

模糊的边界：论网络时代军事信息泄密问题

孙 林

(中共中央党校 党建部, 北京 100091)

摘 要: 在网络时代, 数字化的信息超越了时间、空间和行业的限制, 在网络空间中海量、迅捷、交互地传播, 信息的强关联为基于网络搜索引擎的公开情报搜集提供了可能。军事信息是各国情报搜集的重中之重, 伴随着大数据、云计算的发展, 信息强关联造成的公开和秘密信息之间的边界日渐模糊, 公开信息泄密和公开情报搜集相伴而生, 造成网络空间更加复杂的安全形势。

关键词: 网络; 军事信息; 网络泄密; 信息安全

中图分类号: D820

文献标识码: A

文章编号: 1672-0962 (2015) 04-0016-04

2013 年曝光的“棱镜门”事件将网络安全问题推上了风口浪尖, 使之成为全世界关注的焦点。实际上在网络时代, 网络攻防战无时无刻不在上演, 其中, 军事信息是重要的对象目标, 军事信息安全问题日渐凸显。一般而言, 军事信息安全问题主要表现为军事泄密、黑客攻击和信息战三个方面 (陈岸然, 2003)。其中, 军事信息泄密问题随着网络终端技术的快速发展而变得越来越严重。在我国, 在研、试验、装备的军事武器以及军事部署、军事活动等军事信息都存在着不同程度的网络泄密问题。网络高度的开放性、互动性和便捷性, 对军事秘密信息的有效防护提出了严峻挑战。

一、军事信息泄密面临的新形势

随着网络信息终端技术的发展, 网络空间、网民社会、网络新媒体、多元社会结构交互发生作用, 使网络成为一个日渐独立、开放、多元、互动密集、联系普遍的新空间、新场域, 通过与现实物理世界频繁进行海量的信息交换, 网络空间的地位和作用不断提升。树大则招风, 墙高则影长, 正如硬币总有正反面, 网络空间在价值跃升的同时, 网络攻击、网络泄密等网络安全问题也随之而来, 这使得军事信息泄密面临更加严峻复杂的新形势, 具体而言表现在以下几个方面:

(一) 大数据技术使军事信息泄密门槛不断降低

基于网络信息技术的大数据技术在“努力将一切数据

化”的同时, 塑造了一个在数据上彼此紧密关联的复杂信息生态。军事信息及其周边信息被数据化之后, 基于数据上的关联, 一些机构和个人可以很容易地利用大数据技术增加数据样本, 以目标军事信息为中心建立大数据的数据块, 通过相关性分析, 获得军事信息中的关键数据或预测军事信息的发展趋势。此外, 大数据技术的快速发展, 使数据之间的边界日益模糊, 相应地, 数据所表达的信息之间的界限同样模糊。信息或数据边界模糊加大了军事信息的保密成本, 由于大数据技术可以利用周边信息的相关性分析得出核心信息, 这样一来, 军事信息的周边信息的重要性在不断提升, 与此对应, 泄密的信息面也在不断扩大, 最终可能会超出军事信息保密能力范围, 这就使泄密的门槛进一步降低。

(二) 网络新媒体使军事信息泄密的几率不断提高

网络进入 Web2.0 时代后, 以多向即时互动为特征的网络沟通成为网络空间的“基础规则”。以微信、新浪微博、推特、脸谱等为代表的新媒体, 依托网络信息终端设备技术的快速发展, 深刻改变了信息传播方式。新媒体将信息接收和发布者叠合起来, 构建原子数量的自媒体, 强力推动社会进入个体互联网时代。在个体互联网时代, 个体的信息获取能力、发布能力和影响力都得到了极大的提高。

不仅如此, 由于个体在时空上的分布是全面的, 即在任何时段、任何相关地点都可能有机体存在, 这就使得军事信息时刻处于被个体感知的状态, 任何重要军事信

收稿日期: 2015-06-03

作者简介: 孙林 (1984-), 男, 安徽颍上人, 法学博士, 中共中央党校党建部讲师, 中国人民大学当代政党研究中心助理研究员, 研究方向为政党与政党制度、网络与政党等。

息的变化,哪怕只是细微的变化都逃不过众多个体的电子感官,这使得军事信息泄密的几率大幅度增加。例如,2012年端午节前,有网络个体拍摄到我国某款战机运输照片,随后更多的个体加入拍摄该型战机公路运输照片的行列,并在网络上发布。将这些照片连起来播放几乎就是该型战机公路运输的全景图,虽然该型战机用迷彩帆布包裹严实,没有展示具体型号,但专业机构和人员很容易就可以通过这一连串照片推测出战机的尺寸和研发进展等重要信息。

(三) 多元社会增加了军事信息保密成本

改革开放以来,我国经济保持持续、快速、健康发展,社会结构逐渐多元化,利益主体和利益诉求逐渐多样化。应当承认,社会主体多元化和个性化已不是一个趋势,而是一个现实。在多元社会中,人们的利益诉求多元、思想观念多样,这在网络空间中表现得更为明显。多元社会使军事信息保密针对的对象更加模糊,亦使军事信息保密敌友难辨。近年来,大学生、白领、出租车司机、机关工作人员泄密或充当境外机构间谍事件表明,多元社会中军事信息泄密人群正在多元化,相应地,军事信息保密工作难度在加大,保密成本在增加。

二、军事信息网络泄密的新特征

保密和泄密是一个此消彼长的矛盾体,要分析军事信息网络泄密的新特征,需要反向从网络情报搜集的角度介入考察。

(一) 军事信息网络搜集的矛盾性

战争的根本问题是如何保存或保护自己并消灭或削弱敌人,换言之,战争本身是矛盾的复合体。网络也同样是复合体,既是矛又是盾,网络能够用来进攻,也同样能够用来防御,网络能够用来搜集军事信息也会泄露军事信息。对各国情报机构来说,网络正如一枚硬币一样,有正面和反面。各国情报机构一方面要采用多种网络信息技术手段对他国的军事信息网站、军事信息数据库、重要军事设施进行网络入侵或攻击;另一方面,还要防止本国的重要军事信息被泄露到网络上,阻止国内外黑客以及他国情报机构对己方军事网站、数据库、重要设施的入侵。由于基于网络技术的信息具有体量大、传播速度快、成本低廉、传播形式多样、多向互动等特征,即使采取公开、和平的手段也能够获取大量的重要的军事情报信息。国外实践表明,从网络上获取的军事信息具有价值高、数量大、成本低、时效快的特点,所以,世界各国无不把网络作为军事信息搜集和反间谍的重要场域与空间。

(二) 军事信息网络搜集的可能性

网络上公开的信息中隐藏了大量的有价值的情报,虽然这些数字信息的价值密度不高,但通过大数据技术能够淘出相当数量的“珍宝”。目前,各种公开出版的报纸、杂志,各种论文、书籍等几乎全部都被数字化变成电子信息

在网上传播,各种军事机构和单位一般也都设有自己的网站或内部基于局域网的信息系统,而且许多军事爱好者、军人也经常上网,一些人经常在网上发布一些含有极高情报价值的信息。国外情报机构通过网络搜索引擎来捕捉、搜集、整合,并进行专业分析,就可以得到非常重要的情报信息。

(三) 军事信息网络搜集的有效性

公开的情报搜集具有有效性。例如,二战期间,英国人雅各布专门研究德国主要报刊发表的有关德军驻防、演习、人事任免、装备更新等方面的军事信息。这些信息单独看来并没有太多的价值,但雅各布把公开搜集的德军信息分类整理,分别用不同的卡片记录不同的信息。经过长期的搜集整理,当他把这些卡片信息综合起来的时候,一份有关德军编制结构、主要军事指挥官以及驻防、装备、训练情况的完整信息就呈现出来了。不仅如此,雅各布利用已有资料信息经过精心研究,还发掘出大量德军的秘密信息(李治民,2004)。在网络时代,这种公开搜集各种军事信息的情报获取方式变得更加简单了,通过网络搜集军事信息的有效性较之二战时期大大增强了。

网络的最大特征是开放,网络上的信息开放为公开搜集军事信息提供了诸多便利。不仅如此,利用网络信息技术对所搜集的信息进行分类整理的效率也较之前有了极大的提高。“魔鬼藏在细节之中”的逻辑与军事信息网络搜集有效性的逻辑是同构的,即秘密信息就藏在公开信息之中。目前,通过网络获取情报已成为不少国家情报部门搜集情报的重要手段。情报搜集大体分为公开渠道的情报搜集、秘密渠道的情报搜集,网络搜集情报也分为公开方式和秘密方式。其中,采用公开或半公开情报信息搜集方式所获取的信息本身或许不具有直接的情报价值,但通过专业人员的分析和研判,就会产生情报价值。美国中央情报局曾做过这样的实验,将网络搜集的公开信息资料交给一个专业的研究团队,委托这个团队利用这些公开信息分析出“俄罗斯如何评价美国国防力量”的结论。结果,这个专业的研究团队在两三周内即对美国国防力量的大部分情况作出了比较准确的判断(李东风,2006)。由此不难看出,基于大量公开信息的网络情报搜集具有不言自明的有效性。据统计,各国情报机构的情报仅有20%是通过秘密渠道获取的,其余都是通过公开的渠道搜集的,这其中又有将近50%来自网络上的公开信息,由此可见,网络泄密问题的严重性。

(四) 军事信息网络搜集主体的专业性

美俄等情报大国均成立了专门的网络战部队和机构,由其负责通过网络搜集军事情报信息。例如,美国中央情报局早在2005年11月就成立了公开信息中心,负责每天在全世界的各种新闻网站、军事论坛、博客、微博等媒介中搜集各种各样的军事信息。通过对这些公开搜集到的信

息进行分类整理、分析研判、归纳总结,美国中央情报局可以准确发现或预测他国的最新军事动向、军事装备发展进展等重要军事信息。

三、军事信息网络泄密的主客体分析

在网络时代,军事信息泄密主体日益多元化,军事信息泄密的面积、密级、程度都比网络兴起之前有较大的改变,具体表现如下:

(一) 军事信息网络泄密主体多元化

网络时代,军事信息网络泄密主体呈现出多元化的特点,不仅从事军事工作的人群中存在泄密行为,连非军事人员也存在泄密问题,概括而言,当前军事信息泄密主体分类如下:

1. 军人。军人因具体从事军事工作,在日常工作中经常接触到相关的军事信息,甚至这些日常工作都是军事信息的一部分。在网络时代,军营不是网外之地,一些军人在上网期间,有意无意地透露出与军事工作相关的信息,就会造成泄密事件。随着移动互联网技术的快速发展,手机等移动终端成为获取信息、交流交易的重要工具,军人使用手机上网聊天泄密的几率也在大大增加(杨涛,等,2011)。

2. 军事科研机构工作人员及其社会关系。军事科研机构工作人员能够掌握大量前沿性军事科技信息,而其又作为社会人存在,在生活中存在泄密的可能。此外,军事科研机构工作人员的社会关系也是军事科技泄密的重要主体。

3. 军事迷。指酷爱军事题材及军旅文化的自发性群体,也称为军事爱好者、军事发烧友,广义上也指有军队情结、爱好军事文化的群体。这类群体在某一方面具有较为专业的知识,在网络虚拟空间中,这些群体在上网聊天、发帖的过程中也可能造成泄密。特别是所谓的“爬墙党”、“卧草党”发布的大量原创性图片、视频、文字,其间可能隐藏了大量具有情报价值的信息。

4. 一般网友。由于受好奇心、虚荣心支配发布涉及军事的信息,也可能导致泄密。

5. 主动或被动的间谍。根据国家安全机关统计,目前被境外间谍机关策反的群众并不罕见,退伍军人、留学生、高校师生、军事发烧友以及军工企业、国防科研单位、政府机关人员等,都是其着重关注的对象。尤其是一些年轻的网友,很可能在不知不觉中被境外人员利用。

(二) 军事信息网络泄密等级高

近年来,随着我军武器装备现代化水平的快速提高,海陆空二炮主战装备信息在网络上传播日益广泛,相关的泄密问题也比较严重。从已公开的情况来看,海军052系列驱逐舰、054系列护卫舰、09x系列核潜艇、03x系列常规动力潜艇、16号航母平台等,陆军99/96系列主战坦克、新型轻型坦克、05式自行榴弹炮、03式远程火箭炮等,空

军两型四代隐身工程试验机、歼11/15系列重型战斗机、歼10战斗机、无人机、红旗系列防空导弹,二炮东风21系列中程弹道导弹、东风31系列远程弹道导弹、东风11/15近程弹道导弹等主战装备的设计外形、基本性能、部署情况、制造工艺细节等都不同程度地在网络上传播,已经造成严重的泄密问题。

(三) 军事信息网络泄密面积大

随着国防教育的深入推进,国内军事论坛、网站、博客、微博、微信公众号如雨后春笋般地涌现出来,人们在方便获取军事信息的同时也提高了军事信息网络泄密的几率。据统计,目前网络泄密发案数已占泄密案件总数的70%,并呈逐年增长趋势,使国家利益受到严重损害(汤巍,2010)。

四、军事信息网络泄密的方式分析

网络传播信息具有多样性的特点,网络上的军事信息可以采用图片、文字、视频、音频等多种表现形式,因此,军事信息网络泄密的方式也是多样的。总结起来,泄密方式主要有以下几种:

(一) 直接泄密

直接泄密是指个体或机构所发布的军事信息为国(境)外情报机构所希望获得的,并在获得后直接使用的信息。需要说明的是,直接泄密者并不一定存在主观上的故意,例如,一些网友将所拍摄的军事图片、视频等信息直接放到网络上以炫耀能力或积累人气,也会在客观上造成直接泄密。直接泄密危害极大,应在法定情形下追究当事人的法律责任。

(二) 间接泄密

军事迷等相关主体经常聚集的各类军事网站是国(境)外情报机构重点关注的场域,军事迷等相关主体上传的图片、文字、视频、音频也可能成为国(境)外情报机构的情报来源。“内行看门道,外行看热闹”,军事迷等相关主体上传的关于军事单位、战略要地、武器装备、军事演习、军事训练、军事生活的图片、文字、视频、音频资料可能并不起眼,但在专业情报分析人员眼中,这些信息却可能具有极其重要的情报价值。例如,一张战斗机的座舱图片,一般人只是感觉高科技、复杂甚至凌乱,但专业情报分析人员却能够分析出战机航电的主要功能、制造工艺、基本性能等重要信息。

(三) 诱导性泄密

诱导性泄密分为线上和线下两种,本文主要关注线上诱导性泄密。包括:1. 卖萌型:境外情报人员注册军事网站或论坛账号,会装作菜鸟提出一些幼稚但有深度的问题,以激起一些专业人士好为人师的欲望,回应作答,导致泄密。2. 找打型:境外情报人员通过发布非常极端的主贴或评论,故意招惹,让专业人士拍砖,引出专业性分析。3.

自行打架吸引劝架者类型: 多名境外情报人员在网络空间上就一件武器性能、一个军事项目或一次军事活动进行非常激烈的争论, 并显露出明显的漏洞, 引诱相关专业人士介入劝架, 专业人士在专业劝导的过程中很容易泄密。4. 网络奖励: 境外情报人员利用网络货币、军衔荣誉、点击量、好评等方式引诱相关网友提供军事秘密信息。5. 网络造谣求辟谣: 利用网络发布军事信息谣言, 如此既可抹黑军队, 又能引诱专业人员和机构进行辟谣, 进而达到搜集情报的目的。通过综合分析, 相关主体被诱导而泄密的主要原因有: 好为人师; 追求虚荣; 兴趣使然; 为利而为; 爱国公心被利用。

五、如何应对网络时代军事信息泄密问题

随着网络的快速普及, 军事信息网络泄密正日益成为世界各国面临的一大难题。针对我国的实际情况, 或可采取以下措施: 一是网络实名制。特别是应该对军事网站和军事论坛实行网络实名制, 遏制境外情报人员非法注册涉及军事信息的网络账号; 二是网络军事信息战略欺骗。相关机构和人员通过主动发布或故意泄露一些虚假军事信息, 扰乱境外情报搜集机构或人员的视听, 造成其误判, 达到战略欺骗的目的; 三是不断完善网络防护技术。防火墙是建立于内、外网络边界上的过滤封锁机制, 内部网络被认为是安全、可靠的, 而外部网络则是不安全和不可信赖的(胡瑞卿, 2008: 1202-1203)。通过不断完善防护技术, 建立防御、跟踪、监控境外网络访问的强大技术体系, 遏止军事信息网络泄密态势的负向发展; 四是建立军事涉密信息分级保护机制。将军事涉密信息按照涉密程度分为绝密、机密、秘密等不同等级, 按照不同标准, 采取不同的

管理措施, 加强防护; 五是大力推广使用国产自主研发的软件。虽然国产并不意味着安全可靠, 但可以很大程度上解决国(境)外软件可能预留的后门或木马隐患问题, 增强信息安全能力; 六是进行保密宣传, 提高网民保密意识。通过大力宣传, 高频率提醒网民严格遵守保密法的有关规定, 发布军事相关信息时要自觉进行自我审查, 减少泄密几率; 七是加强立法, 从严治理。网络不是法外之地, 要通过立法明确军事网站及军事网络服务提供者的法律责任, 严格执法和监督, 充分保障军事信息网络泄密案件防范和查处工作的顺利开展。

习近平总书记在主持召开中央网络安全和信息化领导小组第一次会议时强调, 没有网络安全就没有国家安全, 没有信息化就没有现代化。军事信息安全是网络安全的重要组成部分, 也是国家安全的重要组成部分, 虽然网络滋生了涉及军事信息泄密的诸多新问题, 但这些问题可以通过发展与完善网络技术得到缓解或化解。为社会信息化建设与网络安全建设确立“两手都要抓, 两手都要硬”战略是我国的必然选择。

参考文献:

- 陈岸然. 2003-06-24. 关注军事信息安全[N]. 解放军报(4).
胡瑞卿, 田杰荣. 2008. 关于网络安全防护的几点思考[J]. 电脑知识与技术(16): 1202-1203.
李东风. 2006-07-11. 美国海军 10 万军人信息外流 网络军事泄密危害大[N]. 环球时报(3).
李治民. 2004-06-01. 军事泄密三例[N]. 光明日报(2).
汤巍. 2010-06-09. 防范网络泄密有新规[N]. 解放军报(6).
杨涛, 王小军. 2011-05-18. 这是一张不可触摸的网[N]. 解放军报(6).

Vague Boundary: Leakage of Military Intelligence in the Internet Age

Sun Lin

Abstract: In the Internet age, the spread of digitized information exceeds the limits of time, space and occupational fields. The strong connections of information provide a possibility for open intelligence gathering based on online search engines, among which military intelligence is of uppermost priority. With the development of mass-data and cloud-computation technologies, the boundary between public information and secret intelligence is becoming increasingly vague. The public leakage of information accompanying open intelligence gathering makes the security situation in cyberspace more complex.

Key words: Internet; military intelligence; leakage of intelligence; information security

(责任编辑: 许莲华)