日本网络战攻势化转型问题研究*

张晓磊

内容提要：“反击能力”概念的提出体现了日本在军事战略上的攻势化转型方向，为日本推动网络战转型做了战略和理念层面的铺垫。拥有并行使网络反击能力是日本推动网络战攻势化转型的集中表现。随着日本网络安全战略的持续强化及与美欧网络安全合作的持续推进，日本推动网络战实现攻势化转型的战略理念愈加清晰，战略动因逐步明朗，政策储备不断完善。日本网络战泛化和网络安全治理军事化的做法将对日本安全战略和中日关系产生重大影响，中日间应加强在网络安全层面的危机管控。

关 键 词：网络战　攻势化转型　网络反击能力　日本安全战略　中日关系

作者简介：张晓磊，中国社会科学院日本研究所副研究员。

中图分类号：D831.3；E313　　**文献标识码：**A

文章编号：1002－7874（2023）03－0032－20

网络战作为一个兼具国家安全学和军事战略学性质的概念，带有多元化和复杂化的特征，国内外学界对此也有比较充分的研究和分析。从日本学界来看，近些年日本学者从网络战的战略理念、技术发展趋势、网络空间的大国博弈、网络战与国际法等方面对网络战进行了多维研究。① 但是，这些研究成果大部分停留在对战略和政策理念的阐释、对国外研究成果的介绍以及对国外政策的分析等方面。而且，鉴于日本刚刚引入“反击能力”这一新概念，推动整体军事战略实现攻势化转型，并逐步推进相关网络战政策落地，目前

* 感谢《日本学刊》编辑部和匿名审读专家提出的意见和建议，文中若有疏漏和不足概由笔者负责。

① 关于网络战研究的一些国外学者研究成果可参见：持永大・村野正泰・土屋大洋『サイバー空間を支配する者』、日本経済新聞出版社、2018年；川崎剛『大戦略論―国際秩序をめぐる戦いと日本―』、勁草書房、2019年；中谷和弘・河野桂子・黒崎将広『サイバー攻撃の国際法―タリン・マニュアル2.0の解説―』、信山社、2018年；土屋大洋『サイバーテロ』、文春新書、2012年；迈克尔・施密特、丽斯・维芙尔：《网络行动国际法 塔林手册2.0版》，黄志雄等译，北京：社会科学文献出版社，2017年。

对日本网络战攻势化转型问题进行分析的学理性研究成果并不多见。[①] 本文认为日本引入“反击能力”概念，将其作为推动网络战攻势化转型的理念基础，在此基础上，拥有并行使网络反击能力是日本推动网络战攻势化转型的集中表现。

一、围绕日本网络战攻势化转型的相关概念界定

2022 年 12 月底，日本政府出台了新版“安全保障三文件”——《国家安全保障战略》《国家防卫战略》《防卫力量整备计划》，并宣布将拥有并增强“反击能力”[②]。其中明确提出，所谓“反击能力”是指“在对我国发生武力攻击、其攻击手段是通过弹道导弹等实施的情况下，根据武力行使三要件，作为防御这一攻击而不得不采取的必要且最小限度的自卫措施，通过灵活运用防区外防卫能力等，使我方具有可在对方领域进行有效反击的能力”。可见，日本将“反击能力”定性为一种自卫权的实施方式，是一种自卫措施。

回顾日本出台三个新安全保障文件的过程可知，日本政府是用“反击能力”概念代替了此前提出的“对敌基地攻击能力”[③] 概念。从法理属性来看，此前在政策讨论过程中“对敌基地攻击能力”引起争议的焦点在于，其与少数西方国家及西方学者所主张的“预防性自卫权”具有相似性，即国家有权对即将发生或迫在眉睫的武力攻击行使“预防性自卫权”，但这种主张在国际条约和习惯国际法上都没有获得支持，因为这意味着“向大国颁发了一张几乎不受限制的使用武力的许可证”[④]。但事实上，“反击能力”这一更为模糊的用语却引发了更大的争议。一是由于删去了“对敌基地”的字眼，使反击

① 目前国内研究日本反击能力问题相关的成果可参见栗硕：《日本“对敌基地攻击能力”构建进程分析》，《日本学刊》2022 年第 2 期，第 118—134 页；邱静：《日本“对敌基地攻击能力”讨论新动向》，《日本学刊》2022 年第 2 期，第 135—160 页。这两篇研究成果是以日方政府反击能力的官方概念前身——对敌基地攻击能力为中心进行讨论的，且均在日本发布“新安全保障三文件”之前，主要聚焦于对日本构筑导弹攻击能力这一现实问题的分析上，并未涉及网络战视野下的对敌基地攻击能力或反击能力问题研究。

② 参见：防衛省『国家安全保障戦略』、『国家防衛戦略』、『防衛力整備計画』、https：//www.mod. go. jp/j/policy/agenda/guideline/index. html[2023 - 03 - 17]。

③ 对于日本国内讨论“对敌基地攻击能力”的过程，在此不做详述，可参见栗硕：《日本“对敌基地攻击能力”构建进程分析》，《日本学刊》2022 年第 2 期，第 118—134 页；邱静：《日本“对敌基地攻击能力”讨论新动向》，《日本学刊》2022 年第 2 期，第 135—160 页。

④ Jan Klabers，*International Law*，Cambridge University Press，2013，p. 193.

目标的范围进一步扩大；二是日方认定敌国武力攻击本国的手段可被无限引申扩大为若干武力攻击形态，包括网络攻击、电磁攻击以及太空攻击等新军事领域的攻击形态，这也意味着日本使用“反击能力”的形式将变得更加多元，行使“反击能力”的条件因用语模糊而存在巨大的自由裁量空间。① 总之，“反击能力”的提出反映了日本在军事战略上的攻势化转型方向，为日本在网络战中推动实现攻势化转型做了战略和理念层面的前期铺垫，也为日本推动网络战转型提供了具体抓手。

（一）网络战中武力攻击的内涵与外延

本文无意将研究核心放在“网络战”本身的概念界定上，出于对网络空间中日本行使反击能力问题的聚焦，笔者从发动反击的前提——出现“敌国的武力攻击”这一视角出发，首先确立网络战中“武力攻击”的内涵和外延，以便厘清本研究问题的指涉范围。

确定网络战中武力攻击概念的前提是在更广义范围内确定学理意义上的“网络空间”及“网络攻击”概念。根据目前为止网络战研究学界最有影响力的成果——《网络行动国际法 塔林手册 2.0 版》② 的最新定义，网络空间主要包括三个层面，即物理层面（如计算机、通信设备等硬件）、逻辑层面（如网络应用、数据等软件）和社会层面（即软硬件的使用者），网络安全问题就与这三个层面息息相关。在网络战视野下，网络攻击的对象牵涉个人、社会和国家，具体而言，对国家层面的攻击包括干涉选举、舆论操纵、窃密、威胁决策者、篡改决策相关信息、攻击军事雷达和通信设施等，对社会层面的攻击包括对重要基础设施的攻击，如输油管、水坝、电力和医疗系统等，对个人层面的攻击则包括网络金融和信息犯罪等。

至于哪些网络攻击属于武力攻击的范畴，归结到一点就是，以键盘、鼠标、电脑病毒和其他恶意软件为“武器”的网络攻击，是否可能成为（或已经成为）一种新的战争形态或作战手段？所谓“战争形态论”，是指单纯的网络攻击能否构成一种战争意义上的使用武力行为，而“作战手段论”是指在

① “反击能力”的概念从被提出之日起，就引起了日本国内的巨大争议。比如从日本律师联合会的一份意见声明可见一斑，参见：日本弁護士連合会「『敵基地攻撃能力』ないし『反撃能力』の保有に反対する意見書」、2022 年 12 月 16 日、https：//www. nichibenren. or. jp/library/pdf/document/opinion/2022/221216. pdf［2023 - 03 - 17］。

② 为行文方便，《网络行动国际法 塔林手册 1.0 版》《网络行动国际法 塔林手册 2.0 版》简称为“塔林手册”。

传统的军事冲突中将网络攻击作为一种单纯的作战手段。目前，在理论和实践中，对作战手段论是普遍承认的，但对战争形态论的认识分歧较大。而日本对上述两种论点，不仅选择了全盘接纳，还对其进行了扩大解释。

日本政府参议院和众议院的答辩会议记录① 明确记载了时任首相安倍晋三和时任防卫大臣政务官宫泽博行在回答网络攻击与武力攻击关系相关问题时的答辩内容，其可以作为研判日本行使网络反击能力的基本指涉范围。从二人的答辩记录看，日本官方认为网络空间中的战争可以分为两种：一种是在传统现实战争视野下作为战争军事行动和武力攻击一环的网络攻击，另一种则指单纯的网络破坏、网络颠覆、网络谍报等单一的网络攻击，而后一种网络攻击只要可被合理预见为会造成物理损伤、人员伤亡的重大攻击，也可被界定为武力攻击的一部分。② 该日本官方观点其实与西方网络战研究学界的主流观点保持一致。

基于此，本文所谈网络战中武力攻击的内涵主要包括战争军事行动中的网络攻击以及造成损伤后果的网络破坏、网络颠覆、网络谍报等单一的网络攻击两部分内容。这在很大程度上决定了日本网络战政策工具箱的整体框架以及未来的政策发展趋势。

（二）网络战视野下的“反击能力”

梳理“新安全保障三文件”出台的整个过程可以看到，“反击能力”概念的前身实际上是“对敌基地攻击能力”。从“对敌基地攻击能力”到“反击能力”的概念转换，其关键节点是 2022 年 4 月 26 日日本自民党向岸田文雄政府提交的政策建议书。在日本政府的决策机制中，由执政党向内阁提交政策建议书是政策从酝酿到正式出台的一个重要核心环节，建议书的出台代表着执政党和内阁之间达成了政策方向及核心内容上的共识。虽然执政党提交的是建议书，但背后体现的却是政府的政策目标和政策意图。自民党在建议书中对“反击能力”做了这样的阐释：“随着导弹技术的快速发展，对其拦截变得困难，这样的拦截恐怕无法实现我国的自卫。基于如此严峻形势，在

① 参见：「安倍首相『サイバー攻撃のみでも武力攻撃』衆院本会議で」、『毎日新聞』2019 年 5 月 16 日、https：//mainichi. jp/articles/20190516/k00/00m/010/234000c［2023 - 03 - 17］；安倍晋三「第 189 回国会（常会）答弁書第二二一号（内閣参質一八九第二二一号）」、2015 年 8 月 7 日、https：//www. sangiin. go. jp/japanese/joho1/kousei/syuisyo/189/touh/t189221. htm［2023 - 03 - 17］。

② 川口貴久「変わりゆくサイバー空間での戦争」、道下徳成編著『技術が変える戦争と平和』、芙蓉書房、2018 年、38 頁。

维持宪法和国际法范围内日美基本角色分工和坚持‘专守防卫’的前提下，我国应该拥有针对包含弹道导弹攻击等在内的武力攻击的反击能力，以便对上述攻击进行有效威慑和应对。反击能力的对象不仅包括攻击国的导弹基地，也包括对方的指挥中枢等。”①

综合梳理自民党的上述阐释和日本政府发布的“新安全保障三文件”中对“反击能力”的定义可以发现，日本政府试图通过从“对敌基地攻击能力”到“反击能力”的概念转换，实现扩大反击对象和范围的意图。“反击能力”在替代“对敌基地攻击能力”后，其内涵和目标已经发生了实质性变化。在“对敌基地攻击能力”语境下，日本行使攻击的目标仅限于敌国的导弹发射基地，但在“反击能力”语境下是不存在这种限制的。在自民党的建议书中，试图通过部分列举的方式体现日本行使反击能力所针对目标的广泛性；而在“新安全保障三文件”中，日本政府通过使用“必要且最小限度”“施加有效反击”等抽象的表述对反击目标做了进一步模糊化处理，只要在发动攻击的敌国区域内且能够实施有效反击，就可能成为日本行使反击能力的目标。可见，日本内阁与自民党之间就对反击能力行使目标的解释达成了一种共识或默契，以便在日后的政策实施过程中为日方行使反击能力创造最大的解释和自由裁量空间。

从学理来看，“反击能力”的概念似乎从字面意义上解决了此前“对敌基地攻击能力”易被等同于“先发制人打击”这一公然违背国际法基本公理的最大争议点，用“反击”的字眼突出了此项能力的自卫性质。但是，通过梳理其演进过程和背后的政策意图就可以发现，“反击能力”的外延远远超出“对敌基地攻击能力”这一概念。虽然日本政府将“反击能力”认定为一种自卫措施②（包括几个核心要素：一是日本遭到了敌国的武力攻击，二是发动反击需要满足日本《武力攻击基本法》所规定的自卫队行使武力的三个基本

① 自由民主党政務調査会・安全保障調査会「新たな国家安全保障戦略等の策定に向けた提言—より深刻化する国際情勢下におけるわが国及び国際社会の平和と安全を確保するための防衛力の抜本的強化の実現に向けて—」、2022 年 4 月 26 日、https：//www. jimin. jp/news/policy/203401. html［2023 -03 -17］。

② 反击能力与自卫权的关系本身是一个值得探讨的学理问题。即便将反击能力作为一种自卫措施，这种措施本身是否超出自卫界限进而达到先发制人打击的程度，在日本国内政策界以及国际法学界也是存在巨大争议的，笔者或将在以后的研究中专文涉及此问题，本文仅限于讨论网络战中的反击能力。2023 年 1 月 30 日，在日本众议院预算委员会会议上，日本首相岸田文雄对反击能力的界定依然含糊其辞，回避行使反击能力是否违反国际法等问题。本文不对此展开深入讨论，而是仅以反击能力所指涉的攻防形态作为研究中心。

要件，三是可以采取必要且最小限度的自卫措施对敌国区域进行反击，四是认为反击能力是一种灵活性的防卫能力），但从文件内容可以看到，对于敌国发动武力攻击的手段以及本国采取防御的手段，仅采取了诸如“弹道导弹攻击等”“活用防区外打击能力等”的不完全列举方式。而从《国家安全保障战略》对反击能力所指涉的外延来看，日本寻求发动的反击绝不仅仅限于弹道导弹反击的狭窄区域，这一概念的外延已经扩展到了从陆海空到天网电的所有现代战争中所指涉的武力攻击区域的反击，尤其是网络战和太空战中所涉及的反击能力值得政界和学界加以关注。在此之前，针对日本发动的网络攻击和太空攻击已经被纳入了《日美安全条约》第五条的适用范围，这也意味着为应对网络攻击和太空攻击，日本已经在行使个体自卫权乃至集体自卫权方面考虑现实应对措施。基于以上学理逻辑，笔者认为推动在网络战中拥有并行使反击能力（简称“网络反击能力”）将是日本网络战政策的未来发展趋势。

二、日本网络战攻势化转型的战略理念、内在动因与政策储备

近些年，日本在国内持续强化网络安全战略①，对外持续推进与美欧的网络安全合作，日本推动网络战以实现攻势化转型的军事战略理念愈加清晰，战略动因逐步明朗，政策储备不断完善。

（一）“能动性网络防御”理念与网络战攻势化转型

如前所述，日本官方对网络战的界定决定了其灰色事态下作战的本质，除了战争军事行动中由对方网军发动的网络攻击以外，单一层面的网络破坏、网络颠覆、网络谍报等已经造成重大损害的网络攻击行为也将被日方视为武力攻击，这反过来推动了日本在网络作战的组织实施主体进行多元化的改革和部署。

从主体角度意义上考虑，网络战是最典型的举国体制，要求政府对整个国家的网络攻防有一个全局性的考虑和布局。如果说网络防御在主体多元或者模糊的情况下还能够勉强维持运转，那么网络反击则急需一个集中统一的实施主体才能够避免网络战出现混乱局面。近些年，随着网络战的技术应用逐步落地，特别是俄乌冲突中网络战与卫星、电子等技术的进一步结合，加

① サイバーセキュリティ戦略本部『サイバーセキュリティ戦略 2013—2021』、内閣サイバーセキュリティセンター（NISC）、https：//www. nisc. go. jp/policy/materials/index. html#material - cyber_security[2023 - 02 - 14]。

速了日本政府在确定网络战集中统一实施主体及决策架构上的推进步伐。

以日本政府制定的前四版《网络安全战略》为基础，日本政府层层推进并最终在新版《国家安全保障战略》中提出了防范网络攻击于未然的“能动性网络防御”理念①，设想在遭受网络攻击之前，进入对方的服务器使其无力发起攻击。② 需要注意的是，为了避免被国际舆论基于国际法指责“能动性网络防御”理念有先发制人打击的嫌疑，该文件将“能动性网络防御”所指涉的网络攻击范围限定于未达到武力攻击程度但可能对国家及重要基础设施产生重大威胁的网络攻击。③ 但是，问题在于如何界定网络攻击是否达到武力攻击的程度。这在国际法实践中是极其困难的，最终的结果一定是当事国会做出最有利于本国利益的解释。从具体表述来看，此处所谓“未达到武力攻击程度但可能对国家及重要基础设施产生重大威胁”的说法与“反击能力”的概念在逻辑上一脉相承，与西方主张的“预防性自卫权”也如出一辙。同理，既然面对连未达到武力攻击程度的网络攻击都要做出先发制人式的预防打击，那么当网络攻击上升到武力攻击的程度时，日本具有并行使网络反击能力，就是一种逻辑上的必然了。总之，无论从何种角度看，结合前述日本政府的官方答辩记录，日本提出的这种所谓“能动性网络防御”为其在网络战中具备和行使反击能力提供了理念和逻辑基础。

日本政府之所以提出“能动性网络防御”理念，与网络战中的攻防特征有着密切关系。日本学者近些年密切关注网络战与国际政治和国家军事理论间的逻辑关系，有学者引入传统军事领域中的“威慑”概念，并将其代入网络战的攻防模式研究中，得出了一些值得注意的结论，能在一定程度上解释日方提出“能动性网络防御”的内在机理和逻辑。日本学者伊东宽④ 认为，网络空间或网络战作为仅次于太空的第五军事领域，有其自身的运行规律和特征，如果将威慑概念代入其中，那么“惩罚性威慑”和“拒止性威慑”在网络战中则有着不同的运行特征。在网络战中，拒止性威慑可以概括为防御

① 防衛省『国家安全保障戦略』、https：//www. mod. go. jp/j/policy/agenda/guideline/index. html［2023 - 03 - 17］。

② 《日本政府为引进“能动性网络防御”新设准备室》，日本共同社网，2023 年 1 月 31 日，https：//china. kyodonews. net/news/2023/01/d5b292fbc4c1. html［2023 - 03 - 17］。

③ 日文原文为“武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する”，参见：防衛省『国家安全保障戦略』、https：//www. mod. go. jp/j/policy/agenda/guideline/index. html［2023 - 03 - 17］。

④ 藤巻裕之編著『グローバルシフトと新たな戦争の領域—精密兵器と競争のフロンティアが国際政治に及ぼす変動と変容—』、東海教育研究所、2022 年、74 頁。

方成功阻止攻击方进入本方服务器；惩罚性威慑则可概括为在本方服务器遭受攻击后对攻击方的服务器进行反击。除了上述两种防御性的威慑概念，安全战略理论中还包括如进攻型现实主义者米尔斯海默[①]等提出的“预防性威慑”概念，对应其在网络战中的内涵，可以将其概括为在预知本方服务器即将受攻击的风险后，预先对即将发动攻击的敌方服务器发动反击。从三种威慑的概念可知，网络反击能力既包括惩罚性威慑的意图，同时也蕴含预防性威慑的目的。而日方提出的“能动性网络防御”理念对应的则是预防性威慑。

日方为何要单独强调预防性威慑？为解释这一问题，需要对比三种威慑机制的实际效果。第一，与传统军事领域相比，网络攻防中攻击方的优势更为凸显，防御一方的劣势更为明显，这决定了拒止性威慑在网络战中的实操空间比较小，类似于导弹攻击和防御。也就是说，在网络战中“防御系统”是极其弱化的，防御和威慑作用微乎其微。第二，惩罚性威慑的有效性也常被质疑，主要是因为攻击方的服务器和身份有可能是伪造的，对错误目标发动惩罚性威慑就无法达到预期效果。而且，这种情况经常发生在未达到武力攻击程度的网络攻击范围内，一旦上升到武力攻击的程度，攻击方就变成了一个交战国或冲突当事国，也就不存在确定主体的环节了。鉴于前两种威慑机制在网络防御中的实际效果不如预期，根据安全战略理论框架中关于进一步强化威慑效果的设计，此时需要通过增加威慑策略以实现威慑需求，预防性威慑就成为一种具有可操作性的路径。基于此，日方提出了“能动性网络防御”的理念。总的来看，网络防御的任务主要依靠惩罚性威慑和预防性威慑，也就是说在网络防御中发动网络反击才具有真正的实操空间。

（二）日本推动网络战攻势化转型的战略动因

从现有国际法体系以及国际安全局势现实来看，日本最有可能在网络战中首先实现对灰色事态作战乃至混合战的实战化操作，在落地行使网络反击能力的同时，也实现对个体或集体自卫权的实际行使，同时规避可能承担的国际法责任。以下三个因素构成了日本积极推动网络战攻势化转型的具体战略动因。

一是基于网络战本身各种概念界定的模糊性和现有发展阶段的约束。截至目前，关于网络战，在国际法上还没有形成公认的成文乃至习惯国际法规则和责任体系，这就使得对传统战争或武装冲突有着强约束力的国际公法体

① 约翰·米尔斯海默：《常规威慑论》，阙天舒译，上海：上海人民出版社，2021 年。

系对网络战并没有相应的约束力。因此，世界各国有更多的自由空间自主认定他国对其发动的攻击属于所谓“网络武力攻击”，并做出相应的网络反击，最后做出对本国利益最有利的解释。

尽管发展包括网络战规则在内的网络规范的国际合作已经持续了 20 多年，但这过程中挫折不断，正如约瑟夫·奈所言，互联网依然是一个看不见的黑客、暗网、攻击遍地的世界[①]，就像在出现国际海洋法规则之前的海盗时代，到目前为止并没有一个能够约束全球各国的通用的网络战国际规则。究其原因，首先，网络空间具有天然的跨国属性，远比日常社会空间复杂多样和变化多端，它早已不是普通物理世界的简单延伸，而是通常所在世界的几何级进化，这就决定了在一个如此复杂空间中产生能被所有国家认可的规则的困难性。其次，随着世界百年未有之变局的到来，全球多极化趋势加强，意识形态对立凸显，各国均有对包括网络战在内的网络空间规范的不同主观认知，这进一步加剧了具有国际法效力的网络战国际规范的产生难度。因此，在国际规范产生之前，各国认为网络空间就是一个实力主义至上、弱肉强食的“社会”，唯有通过安全自助的方式才有可能达到维护本国网络安全的目的。这一思维与曾经崇尚实力主义的日本的战略基因具有较大相似性，也成为日本推动网络战攻势化转型的战略认知基础。

二是日本可以利用在网络战问题研究上依托西方的所谓“话语强权”，在行使网络反击能力的同时成功规避可能需要承担的国际法责任。从 20 世纪 90 年代中期以来，西方尤其是美国国际法学界围绕“网络战”相关国际法问题进行了大量研究，并相继出版了一些具有影响力的学术成果，比如《网络行动国际法 塔林手册 1.0 版》以及《网络行动国际法 塔林手册 2.0 版》[②]。积极参与相关研究的学者大多数是美国等西方国家的军事法、战争法专家，并具有错综复杂的军方或政府背景，因此这些西方研究成果普遍倾向于对涉及自卫权的《联合国宪章》第 2 条第 4 款和第 51 条进行扩大化解释，进而降低行使自卫权的门槛，倡导将诉诸武力权适用于“网络战”，重视通过单边军事行动应对外部网络威胁。而在幕后推动“塔林手册”等研究成果密集发布的

① Nye Jr. Joseph S.，“The End of Cyber – Anarchy? How to Build a New Digital Order”，*Foreign Affairs*，Vol. 101，January/February 2022，pp. 32 – 43.

② 参见：Michael Schmitt ed.，*Talinn Manual on the International Law Aplicable to Cyber Warfare*，Cambridge University Press，2013，pp. 1 – 11；*Michael Schmitt* ed.，*Tallinn Manual* 2.0 *on the International Law Applicable to Cyber Operations*，Cambridge University Press，2017。

正是北约网络防御中心。2022 年日本加入此中心，一个重要战略意图就是要尽快融入西方的网络战研究话语体系，从而尽快分享所谓的“话语权红利”。这也为日本官方为何选择与西方主流学界观点相同的网络战攻击范围的泛化论提供了一个佐证。

三是从网络战规制构建的未来趋势看，总会出现一套习惯甚至成文国际法规则体系对其进行约束。日本加入北约网络防御中心的额外红利便是可以在未来的网络战国际法规则体系的运用和解释上拥有更多主导权。从《网络行动国际法 塔林手册 2.0 版》发布开始，西方学者群体中出现了越来越多将学说转化为实在法的倾向和需求。该手册的主编、在西方最具影响力的网络战研究专家施密特教授甚至宣称，“‘塔林手册’相关内容属于各国最权威的公法学家学说’”，该手册所包含的各项规则“由国际专家组一致采纳并代表习惯国际法”。① 可见，“塔林手册”的研究导向正在发生比较危险的“异化”，其西方作者们开始跳出研究的局限，希图推动或引导国际舆论，使自身的研究内容成为未来网络战规制的国际法律规范（至少可以先成为一种习惯国际法）。这一导向也逐步出现在西方智库学者的政策建议中，如同约瑟夫·奈所建议的，“通过在西方国家间建立规则联盟，并优待遵守规则的盟友和伙伴，对违反规则的对手进行相应的攻击和制裁，美国可以、也必须领导各国建立新的国际互联网规范”。② 这明确无误地把日美军事同盟的适用领域指向包括网络战规制在内的互联网规范治理等问题。日本推动网络战攻势化转型，是对日美同盟不断拓展适用范围的响应，更是其扩展在同盟中角色的一种战略手段。岸田政府不但希望在传统军事作战领域中重获“矛”的角色，更期待在网络战这一第五维战场③ 与盟主美国“并肩作战”。

（三）日本推动网络战攻势化转型的政策储备

整体来看，为推动网络战实现攻势化转型，日本正在指挥体制、国际机制以及国内法律等三个方面进行全面的政策储备。建立指挥体制的目的

① Michael Schmitt，“International Law in Cyberspace：The Koh Speech and Talinn Manual Juxtaposed”，*Harvard International Law Journal Online*，Vol. 54，No. 13，2012，p. 15.

② Nye Jr. Joseph S.，“The End of Cyber－Anarchy? How to Build a New Digital Order”，*Foreign Affairs*，Vol. 101，January/February 2022，pp. 32－43.

③ 在国际军事冲突问题上，除传统的陆、海、空、天四维之外，计算机网络已成为第五维战场，美国军方在 2010 年成立网络战司令部时明确承认这一点。参见吴敏文：《美国“网军”横空出世，网络成为美军第五维战场》，《中国青年报》2017 年 8 月 24 日，https：//www. chinanews. com. cn/mil/2017/08－24/8312422. shtml［2022－08－16］。

在于明确网络战的指挥主体，提高指挥效率，保障网络反击的成功概率；加强国际机制则主要是为了建立所谓“西方的网络战规制联盟”，占得先手，获得规制主导权和主动权；而完善国内法律则是为了与新安全保障法体系实现无缝衔接，获得国内舆论的支持以及保障网络反击时的法律支撑。

1. 一体化指挥体制的酝酿

2023 年 1 月 31 日，日本宣布在内阁官房设置“网络安全保障体制完善准备室”，强调“把网络安全保障应对能力提高到与欧美主要国家同等以上水平作为紧急课题”，这标志着日本开始围绕拥有网络反击能力完善相应网络攻防体制。在此之前，2022 年 11 月 23 日，日本政府宣布计划任命网络防御总负责人并设立承担指挥防御网络攻击的指挥中枢职能的新组织。[①] 其中，总负责人负责与美欧网络安全机构一把手协调，以加强应对能力；新组织将吸纳设在内阁官房的“内阁网络安全中心”（NISC）的职能并扩充权限，负责指挥自卫队网络防卫队和警察厅网络警察局，预计其将设在内阁官房国家安全保障局（NSS）旗下。NISC 的一把手由事务次官级的内阁官房长官助理兼任，未来其级别将被进一步提高以对标美国，2022 年美国新设国家网络总监职位统管网络安全部门，深化各部门协作。这意味着日本开始依此模式酝酿以拥有和行使网络反击能力为中心搭建一体化指挥体制。

上述举措也是对日本新国家安全战略的具体落实。2022 年 12 月，日本政府在“新安全保障三文件”中明确提出要强化网络防御，引入“能动性网络防御”理念，设置统一协调网络安全保障政策的新组织，完善立法并强化运用。根据日本政府的计划，“网络安全体制完善准备室”将就设置统一协调网络安全领域政策的新组织及必要立法等开展研究，并在此基础上改组“内阁网络安全中心”，设置新的司令塔组织，强化情报收集及分析能力，谋求防范对手发动网络攻击于未然的立法及运用体制。（参见图 1）

这些举措将使日本网络战的指挥主体更加明确和集中，同时有助于提高政府内部统筹协调的效率，提高对各种类型网络攻击的反击成功率。归结到一点，日本正在推动网络战的一体化模式，加强政府对网络战的集中统一领导，这是保障网络战攻势化转型效果的政治基础。日本加速推进上述措施，

① 「『能動的サイバー防御』準備室、内閣官房に新設政府」、『日本経済新聞』2023 年 1 月 31 日。

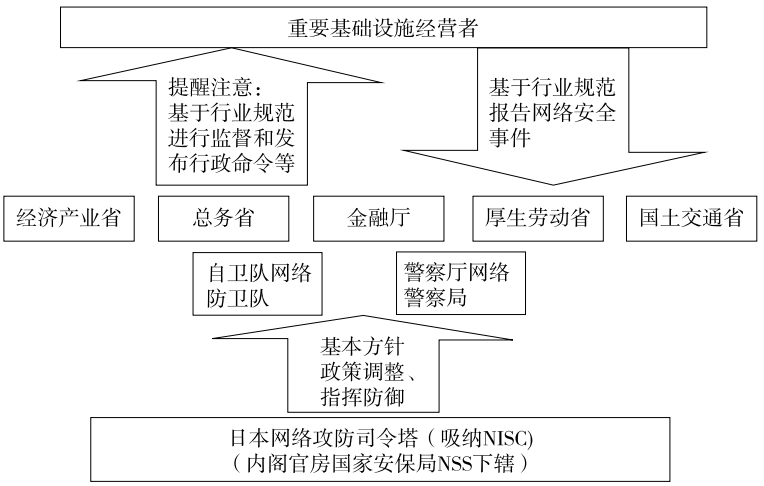

图 1　日本网络安全决策机制构想图

资料来源：笹川平和财团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『日本にサイバーセキュリティ庁の創設を!』」、2018 年 10 月、https：//www. spf. org/security/publications/20181029_cyber. html[2023 - 03 - 18]。

一方面是对标美欧网络战规制机制的战略需求，另一方面则是因为网络攻击的风险正在加速扩散。随着大数据、人工智能、机器人和物联网的兴起和蓬勃发展，预计到 2030 年互联网接入移动设备将接近 1 万亿台。① 这意味着网络攻击的覆盖范围和物理破坏性会越来越大，甚至会在关键时刻削弱国家的整体防御能力。随着所面临威胁的加剧，网络反击的策略需要做相应的优化和细化。

2. 日美网络战集体自卫机制的确立

对标欧美主要国家是日本完善网络安全保障体制的一个指向性明确的战略目标。在欧美主要国家，网络安全体制最主要的趋势特征是“网络战”的泛化。据此，日本既着眼于将来自他国的特定网络攻击视为武力攻击，并寻求通过自卫权加以应对，也积极谋求使用网络行动对其他国家和实体加以打击。2011 年 5 月，奥巴马政府在其《网络空间国际战略》中宣称，美国将使用军事手段（自卫权）来回应“通过网络空间从事的某些敌对行动”。② 2017

① Nye Jr. Joseph S.，“The End of Cyber - Anarchy? How to Build a New Digital Order”，*Foreign Affairs*，Vol. 101，January/February 2022，pp. 32 - 43.

② The White House，“International Strategy for Cyberspace：Prosperity，Security，and Opennes in a Networked World”，http：//www. whitehouse. gov/sites/default/files/rs_viewer/international_ stat - egy_ for_ cyberspace. pdf[2023 - 03 - 18].

年 1 月，时任北约秘书长斯托尔滕贝格（Jeans Stoltenberg）在达沃斯世界经济论坛的发言中宣称，北约已经确认网络攻击可以触发《北大西洋公约》第五条规定的集体自卫权。① 欧美国家的这些发展趋势不断推动日本在网络安全体制构筑上走向“网络战”泛化，从在网络战中实现个体自卫到实现与欧美国家的集体自卫，则是这一道路的明确路径。可以预计，未来在“太空战”领域，这一泛化道路也将是日本安全政策的必然趋势。事实上，2023 年 1 月的日美外长防长“2 +2”会谈已经明确显示，《日美安全条约》第五条将把应对以日本卫星等太空目标发动的攻击纳入新的适用范围。②

早在 2019 年的日美“2 +2”会谈联合声明中，对日本及驻日美军的网络攻击就已经被纳入《日美安全条约》第五条的适用范围③，该声明明确指出双方一致认为网络攻击在某些情况下可能构成《日美安全条约》第五条提到的武装攻击。④ 这意味着至少在日美之间已经形成了一个由双边条约认定的网络反击集体自卫机制。也正是从 2019 年开始，日本在网络安全战略上逐步由守转攻，从模糊的网络安全与风险防范逐步转向目标明确的网络攻防实战。可见，日本网络战攻势化政策的确立离不开美方外力的刺激和推动。为进一步推动日美网络攻防合作机制，2023 年 1 月 6 日，日美两国还签署了《加强网络安全的谅解备忘录》，规定为减轻网络攻击对政府系统造成的损害，两国将对政府采购的软件制定同等级别的安全标准。⑤

从实操层面看，日本也为网络反击能力在日美网络战集体安全机制中的行使与运用做了政策铺垫。一是通过政府在国会答辩的方式明确行使反击能

① NATO，“Redefining Europe’s Security Agenda：Panel Discussion with NATO Secretary General Jeans Stoltenbergat World Economic Forum Annual Meeting in Avos”，http：//www. nato. int/cps/en/natohq/0opinions_140226. html［2023 －03 －18］.

② 防衛省「日米安全保障協議委員会（日米『2 +2』）（概要）」、2023 年 1 月 11 日、https：//www. mofa. go. jp/mofaj/na/fa/page4_005748. html［2023 －03 －18］。

③ 日文原文为“国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安保条約第 5 条にいう武力攻撃に当たり得ることを確認した”，参见：防衛省「日米安全保障協議委員会（日米『2 +2』）」、2019 年 4 月 19 日、https：//www. mofa. go. jp/mofaj/na/st/page4_004913. html［2023 －03 －18］。

④ 第五条规定，“如果对日本或驻日美军发动武装袭击，两国必须作出共同反应”。参见：「日本国とアメリカ合衆国との間の相互協力及び安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定」、https：//www. mod. go. jp/j/presiding/treaty/chii/chii. html［2022 －03 －17］。

⑤ 「ソフトウエアに安全基準日米、サイバー防衛で覚書へ政府調達でインフラなどの対策強化」、『日本経済新聞』2023 年 1 月 5 日。

力属于日本行使集体自卫权的权限范围。2022 年 5 月 17 日，日本防卫副大臣鬼木诚在国会的答辩认为，在基于安全保障法制的集体自卫权行使范围内，发动对敌基地攻击在法理上是被允许的。具体来说，即在日本处于存立危机事态下（包括与日本有密切联系的国家受到武力攻击并危及日本存亡的事态），日本有权行使包括反击能力在内的集体自卫权。① 二是通过加入北约网络防御中心的方式，为在网络战实践中摸索具体的网络反击集体自卫规则积累经验，并以此为契机加强双多边网络战演训。北约网络防御中心组织专家编写的《塔林手册》第 74 条明确规定了网络战中的集体自卫规则，“自卫权可以集体行使。对构成武力攻击的网络行动的集体自卫，仅能根据受害国的请求并在请求的范围内行使”。② 因此可以说，日本在具备网络反击能力的制度储备上采取了“以外促内”的推进方式，即首先在双边集体安全条约上打开突破口，并在多边规则上做好铺垫，再伺机推动国内补充完善相应的制度和法律。

3. 国内法律与制度储备

根据前述日本政府对网络能动性防御和反击的设想，需要通过长时间的持续实时网络监控，识别和分辨网络攻击源，在定位后通过入侵敌方服务器或解除其破坏力达到反击的目的。而从现有日本国内法律来看，这些反击措施的推进还缺少相关法理基础，缺少关于反击实施主体授权、法律责任设定、监控存在安全隐患的国内通信的授权、国民个人通信隐私边界设定等问题的系统性法律规范。在日本政府酝酿围绕“能动性网络防御”理念推进日本网络安全法制逐步完善的过程中，诸多网络安全问题的研究者开始提出相关的法律修改意见和建议，比如应该尽快在国内推动对《网络安全基本法》的大幅修改。具体内容包括：一是将国家和政府作为网络防御的主体，将网络防御作为政府的法定责任。二是在此基础上赋予内阁及相关网络防御部门能够反向入侵对方攻击服务器的权限，提高主动开展网络防御的能力，增强日本的网络战能力。三是通过完善宪法解释设定通信秘密权的保护仅限于国民个人，通过修改《电气通信事业法》使得监控存在安全隐患的国内通信合法化。四是通过修改日本的《刑法》以及《禁止未授权访问法》等，授权政府溯源

① 「衆議院議員長妻昭君提出存立危機事態における『着手』に関する質問に対する答弁書（内閣衆質二〇八第六一号）」、2022 年 5 月 17 日、https：//www. shugiin. go. jp/internet/itdb_shitsumon_pdf_t. nsf/html/shitsumon/pdfT/b208061. pdf/ $ File/b208061. pdf[2023 - 03 - 18]。

② 迈克尔·施密特、丽斯·维芙尔：《网络行动国际法 塔林手册 2. 0 版》，第 355 页。

并进入敌国目标服务器等。①

为有效行使网络反击能力，日本还在进行各方面的战力储备，包括人才教育和储备、机构跨领域合作、作战队伍规模化等。除了上述提到的成立网络攻防新组织，防卫省与自卫队将在提高自身网络安全水平的同时，推进有助于加强与相关省厅、重要基础设施运营商以及防卫产业合作的措施。此外，日本政府计划将陆上自卫队通信学校改编为陆上自卫队系统通信网络学校，扩充培养网络人员的基础；从 2027 年度起，探讨在防卫大学新设网络防御学科，重点学习恶意网络病毒的搜索方法及实践技术，以强化自卫队队员的网络防御技术和实战能力。② 而且，日本政府计划以 2027 年度为目标，将自卫队网络防卫队的规模扩至约 4000 人，加上网络跨域作战的人员，防卫省及自卫队下辖的网络工作人员共约 2 万人。③

在网络战的军事演训方面，2022 年 11 月日本宣布加入北约网络防御中心④，该中心在网络防御训练、战略研究等领域拥有强大力量，主要任务是为北约及其成员国提供技术、战略、行动和法律领域的网络防御专业支持。作为一个国际军事组织，北约网络防御中心多次举行实战化网络攻防演习，特别是用网络攻击他国的关键性基础设施。日本此举标志着已经加入了北约国家的网络战攻防演练体系，而这也将为日本未来行使网络反击能力提供充足的类实战经验。

值得注意的是，日本要想推动实现行使网络反击能力，目前还存在着较大的技术短板。美国前国家情报总监丹尼斯・布莱尔曾称美日同盟的最大弱点是网络防御，日方退役海军上将吉田正纪对此也表示认可，认为日方需要尽快提高自身的技术能力。比如在防务部门的通信基础设施建设上，日方的技术配备就较为薄弱，并不具备现代战争所需的高速、大容量、高度保密、高度防御的通信体系。具体表现为：（1）自卫队还不能使用高频段的电子战设备；（2）5G 部署没有进展，多使用 4G 和 LTE 通信标准实现坦克等设备与

① 大沢淳「サイバー戦争 日本の危機―サイバー安保基本法―」、『日本経済新聞』2022 年 12 月 20 日。

② 「防衛大にサイバー学科 27 年度にも新設」、『日本経済新聞』2023 年 1 月 11 日。

③ 防衛省『防衛力整備計画』、https：//www. mod. go. jp/j/policy/agenda/guideline/index. html［2023－03－17］。

④ 「NATOセンターに参加 サイバー強化で防衛省」、『日本経済新聞』2023 年 1 月 5 日。

自卫队队员间的联系；（3）无人机被降级使用等。①

从前述网络空间的定义以及网络安全的指涉范围来看，网络攻防实际上与太空技术、电磁技术、通信技术等相互联系，又互为一体，所以日本在“新安全保障三文件”特别是《防卫力量整备计划》中将“跨域综合作战能力”作为一个整体和体系进行加强。比如在太空领域，通过采取利用民用卫星等各种补充措施，以获得目标探测、追踪能力为目的，构建卫星星座；除以往的X波段通信之外，还将推进抗振性更高的通信多层化举措等。在电磁波领域，日本政府也计划配备具有通信雷达干扰功能的网络电子战系统（NEWS），开发进行各种通信干扰及电子干扰的单机架电子战机，配备从地面进行雷达干扰的对空电子战装置，运用车辆搭载型激光装置应对小型无人机（UAV），等等。②

三、网络战攻势化转型对日本安全战略和中日关系的影响

日本持续推进自身具备和行使网络反击能力、推动网络战攻势化转型，将带来潜在的长远影响，从网络空间和主权观、网络安全治理等层面进一步刺激日本安全战略极端化的发展倾向，并在网络空间合作、亚太地区秩序等层面给中日安全关系带来负面冲击。

（一）对日本安全战略的影响

从安全观角度来看，日本网络空间观和网络安全观的偏执、异化倾向是日本国家安全观逐步偏激的具体表现，同时也对日本国家安全战略的进一步激进调整起到了推波助澜的作用。从2013年到2021年，日本每三年左右发布一次《网络安全战略》③，迄今已经出台四版。从2018年版的《网络安全战略》起，日本的网络空间观、网络安全观开始出现偏执、异化倾向。2018年的第三版《网络安全战略》开始渲染大规模网络攻击的巨大威胁，同年年底发布的《防卫计划大纲》中也对应强调了网络防卫能力的重要性。这说明网络安全

① 「サイバー戦争 日本の危機（2）命綱の通信、非力な自衛隊 Wi－Fi・5G、整備遅れる」、『日本経済新聞』2022年12月21日。

② 防衛省『防衛力整備計画』、https：//www. mod. go. jp/j/policy/agenda/guideline/index. html［2023－03－17］。

③ サイバーセキュリティ戦略本部「サイバーセキュリティ戦略2013—2021」、内閣サイバーセキュリティセンター（NISC）、https：//www. nisc. go. jp/policy/materials/index. html#material－cyber_security［2023－02－14］。

战略已经成为日本国家安全战略的重要组成部分。2021 年 7 月日本发布第四版《网络安全战略》，进一步强调国家面临大规模网络攻击的国家安全威胁，并渲染网络攻防已经成为国家间综合博弈的又一个主要战争形式。2022 年的新版《国家安全保障战略》也相应强调强化举国网络防御体制，将自卫队等国家暴力机器纳入网络防御主体，进一步强化了网络安全战略在日本整体国家安全战略中的地位。从时间线来看，每一次《网络安全战略》发布的当年或次年，日本都会对本国的整体国家安全战略进行一些重大调整，包括2013 年 12 月出台首个日本版《国家安全战略》、2015 年推出“新安全保障一揽子法案”、2018 年 12 月发布新版《防卫计划大纲》以及 2022 年 12 月通过“新安全保障三文件”。可以看到，日本的网络空间观、网络安全观已经成为日本国家安全观偏激化调整的晴雨表，特别是网络空间观和网络安全观的偏执、异化倾向，以及网络主权观的极端泛化苗头，更集中体现了日本国家安全战略的重要调整方向。

从网络安全治理视角看，日本在构筑网络安全治理机制过程中出现了明显的网络战泛化、网络空间军事化的倾向，这集中体现了日本国家安全战略背离战后和平主义的初衷，并退回到极端和异化的冷战思维。日本“能动性网络防御”的理念折射出其“武力制网”的政策倾向，这沿袭了西方某些大国对自卫权扩大化解释的无理做法，带有极大的主观性和任意性，反映出日本寻求通过单边军事行动来应对外部网络威胁的零和博弈思维。这一思维会冲击其传统防卫领域的安全战略及策略，产生极大的反噬效应，将严重破坏国际法基本原理和国际道义及公理。

从军事战略层面看，日本推动网络战攻势化转型为其介入台海局势提供了新的抓手。随着近年来日美在安全合作中设置涉台海议题，日本被动卷入或主动介入台海局势的可能性正在变大。此前日本已在日美合作、防务交流等层面持续进行政策储备：2021 年 12 月，日本宣称日美两国军事部门已制定“设想台湾出现突发事态”的“新日美联合作战计划”，为其介入台海提供所谓“依据”①；2022 年 6 月，日本决定向其驻台北事务所派遣防卫省“现役”职员，以加强与台湾当局的意见和情报交换②。“新安全保障三文件”通过后，日本更在涉台战略战术和军力部署上周密计划，突出“能动防御”“以攻

① 《日媒：为介入台海局势 日美两国正在加紧进行各种准备》，央视网，2021 年 12 月 30 日，http：//www. news. cn/mil/2021 - 12/30/c_1211506367. htm[2023 - 04 - 17]。

② 《日媒称日本拟首派现役自卫官“驻台”》，中国台湾网，2022 年 6 月 5 日，http：//www. taiwan. cn/taiwan/jsxw/202206/t20220605_12441260. htm[2023 - 04 - 17]。

代守”“反区域拒止”，包括酝酿在距离台湾仅 110 公里的与那国岛部署导弹部队、购买美制“战斧”巡航导弹、规划 2026 年之前具备陆海空三位一体的远程打击能力等。日本以“打台湾牌”为依托、强军备战的行径，已成为影响中国国家安全的新外部干扰因素，并可能演变为重大地区安全风险。2023 年 1—3 月，日本笹川和平财团、国际问题研究所（JIAA）等政策智库[①] 更是接连围绕“日美台应对台海有事”进行兵棋推演，为日本政府决策提供参考。上述“台湾有事”兵棋推演显示，应对针对台湾地区的网络攻击成为日本推演的固有假想推演场景，网络战和太空战将成为未来台海冲突博弈的重要内容。

（二）对中日安全关系的影响

日本加剧网络安全治理军事化的做法将打击中日在网络空间层面加强合作的积极性。中日之间的网络安全治理合作并非没有基础，两国一度在东亚中日韩多边层面形成了持续性的网络安全治理多边合作局面。在 2002 年东盟与中日韩（10 +3）领导人会议上，信息通信被确定为中日韩三国的重点合作领域之一；同年 9 月，中日韩三国正式建立信息通信部长会议机制并成立司局级工作组；11 月，三国互联网协会结成联盟，并签署“谅解备忘录”；2011 年，三国签订了“国家级计算机安全事件响应小组联合合作备忘录”。在这一框架下，三方近年来成功处置了多起重大网络安全事件，7 ×24 小时热线机制也在发挥重要作用。2014—2017 年，中日韩举行了三次关于网络安全事务磋商机制的会议。2016—2017 年，中国国际问题研究院与日本庆应义塾大学、韩国高丽大学共同举办了两次网络安全二轨对话会。[②] 5G 时代到来后，随着人工智能、大数据、云计算、物联网等新技术的应用与推广，中日韩三国本应借助时代的潮流进一步加强合作，但从 2018 年 12 月日本公布新版《防卫计划大纲》并提出要强化网络作战部队的人员规模和作战能力，2022 年 12 月又出台了新版《国家防卫战略》和《防卫力量整备计划》，网络战攻击态势进一步强化，日本从网络攻防层面发展对华非对称战力、加强对华威慑的意图更为明显。如果不及时悬崖勒马，日本对华整体安全政策可能会进一步偏向军事对抗，中日双方安全风险将从传统领域向新边疆领域扩大和蔓延，继而增加中日之间发生军事冲突的可能性，从而损害中日关系的稳定发展。

① 小谷哲男「台湾海峡有事シミュレーション—概要と評価—」、日本国際問題研究所研究レポート、2023 年 3 月 30 日、https：//www. jiia. or. jp/research - report/security - fy2022 - 04. html[2023 - 04 - 17]。

② 徐龙第：《中日韩网络合作：进展、基础与前景》，《信息安全与通信保密》2018 年第 2 期，第 46—50 页。

日本网络战攻势化转型基于其网络安全泛化的战略和威胁认知，使日本在对待人工智能等新兴网络技术政策时首先秉持威胁在先的基本认知，且将其与社会制度、意识形态、价值观等问题捆绑，加大了中日之间在网络安全政策层面进行合作的困难和障碍。2023 年 4 月 29 日的七国集团数字与技术部长级会议上，日本利用主场优势，诱导与会国家在人工智能政策上倡导制定具有排华倾向的风险评估国际标准，以西方民主价值观作为所谓的划分依据，在 AI、数据流动、网络基础设施等多个层面推行所谓基于法治、人权的高性能人工智能风险评估国际规范，其中特别提到了在人工智能领域针对网络攻击的防御系统的建设上制定符合七国集团认知的统一标准。① 这也充分体现了日本在网络安全乃至网络攻防层面的主动性、进攻性、零和博弈性和泛军事化的攻势化战略理念。

从学理层面看，日本的网络战攻势化转型也会增加中日双方在包括网络战在内的网络安全规范相互约束上的困难。约瑟夫·奈认为，协调、审慎、声誉成本和国内压力（包括公共舆论和经济变化）是影响国家之间相互约束效力的四个变量。② 对规范产生共同的良好期待并加强协调是中日加强进一步合作的前提，但推动网络战攻势化转型将给双方产生的共同期待带来明显消极影响。审慎是由于担心在不可预测的系统中造成意想不到的后果，也可以发展出不使用或有限使用某些武器的规范或限制目标的规范。而日本提出的“能动性网络防御”原则和体现出的预防性威慑理念无疑站在了审慎的对立面。

与此同时，对国家声誉和软实力受损的担忧也会带来自愿的克制，希望这会成为日本在推动网络战转型上的“减速器”。自 2022 年 12 月岸田政府出台“新安全保障三文件”后，日本国内部分在野党比如日本共产党以及国内外舆论开始出现一些对日本是否还能坚持战后和平主义道路的担忧和质疑的声音，这可能会使日本的激进安全政策有一定收敛。

四、结　语

凡事预则立、不预则废。面对中日之间不断上升的网络安全冲突风险，

① 「AIのリスク認識共有 G7 担当相会合閉幕、安全活用で一致」、『日本経済新聞』2023 年 4 月 30 日、https：//www. nikkei. com/article/DGXZQOUA2740N0X20C23A4000000/［2023 - 05 - 01］。

② Nye Jr. Joseph S.，“The End of Cyber - Anarchy? How to Build a New Digital Order ”，*Foreign Affairs*，Vol. 101，January/February 2022，pp. 32 - 43.

两国应增强对网络安全领域敏感问题的辨识意识和预判能力，加强风险管控。第一，要从构建建设性安全关系这一共同的战略共识出发，在现有的中日高级别政治对话、中日战略对话、中日安全对话以及外交当局定期磋商、中日海洋事务高级别磋商等协调对话平台中增加网络危机管控的议题，增强在网络空间的战略互信。第二，在网络冲突规则方面充实现有的海空联络机制，探讨中日之间确立可操作性强的网络冲突规则的可能性。第三，将网络作战力量也纳为中日防务交流的对象，加强中日相关防务部门间的互访与交流，培育作为过程的信任建立措施（CBMs）是巩固两国安全机制并实现更高层级安全关系的重要手段。第四，增加学界关于网络安全问题的对话和交流。中日学界都非常关注“塔林手册”中诸多网络空间的国际法规则问题，比如中国学者黄继雄团队① 和日本学者中谷和弘② 等分别于近年翻译了“塔林手册”，并阐释了关于网络空间国际法规则的各自观点，但目前还未见到两国学者关于这些问题的密集交流，这或许是中日学界亟待解决的问题。

中日加强网络战在内的网络安全危机管控具有必要性，但加强管控是否具有可能性，这又是一个兼具学理和现实意义的问题。客观来说，中日之间具有意识形态的差异性，而这可能会减弱双方的战略互信，进而产生陷入安全困境、导致自我预言实现的风险。但正是由于有了对上述风险的预期和认知，两国才更应该建立相关协商进程来遏制冲突和风险。约瑟夫·奈在谈到美俄之间网络危机管控可能性时也没有过于悲观，认为“意识形态的差异会使达成详细协议变得困难，但更大的意识形态差异也没有阻止在冷战期间帮助避免事态升级的协议”③。因此需看到，意识形态差异仅增加了两国危机管控的困难，并不意味着完全失去了管控可能，我们对中日之间的网络危机管控应该保持谨慎乐观。

（责任编辑：陈梦莉）

① 迈克尔·施密特、丽斯·维芙尔：《网络行动国际法 塔林手册 2.0 版》，2017 年。

② 中谷和弘・河野桂子・黒崎将広『サイバー攻撃の国際法―タリン・マニュアル2.0の解説―』、信山社、2018 年。

③ Nye Jr. Joseph S.，“The End of Cyber－Anarchy? How to Build a New Digital Order ”，*Foreign Affairs*，Vol. 101，January/February 2022，pp. 32－43.

Abstracts

The Offensive Transformation of Japanese Cyberwarfare

Zhang Xiaolei

The concept of "counterattack capability" reflects Japan's offensive transformation direction in military strategy, laying the groundwork for Japan's promotion of cyber warfare transformation at the strategic and conceptual levels. The possession and exercise of cyber counterattack capabilities is a concentrated manifestation of Japan's promotion of the offensive transformation of cyber warfare. In recent years, with the strengthening of Japan's cyber security strategy and the continuous promotion of cooperation with the U. S. and Europe in cyber security, Japan's military strategic concept to enhance the offensive transformation of cyber warfare has progressively crystallized, and policy reserves have been continuously improved. The generalization of Japanese cyber warfare and the militarization of cyber security governance will have a significant impact on Japan's security strategy and Sino-Japanese relations. China and Japan should strengthen crisis management and control at the level of cyber security.

The Trend of Militarization of the Japan Coast Guard

Cheng Yun

The Japan Coast Guard is moving towards militarization, which has become even more apparent with the introduction of new versions of the "three defense documents" and the "Outline of Control Essentials". Despite the Japanese government's strong denial of militarization and their repeated emphasis on the police attribute of the Japan Coast Guard, the boundaries between "police" and "military" remain blurred, and there is a further promotion of seamless connection between the two departments. The article argues that the essence of the militarization of maritime police lies in the continuous expansion of their functions aligned with the navy's mission and the promotion of their own system reform. The recent developments in the construction of the Japan Coast Guard align with this direction. The trend of militarization within the Japan Coast Guard is primarily reflected in three aspects namely operations, equipment and personnel cultivation. In terms of operations, it is evident in the integrated construction of the intelligence system, logistics system and command system between The Japan Coast Guard and Japan Maritime Self-defense Forces. The equipment aspect is seen in the common research and development of weapon technology and the improvement of equipment interoperability. Although there are currently significant differences in terms of personnel cultivation between the two sides, personnel exchanges continue to progress. In the future, the militarization of the Japan Coast Guard will bring about a series of negative impacts. It will not only deepen the security dilemma between China and Japan, but also hinder the direction of international cooperation among maritime police in East Asia. Furthermore, it will further bind