俄乌战争中网络对抗的影响与启示

王伟杰，3210106034

摘 要： 俄乌战争爆发后，除了正面战场的冲突，两方在网络信息方面的冲突也越来越激烈，这是现代战争一个不容忽视的方面。战争期间，双方在网络破坏、社交舆论和信息网络各个方面进行了政治社会动员、放大矛盾情绪和经济制裁打压动员等措施。社交媒体不仅随时将战争情况实时播报给世界民众，还在一定程度上左右战争进度。通过分析俄乌战争中的网络对抗能得到一些关于现代战争的启示。

关键词： 俄乌战争；网络战；社交媒体；信息战；公共舆论

The Influence and Enlightenment of Network Confrontation in the Russian Ukrainian War

Wang Wei-jie,3210106034

Abstract: After the outbreak of the Russian Ukrainian war, in addition to the conflict in the front battlefield, the conflict between the two sides in network information is becoming increasingly fierce, which is an aspect of modern war that cannot be ignored. During the war, the two sides carried out political and social mobilization, amplification of contradictory emotions and economic sanctions to suppress mobilization in all aspects of network destruction, social public opinion and information networks. Social media not only broadcasts the war situation to the world people in real time at any time, but also influences the progress of the war to a certain extent. By analyzing the network confrontation in the Russian Ukrainian war, we can get some enlightenment about modern war.

Key words: Russia Ukraine War; Network warfare; Social media; Information warfare; Public opinion

1 黑客打击政治化

在之前的军事行动中，美国已经熟练使用过黑客技术进行军事打击。如 2019 年委内瑞拉国内危机时，委内瑞拉政府就曾经指控过美国是造成 3 月国家级大停电的元凶，当时国内公民生产生活陷入大面积瘫痪，7 月委内瑞拉再次大面积停电，这使得政府公信力急剧降低。2019 年 6 月特朗普在对伊朗军事行动的最后阶段也曾叫停过军事打击而使用网络攻击手段“摧毁了一个非常重要的数据库”。这些例子说明网络空间早已可以承载国家之间的政治与军事问题，并且与现实相关联的特点。

而在 2022 年以来，乌克兰连续遭受大规模网络攻击，政府、军队等网站主要受到分布式拒绝服务攻击，许多重要网络系统瘫痪，一些非盈利性政府、非政府组织的数据被破坏。乌克兰指责俄罗斯为凶手，但俄罗斯一直否认。直到 2 月 27 日，乌克兰宣城自己组建了一支“信息志愿部队”，开始对俄罗斯实施网络作战任务。这支队伍还有一些“黑客志愿者”对俄罗斯的军方设施和国家级媒体等网络进行破坏攻击，阻挠

俄罗斯的各种军事行动并泄露了大量机密文件，对俄罗斯的正面军事行动造成了阻滞和打击。

乌克兰能够成功打击俄罗斯也离不开美国的大力支持，美国提供的“星链”系统（Starlink）帮助乌克兰被攻击的一些基础设施恢复了正常运转，目前“星链”系统仍在为乌军的指挥机构和一线部队间的通信服务。美国还针对俄罗斯的信息核心技术和基础设施阻断了“供应链”，包括甲骨文、惠普等大型美国公司已经暂停向俄罗斯交付产品，在美国的商业控制清单（CCL）中，微电子、电信项目、传感器、导航设备、航空电子设备、海洋设备和飞机部件等各种设施已经被纳入禁令，全面制裁俄罗斯的电子信息领域。当地时间 5 月 4 日，《纽约时报》报道，美国为乌克兰提供了大量俄军情报，这些情报帮助乌军击杀多位俄军将领，乌克兰官员也承认获得过美军帮助。

至此，黑客已经正式登上政治舞台，不过美国等国家动用国家力量进行网络攻击还是第一次出现在大国之间的较量中，之前的一些网络冲突只是运用在对小国的制裁等行动中。所以在这次行动中，美国的行动也极为谨慎，不仅出台了大量的法令，还通过召集民间黑客组织介入等方式拓宽攻击渠道，但这也使得战争结束后民间黑客组织与国家之间的关系变得极为复杂。

2 舆论攻击占据制高点

新时代的媒体占据了绝大部分人的生活空间，舆论也是主导公民对某场战争正义性的唯一认知来源。于是关于俄乌战争的舆论掌控争夺就变得异常激烈。美国在国际舆论中的地位使得俄罗斯在战争中的舆论地位处于及其不利的位置。在冲突爆发之前美国就将俄罗斯的出兵日期等信息公布在了网络平台，并删除了油管（Youtube）等相关平台上的俄罗斯官方账号，这使得大部分网民只能获得乌方的一家之言。

甚至美方还散布消息指责中国帮助俄罗斯进行战争，迫使中国声明不对任何国家进行军事上的帮助。互联网不仅可以通过公共舆论宣传使某一方成为“民心所向”，还可以通过“公共外交”使得第三方无法介入这次战争，为自己赢得一个稳定的战争环境。如果某些国家手中掌握着社交平台的控制权，那么这将成为一个极其强大的杀器，海量用户将通过这些平台展开看似无实质意义的“攻击”，并对第三方甚至战争参与者的决策产生重大影响。

舆论战的特点是参与方不再局限在实际利益相关者，而是使全球网民都成为了战争者的“武器”，互联网对战争的全程直播使得社交媒体的舆论压力迅速传播到军队中并对军事行动产生影响。而目前一些较强大的社交媒体掌控者是可以通过封控账号等形式强行掌控战争的主导权，左右各方的军事行动部署。

总的来说，网络空间舆论的战争就是战争双方争夺战争合法性和战争进程解释权的网络对抗战争。

3 互联网资源在军事制裁中的应用

信息技术的大规模使用已经改变了现代战争的风貌，各种科技公司已经或者正在掌握网络空间的技术节点和重要的数字资源。它们不仅掌握了大量的经济资源，还分担了一些原本应由国家掌控的资源，如网络安全等公权力。随着越来越多的西方互联网企业在俄乌战争中选择支持乌方，俄罗斯也被它们所掌握的互联网资源“制裁”。域名解析层上，多家互联网运营商曾经对俄罗斯发起“断网”行动，停止向俄罗斯用户提供服务；内容层上，一些互联网企业删除了俄罗斯相关账户，制止俄罗斯发布相关信息；应用层方面，苹果等公司宣布下架俄罗斯的一些产品应用，谷歌地图甚至开放俄罗斯军事设施的高清俯视图，给俄罗斯带来很大的军事安全隐患。

现在，互联网资源也有各国进行“军备竞赛”的嫌疑，美国目前仍旧是互联网资源最大的持有者，技术优势使得它成为拥有网络情报搜集能力和网络攻击能力的强大国家。而在西方阵营之外，更多的东方甚至非洲国家在互联网领域几乎是没有任何话语权的。未来，美国必将凭借其巨大的技术和产业规模优势，继续推进其在互联网资源领域的霸主地位。

4 在面对新时代网络对抗中的启示

俄乌战争看起来似乎只是一场双方战争，但是通过网络，他们将世界各地的黑客、网民都拉入了“战场”，呈现了数字战争的新形态，甚至网络对抗的战争将会比现实中的战争持续更长时间。尽管过去中国在维护网络安全方面已经做出了极为巨大的努力，但在目前的形势看来还是不够的，我们不仅要在危难到来时有保护我们的军事信息的能力，还要有应对铺天盖地而来的舆论压力、信息技术制裁压力、黑客攻击压力等。

在此形势下，维护多边主义主导的网络空间局势仍是必要的。在网络对抗战中，事态往往不是纯粹的双方战争，而是各种民间组织、国际组织、各国政府均参与其中的一场博弈。如果仅靠利益相关者进行调解很难遏制这种危害网络空间安全的行为。国际社会应该在相互尊重，彼此充分交流的基础上加强网络问题方面的合作，建立一整套关于网络信息空间的协议，保护各方网络公平。

中国在如今的网络空间对抗行为中应该加强自身的信息技术建设，积极与国际方面合作突破壁垒，同时建立有公信力的一个或几个社交媒体平台，防止我们的信息被“卡脖子”，杜绝某些国家牢牢将网络控制权把握在自己手中的行为。这是确保网络安全整体趋于稳定的最重要的方面，也是我们作为网络大国不可忽视的重要安全问题。

参考文献：

[1] 赵子鹏,张光迎.黑客组织站队俄乌冲突的影响分析[J].中国信息安全,2022,No.152(07):108-111.

[2] 郎平.从俄乌冲突看网络空间武器化倾向及其影响[J].中国信息安全,2022(06):66-69.

[3] 严明.对俄乌冲突中网络空间对抗的思考[J].中国信息安全,2022(06):70-72.

[4] 李恒阳.俄乌冲突网络对抗及其对网络空间安全的影响[J].中国信息安全,2022(06):83-86.

[5] 刘军.社交媒体对俄乌冲突的影响分析[J].人民论坛,2022(13):108-111.

[6] 罗昕.计算宣传:人工智能时代的公共舆论新形态[J].人民论坛·学术前沿,2020(15):25-37.DOI:10.16619/j.cnki.rmltxsqy.2020.15.003.

[7] 冯绍雷.欧洲对抗与亚洲突围——全球转型中的欧亚新博弈[J].俄罗斯研究,2022(01):84-91.

[8] 董青岭,戴长征.网络空间威慑:报复是否可行?[J].世界经济与政治,2012(07):99-116+159.

课程（论文）心得与建议:

在撰写这篇论文之前，我其实对俄乌战争并没有一个大致的概念，甚至连他们之间为什么会有这场战争都不是很清楚，在程老师的课堂上让我燃起了对这场战争一探究竟的兴趣，于是我就去查阅了一些相关的资料。我的专业是软件工程，隶属于计算机科学与技术学院，对于信息化方面的东西有一种莫名的敏锐察觉力，很快就发现了这场战争与我意识中的传统战争很大的不同之处就在于网络对抗的加入，于是我进一步地去查阅资料，思考分析，最终完成了这篇论文。

我认为这门课程极大地使我提高了对军事方面的一些认识，了解了各个国家的军事教育理念和我们还需要努力去做的地方。在今后的学习生活中我也会去专门留意一些目前的国防进展，做一个合格的中国公民！