其次,在应对网络犯罪方面,日本积极发起合作倡议。2014年5月,日本与东盟举行了由外交、警察和司法部门参与的"日本—东盟网络犯罪对话",开展定期沟通和具体合作。2016年,日本政府支持组织了为期两年的"东盟网络能力发展项目",为380名东盟国家学员提供关于应对网络犯罪的相关课程。⑩ 最后,在塑造网络空间国际共识方面,日本不仅通过网络安全方面的外交对话机制推动与东盟国家达成共识,还发起了一系列针对学生群体的交

---

① 「サイバー空間に関するブダペスト会議」、外務省、2012年10月10日、https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/cyber_1210.html。

② 『情報セキュリティ2012』、情報セキュリティ政策会議、2012年7月4日、10頁、https://www.nisc.go.jp/active/kihon/pdf/is2012.pdf。

③ 『サイバーセキュリティ戦略(2015)』、情報セキュリティ政策会議、2015年9月4日、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf。

④ 「サイバーに関するG7の原則と行動」、外務省、2016年5月、https://www.mofa.go.jp/mofaj/files/000160315.pdf。

⑤ 『サイバーセキュリティ戦略(2015)』、情報セキュリティ政策会議、2015年9月4日、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf。

⑥ 「サイバーセキュリティ分野における開発途上国に対する能力構築支援(基本方針)(概要)」、内閣官房内閣サイバーセキュリティセンター、2016年10月、https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou09.pdf。

⑦ [日]村上啓「サイバー外交政策に関する研究-キャパシティビルディングを中心に-」、情報セキュリティ大学院大学博士論文、2018年3月、88頁。

⑧ 「防衛省・自衛隊:サイバーセキュリティ(ベトナム:平成29年12月11日~20日)」、https://www.mod.go.jp/j/approach/exchange/cap_build/vietnam/h291211.html。

⑨ "Japan Leads Regional Effort to Fight Cyber Crime," Indo-Pacific Defense Forum, May 10, 2019, https://ipdefenseforum.com/japan-leads-regional-effort-to-fight-cyber-crime/.

⑩ "ASEAN Cyber Capacity Development Project (ACCDP)," INTERPOL, https://www.interpol.int/en/Crimes/Cybercrime/Cyber-crime-training-for-police/ASEAN-Cyber-Capacity-Development-Project-ACCDP.

流活动,塑造东盟下一代的网络空间观。在内阁网络安全中心主导下,日本与东盟自 2012 年起举办了一系列网络安全宣传活动,包括海报制作、教学动画翻译、资料共享,以及创办用于双方学生交流网络安全文化的“国际网络安全咖啡厅”等。①

四、网络安全政策的发展趋势

总体来看,日本网络安全政策的迅速发展不仅服务于本国的安全目标,更与日本政府积极的全球外交战略紧密结合。日本政府正从机构增设、法律授权、技术创新和对外战略等方面不断调整网络安全政策的发展方向,试图强化日本在网络空间的国际竞争力,在数字时代抢占优势地位。

4.1　建设实务型网络安全中央机构

如前所述,日本内阁网络安全中心等机构的重要性不断增强,但其职能范围仍限于宏观战略制定、政府内信息传递和监督等“顾问型”工作,并无实际处理网络威胁和网络攻击的领导统筹能力,不足以成为“全政府”应对的核心枢纽。与此相对,许多欧美国家都建立起应对网络攻击的一体化机构,如英国国家网络安全中心、美国网络安全与基础设施安全局、德国联邦信息安全局等。因此,日本各界建议设立进一步强化政府主导作用的实务型网络安全中央机构。

日本学者白石隆指出,当前日本防卫系统与新干线、银行、电力、通信等系统都建立在互联网基础之上,日本政府应创立一个专门管理网络安全的机构,以应对国家安全的这种脆弱性。② 2018 年,日本笹川和平财团安全保障研究部建议日本政府设立“网络安全厅”,在组织架构上作为与警察厅、金融厅等部门平级的内阁府外局。该部门应统合原本由各省厅、独立行政法人等多个机构进行的网络空间信息收集、分析,统一指挥针对政府机构和重要基础设施的网络攻击,下设多个由网络安全专家组成的机动处理分队,并全盘领导网络安全产业发展、研究开发和人才培养等工作。③ 2019 年 5 月,日本自民党网络安全对策本部部长高市早苗向时任首相安倍晋三提交了创设网络安全厅的政策建议书。④ 在网络安全问题不断复杂化以及学界、政界和舆论的持续推动下,日本网络安全领域组织机构的优化已成必然趋势,中央政府层面的网络安全机构将从“顾问型”向“实务型”部门转变。同时,这一态势也将与日本防卫部门成立横跨宇宙、网络和电磁波等新领域统一作战部队的构想相配合,进一步提升日本政府应对网络安全事件的能力与效率,为日本在网络空间构建“积极防卫体制”奠定坚实的组织基础。

4.2　实现法律“松绑”

目前,日本网络安全能力的发展仍然受到一系列法律制度掣肘。首先,对于易受网络攻击的重要民间主体,日本政府难以通过情报监控及时、充分地获取信息。日本宪法第 21 条对通信秘密提供保护,《电气通信事业法》第 4 条也规定通信运营商不得侵犯通信秘密。因而,英美等国在强化网络安全时采取的情报监听、监控手段在日本面临合法性问题,这在一定程度上限制了日本政府在网络攻击预警和应急处置方面的能力。其次,自卫权在网络空间的适用情况相对模糊。国际社会对于何种程度的网络攻击可被界定为“武力攻击”尚无定论。除针对国家防御系统的破坏型网络攻击以及与军事行动结合进行的网络攻击之外,其他针对民间主体的数据窃取、功能妨碍,以及以数据抹除为目的的破坏型网络攻击均难以被界定为武力攻击。因而,当重要基础设施遭受网络攻击时,日本防卫力量往往难以发挥作用。最后,现有法律框架下的自卫队交战规

① ［日］村上啓「サイバー外交政策に関する研究-キャパシティビルディングを中心に-」、情報セキュリティ大学院大学博士論文、2018 年 3 月、89 頁。

② 「超スマート社会 サイバー機関創設必要 白石隆(寄稿)」、『読売新聞』、2017 年 3 月 5 日。

③ 「日本にサイバーセキュリティ庁の創設を!」、笹川平和財団安全保障事業グループサイバー空間の防衛力強化プロジェクト政策提言、2018 年 10 月、29 頁。

④ 「サイバー対策へ新庁を、自民提言、25 年創設めざす」、『日本経済新聞』、2019 年 5 月 14 日。

则对网络攻击存在适用性问题。有日本学者认为,网络攻击具有“进攻方占优”的特征,即进攻方寻找系统漏洞、发动攻击的成本远小于防御方进行全盘防御的成本,所以“先发制人”是网络战中更具吸引力的策略。① 此外,在已知攻击者的情况下对其进行出于防御目的的攻击,即“攻防一体”也已成为极具影响力的网络战理念。然而受“专守防卫”原则约束,自卫队无法采取这些策略,这也对强调“攻防一体”“防御前置”的美军与其开展网络安全合作带来障碍。

对于上述一系列法律约束,日本产业界和学界关于为日本网络安全能力发展“松绑”的呼声不断。笹川和平财团的政策报告就提议对相关法律进行修改,如规定通信运营商有义务将储存的通信记录提交给网络安全部门,将向网络安全部门提交网络事件报告作为重要基础设施运营商的法定义务等。② 在自卫队网络空间行动的法律授权方面,国际政治学者川口贵久表示,日本政府和日美同盟应该对网络空间武力攻击认定设置“阈值”,即明确设定哪些类型和主体发起的网络攻击相当于武力攻击,他认为应将“先发制人行动”(preemptive action)作为自卫权的行使方式之一。③ 日本网络安全专家名和利男认为,日本必须改变与网络相关的法律制度、组织机制和文化观念,否则日美网络合作只会停留在“纸上谈兵”阶段。④ 随着网络安全防卫实务的持续推进,日本政府修改和完善相关法律将成为必然趋势。

4.3 推动前沿信息技术军事化

当前,日本政府将增强技术实力、争夺技术优势视为关乎未来国家安全的重要任务。同时,日益增多的网络攻击和信息技术对传统战争可能带来的颠覆性改变也推动日本政府将信息技术研究向“军事化”推进。日本防卫省已经将人工智能、量子技术(如量子计算机、传感和通信)作为研究开发的主要方向。其中,人工智能技术在日本防卫领域的研发与运用尤其呈现加速态势。

人工智能是世界大国“科技竞赛”的主要赛道,人工智能在军事领域的运用也成为各军事强国重点投入的科研方向。日本自卫队尝试向通信、监测系统引入人工智能技术,提升防御能力。2019年,日本政府发布《人工智能战略2019》,防卫省宣布将人工智能引入网络防卫队信息通信系统,以更高效地应对恶意软件的攻击,并通过对过往案例的“深度学习”提高病毒检测率、应对未知病毒,进而对未来可能发生的攻击进行预测。⑤ 同时,自卫队于2020年启动海上自卫队巡逻机系统搭载人工智能技术的开发研究,该技术将取代人工识别图像情报信息的模式,帮助机上警戒监测和情报收集系统提高对障碍物、敌方目标的自动识别能力及识别效率。⑥ 此外,日本还将目光转向“无人化武器装备”。虽然日本政府表示暂未计划开发致命性全自主武器(fully autonomous lethal weapons systems),但认为不应对高度自动化武器系统进行限制,并强调国际社会应就致命性自主武器建立相应标准和规则。⑦ 可以预见,人工智能技术从“防御性使用”向“攻击性使用”的转变,也将是日本发展网络空间军事技术过程中值得关注的问题。

4.4 日美联手牵制中国

特朗普政府上台之后,压制中国经济的发展、阻止中国高科技领域研发和生产的快速发展已成为

① [日]川口貴久「サイバー空間における安全保障の現状と課題—サイバー空間の抑止力と日米同盟」、平成25年度外務省外交・安全保障調査研究事業(調査研究事業)「グローバル・コモンズ(サイバー空間、宇宙、北極海)における日米同盟の新しい課題」、2014年3月、17頁。

② 「日本にサイバーセキュリティ庁の創設を!」、笹川平和財団安全保障事業グループサイバー空間の防衛力強化プロジェクト政策提言、2018年10月、36-37頁。

③ [日]川口貴久「昨今のサイバー安全保障政策の課題:サイバー攻撃と自衛権」、日本国際問題研究所(外務省外交・安全保障調査研究事業)平成26年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート、2014年8月、4頁。

④ 「日米同盟、新領域で深化、サイバー攻撃に抑止力、中ロ念頭、法的課題残る」、『日本経済新聞』、2019年4月20日。

⑤ 「防衛省、AI導入拡大、サイバー対策や装備補修」、『日本経済新聞』、2019年6月17日。

⑥ 「海自哨戒機にAI、防衛省、研究へ、省人化識別能力も向上」、『日本経済新聞』、2019年11月9日。

⑦ “Possible Outcome of 2019 GGE and Future Actions of International Community on LAWS,” Ministry of Foreign Affairs of Japan, https://www.mofa.go.jp/mofaj/files/100113384.pdf.

美国政府的当务之急。[①] 在此背景下,中美之间的网络安全摩擦增多,两国不断激化的战略竞争正向网络空间蔓延,国际网络安全形势愈发复杂。在此背景下,作为美国重要盟友的日本正转向与美国合作一致对华。自 2019 年起,日本防卫白皮书已将中国作为首要“网络空间威胁”加以关注,日本媒体也竭力渲染中国的“网络安全威胁”,为日美同盟的网络空间“军事化”政策提供合理性,并谋求加入美国主导的情报联盟(即“五眼联盟”)。[②]

与此同时,日本将在国际网络空间的规则制定、科技竞争等更为广泛的相关议题上参与对华竞争。在网络空间治理模式方面,以美国、欧盟为首的西方国家与中国、俄罗斯所代表的发展中国家在治理理念、规则等方面存在较大差异,日本一贯支持美国、宣扬所谓“自由、民主、透明”的国际网络规则。在科技竞争方面,5G、人工智能等数字技术研发已成为中美竞争热点。目前,日本已通过加强外资限制等措施排除华为等中国企业进入日本市场,以配合美国在高科技领域的对华“脱钩”战略。2021 年 4 月,日美政府首脑会晤后发表的联合声明明确表示,将进一步深化在人工智能、量子信息技术等领域的科研合作,共同“守护科技优势”并“运用科技领导力”。[③] 可以预见,在拜登政府加强对华战略竞争的背景下,日本在网络安全议题上会承担更多“同盟义务”,日美联合牵制中国网络能力发展的倾向将更为显著。

编辑　贡　杨

Japan's Cybersecurity Policy and Its Development Trends

BAO Xiaqin[1] HUANG Bei[2]

(1.*Fudan University*, *Shanghai* 200433, *China*; 2.*Tsinghua University*, *Beijing* 100084, *China*)

Abstract: Along with transformation of the national security strategy, the Japanese government has currently been actively adopting its cybersecurity policy to become a strong cyber power by building centralized institutions, strengthening cyber security capabilities and promoting cooperation between governmental and private sectors. Also, regarding cyberspace as a prominent realm to promote its influence in international security affairs, the Japanese government aims to play a leading role in cyberspace through international cyber dialogues, cybersecurity international cooperation, international rules negotiation and cybersecurity capacity building assistance. As information technology innovation is profoundly shaping international politics, it is necessary to take a deep look into the development of Japan's cybersecurity strategy.

Key words: cybersecurity; cyber governance; international rules; development trends

① 周琪:“高科技领域的竞争正改变大国战略竞争的主要模式”,《太平洋学报》,2021 年第 1 期,第 2 页。

② 「米英など5カ国『ファイブアイズ』、日独仏と連携　サイバー攻撃、中国の機密情報共有」、『毎日新聞』、2019 年 2 月 4 日;「日本がファイブアイズに自国のプラットフォーム・インテリジェンスを差し出す可能性」、『ニューズウィーク日本版』、2021 年 5 月 26 日、https://www.newsweekjapan.jp/ichida/2021/05/post-24_1.php。

③ The White House, “U.S.-Japan Joint Leaders' Statement: ‘U.S.-Japan Global Partnership for a New Era’” April 16, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/u-s-japan-joint-leaders-statement-u-s-japan-global-partnership-for-a-new-era/.