第23话

电子信息战争

一切战争都是以欺骗为基础的……拿出诱饵来引诱敌人。装乱,压死他。

孙子

武力和欺诈是两种基本美德的交战。

- 托马斯·霍布斯

23.1 简介

几十年来,电子战与计算机安全是一个独立的主题,尽管它们使用一些通用技术。随着五角大楼开始将这两个学科的元素融合到信息战的新主题中,紧随其后的是俄罗斯和中国,这种情况在二十世纪的最后几年开始发生变化。2007 年俄罗斯对爱沙尼亚的拒绝服务攻击将其牢牢地列入了许多政策议程； Stuxnet 将其带入黄金时段;以及俄罗斯干预 2016 年的两大政治事件,即英国脱欧公投和美国大选,让立法者意识到这可能会让他们失去工作。

电子战的一些知识对安全工程师很重要还有其他原因。许多最初为战士开发的技术已被改编为商业用途,并且具有启发性的相似之处比比皆是。

为控制电磁频谱而进行的斗争是电子安全的第一个领域,它经历了攻击和防御的长期共同进化,涉及有能力的有动机的对手,从而产生了具有独特深度和微妙性的欺骗策略和战术。尽管这个主题在 1989 年冷战结束后变得冷淡,但最近随着中国努力成为美国的竞争对手,随着俄罗斯对其武装部队进行现代化改造,以及随着人工智能进入雷达、声纳和相关领域,它又重新兴起了系统。战争即将再次变得高科技,这与 2000-2020 年不同,它强调的是黑客入侵人们的电话和特种部队然后踢他们的门。

电子战也是我们学习拒绝服务攻击（计算机安全人员多年来忽视的一个话题）以及涉及直接因素和心理因素的混合攻击的第一位老师。最后，许多为击败敌方雷达而发展起来的技术，包括各种诱饵和干扰，在假新闻、巨魔农场和后现代宣传的新“信息战”世界中有着有趣的相似之处。

23.2 基础知识

老式的计算机安全是关于机密性、完整性和可用性的，而电子战则恰恰相反。优先事项是：

1. 拒绝服务，包括干扰、模仿和物理攻击；
2. 可能针对自动化系统或人的欺骗；和
3. 利用，不仅包括窃听，还包括从敌人使用其电子系统中获取任何有价值的作战信息。

在学说层面，电磁战通常被认为是
包括

- 电子攻击，例如干扰敌方通信或雷达，以及
  使用高功率微波干扰敌方设备；
- 电子保护，即在面对攻击时保留一些雷达和通信能力。它的范围从设计抗干扰系统，到加固设备以抵抗高功率微波攻击，再到使用反辐射导弹摧毁敌方干扰机；和
- 电子支持，提供必要的情报和威胁识别，以实现有效的攻击和保护。它允许指挥官搜索、识别和定位有意和无意的电磁能量源。

这些定义来自 Schleher [1662]。密码学的传统主题，即通信安全 (Comsec)，只是电子保护的一小部分，就像它只是现代民用系统中信息保护的一小部分一样。电子支持包括信号情报或 Sigint，它由通信情报 (Comint) 和电子情报 (Elint) 组成。前者收集敌方通信，包括消息内容和有关哪些单位正在通信的跟踪数据，而后者则关注识别敌方雷达和其他非通信电磁能源。

欺骗是电子攻击的核心。目标是通过操纵他们的感知来误导敌人，以降低他们情报和目标获取的准确性。它的有效使用取决于明确谁

（或什么)被欺骗,关于什么和多久,以及 如果欺骗的目标是人类 利用骄傲、贪婪、懒惰和其他恶习。欺骗可能具有极高的成本效益,并且与商业系统越来越相关。

物理破坏是其中的重要组成部分;虽然一些敌方传感器和通信链路可能会因干扰（所谓的软杀伤)而失效,但其他传感器和通信链路将被摧毁（所谓的硬杀伤）。成功的电子战取决于以协调的方式使用可用工具。

电子武器系统与其他武器一样,都有传感器,例如雷达、红外线和声纳;将传感器数据传送到指挥和控制中心的通信链路;以及干扰器、激光、导弹、炸弹等输出设备。我将首先讨论通信系统问题,因为它们是最独立的,然后是传感器和相关的干扰器,最后是电磁脉冲发生器等其他设备。一旦我们完成了电子战,我们将看看我们可能会接管信息战的课程。

23.3 通信系统

直到 1860 年左右,军事通信以物理调度为主,然后是电报直到 1915 年,然后是电话和无线电,直到冷战结束[1380]。如今,典型的指挥和控制结构由支持数据、语音和图像的各种战术和战略无线电网络组成,通过点对点链路和广播运行。也有固定链路,包括因特网和分类 IP 网络。如果没有态势感知和指挥部队的手段,指挥官很可能是无效的 。但保护通信安全的需求无处不在,威胁也多种多样。

- 一种明显的流量类型是固定站点（例如军队总部)与政治领导层之间的通信。这里的一个重大历史威胁是密码安全可能被渗透,命令、情况报告等受到损害,无论是作为密码分析的结果,还是 更有可能 设备破坏、人员颠覆或密钥材料被盗。在某些情况下,插入欺骗性消息也可能是一种威胁。密码安全可能包括防止 trac 分析（例如通过某些链接的恒定比特率加密)以及传输消息的机密性和真实性。次要威胁是链路可能被破坏,无论是由于电缆或中继站的破坏,还是由于资源共享的流量泛洪。

- 与现场特工等隐蔽资产的通信有更严格的要求。在这里,除了密码安全之外,位置安全也很重要。特工必须采取措施将因通信监控而被抓到的风险降至最低。如果他们使用敌人可以监视的媒体发送消息,例如互联网或

无线电,那么一些努力可能会进入令人沮丧的流量分析和无线电测向。

· 战术通信,例如总部与战地排之间的通信,也有更严格（但略有不同不同)的需求。无线电测向仍然是一个问题,但干扰可能至少同样重要,故意欺骗性消息也可能是一个问题。到 1980 年代,出现了一种设备,可以捕获敌方空中管制员的语音命令,将其切割成音素并拼接回欺骗性命令,以便在空战中获得战术优势 [730]。随着使用机器学习的深度伪造技术开发语音变形技术,对通信进行欺骗攻击的风险将会增加。因此,密码安全性可能越来越多地包括真实性以及机密性和隐蔽性。

· 控制和遥测通信,例如从飞机发送到其刚刚发射的导弹的信号,应该受到保护以防止干扰和修改。如果它们可以是隐蔽的（以免触发目标的警告接收器)也很好,但这与击败防御性干扰系统所需的功率水平存在紧张关系。一个常见的解决方案是使通信自适应 以低概率拦截模式启动 o ,但根据需要提高功率以响应干扰。

因此,根据具体情况,通信保护需要内容保密性、真实性、对流量分析和无线电测向的抵抗力,以及对各种干扰的抵抗力。它们以一些微妙的方式相互作用。例如,1980 年代初期为东欧持不同政见者组织设计的一台收音机在通常由美国之音和 BBC 世界服务占用的无线电波段中运行 这些波段经常被俄罗斯人干扰。这个想法是,除非俄罗斯人准备好关闭他们的干扰器,否则他们将不得不更加努力地寻找方向。

攻击通常还需要多种技术的组合 即使目标不是分析或测向而只是拒绝服务。

根据苏联的条令,对军事通信基础设施的全面而成功的攻击将包括物理摧毁其中的三分之一,通过干扰、木马或欺骗等技术阻止三分之一的有效使用,然后让对手能够通过尝试通过超过其安装容量的三分之一的所有流量来禁用剩余的三分之一 [1156]。这甚至适用于游击战争;在马来亚、肯尼亚和塞浦路斯,叛军成功地破坏了电话系统,足以迫使警察建立无线电网络 [1380]。

北约在 80 年代制定了类似的条令,称为反指挥、控制和通信作战（C-C3,发音为 CC 立方体）。

它在第一次海湾战争中实现了第一次开花。当然,攻击军队的指挥结构要古老得多;在向他的手下开枪之前先向他开枪是基本常识。

23.3.1 信号情报技术

在通信受到攻击之前,必须绘制出敌人的网络。
信号情报中最昂贵和最关键的任务是从无线电信号的杂音和电话网络和互联网等系统的大量流量中识别和提取有趣的材料。

在无线电信号的情况下,通信情报机构收集各种各样的信号类型,并建立广泛的数据库,以了解哪些电台或服务使用哪些频率以及如何使用。通常可以通过信号分析来识别单个设备。赠品可能包括任何无意的频率调制、发射器开启瞬态的形状、精确的中心频率和末级放大器谐波。这种 RF 指纹识别 (RFID) 技术在 1990 年代中期被解密,用于识别克隆手机 [776、1662]。它是第二次世界大战技术的直接后代,通过他的拳头识别无线电操作员 他使用摩尔斯电码的方式 [1224]。

无线电测向 (RDF) 也很重要。在过去,这涉及在两个监测站使用定向天线对感兴趣的信号进行三角测量。因此,间谍可能有几分钟的时间在不得不搬家之前向家里发送消息。现代监测站使用到达时间差 (TDOA) 通过比较两个站点接收到的信号的相位来准确、自动地定位可疑信号;如今,任何超过一秒左右的传输都可能是赠品。

Trac 分析 按来源和目的地查看消息数量 也可以提供非常有价值的信息。在第一次世界大战中,无线电信息量的大幅增加以及最近向五角大楼的比萨饼运送量的增加都预示着即将发生的袭击。然而,当在公共网络上筛选 trac 时,trac 分析真正发挥作用,其重要性(无论是出于国家情报还是警察目的)都很难被夸大。直到 1990 年代后期,trac 分析都是情报机构的领域 当 NSA 行动人员称自己为“狩猎采集者”时,trac 分析在很大程度上是“狩猎”。然而,在本世纪,trac 分析已经走出阴影,成为主要的研究课题。我在第 26.2.2 节的执法和情报监视的背景下讨论了这一点。

其中一项基本技术是滚雪球搜索。如果你怀疑爱丽丝从事间谍活动(或毒品交易,或其他),你会记下她打电话的每个人,以及每个打电话给她的人。这为您提供了数十名嫌疑人的名单。你排除了银行和医生之类的人,他们从太多人那里接到分析电话,然后对每个剩余的号码重复这个过程。递归地执行此过程两到三次后,您积累了数千个联系人 它们像滚下山坡的雪球一样累积。您现在筛选您收集的雪球 例如,筛选已经在您的黑名单中的人,以及筛选出现不止一次的电话号码。因此,如果 Bob、Camilla 和 Donald 是 Alice 的联系人,Bob 和 Camilla 与 Eve 有联系,Donald 和 Eve 与 Farquhar 有联系,那么所有这些人都可能被视为嫌疑人。您现在绘制一棵友谊树,它给出了爱丽丝网络的初步近似值,并通过将其与其他情报来源进行比较来完善它。 9/11 之后,隐蔽社区检测成为一个非常热门的话题,并且

研究人员尝试了各种层次聚类和图划分方法来解决这个问题。一种领先的算法是由 Mark Newman [1434] 提出的;它使用谱方法将网络划分为其自然社区,以最大限度地提高模块性。此类技术的标准参考文献是 Easley 和 Kleinberg [599]。

但即使有用于分析抽象网络的良好数学工具,现实也更加混乱。人们可以有多个号码,他们也可以共享号码。
当阴谋者采取积极的反制措施时,它会变得更加困难； Bob 可能会通过他的工作号码接到 Alice 的电话,然后从电话亭给 Eve 打电话。 （如果你管理着一个恐怖分子小组,你的信号员应该在牙医或医生或其他有太多活跃联系人而无法有效分析的地方找到一份工作 ）。此外,您还需要一些将电话号码与人相关联的方法。即使您可以访问电话公司的未列出号码数据库,预付费手机也可能是一个令人头疼的问题,被黑的 PBX 和 Signal 等加密消息服务也是如此。将 IP 地址绑定到人身上就更难了； ISP 并不总是长期保留 Radius 日志。我在其他地方更详细地讨论了所有这些问题,包括埃德斯诺登在第 2.2.1 节中揭露的美国国家安全局所做的事情和第 26.2.6 节中五眼联盟情报共享协议的历史。现在,我只想说匿名通信并不新鲜。世世代代都有信箱和公用电话亭。但它们并不是骗子的通用答案,因为正确使用匿名通信所需的纪律超出了大多数罪犯的范围。例如,据报道,其中一名所谓的 9/11 策划者在他在巴基斯坦的手机中使用一张预付费 SIM 卡后被捕,该预付费 SIM 卡是在瑞士购买的,与另一批次使用的 SIM 卡相同基地组织行动。

信号收集不仅限于让电话公司允许访问电话内容和明细帐单记录。它还涉及范围广泛的专门设施,正如埃德·斯诺登在 2013 年披露的那样并在第 2.2.1 节中进行了描述。甚至在此之前,由于调查记者的一系列泄密和工作,我们已经了解了大致情况。 Nicky Hager [849] 在 1996 年出版的一本书中描述了一个五眼收集网络。这被称为 Echelon,由许多固定的收集站组成,这些收集站使用称为字典的计算机监控电话、传真和数据流量,这些计算机在经过的流量中搜索有趣的电话号码、网络地址和机器可读内容;此 trac 选择是由情报分析员输入的搜索字符串驱动的。

在 Google 成立的两年前,Echelon 就已经是全球电话系统的 Google 了。斯诺登描述的 2013 年系统将其扩展到 IP 网络和当今更大的流量。它已经成为一个庞大的分布式搜索引擎,在全球拥有一百多个节点。摄取的流量首先要进行大量数据缩减 视频和广播文件被丢弃 然后内容会保留几天,以备不时之需。 Trac 数据也会保留,但会保留更长时间。

该固定网络根据需要辅以战术收集设施。
例如,海格描述了在 1980 年代军事政变期间派遣澳大利亚和新西兰海军护卫舰监视斐济国内通信的情况。Koch 和 Sperber 在 [1062] 中讨论了 1990 年代美国和德国在德国的设施； Fulghum 在 [730] 中描述了机载信号收集；

卫星也被用来收集信号,而且还有东道国不知道的秘密收集设施。例如,在第 2.2.1.9 节中,我描述了 Operation Socialist,其中 GCHQ 入侵了比利时电话公司以获取通过比利时路由的第三方移动电话流量以及布鲁塞尔欧盟机构的通信。

自斯诺登泄密以来,超过一半的 IP 流量已被加密,这已将情报和执法的重点在某种程度上转移到从端点收集信息。这就把我们带到了攻击的话题上。

23.3.2 对通信的攻击

一旦绘制了敌方网络图,您可能希望对其进行攻击。人们经常谈论“密码破译”,但这是一种过于简单化的说法。

首先,虽然一些系统已经被纯密码分析破解,但这种情况相当罕见。大多数生产攻击都针对设备或关键材料的供应或保管。例子包括第二次世界大战期间美国驻罗马大使的贴身男仆盗窃国务院密码本 [1001];一次一密的制造和分发错误导致对苏联外交踪迹的“Venona”攻击[1001];以及 CIA 和德国的 Bun desnachrichtendienst 对瑞士公司 Crypto AG 的秘密所有权,我将在第 26.2.7.1 节中讨论。埃德·斯诺登 (Ed Snowden) 披露了 GCHQ 从 Gemplus 窃取卡个性化文件的事件,Gemplus 承诺提供数百万张 SIM 卡中的密钥,使情报界能够访问数百万部手机的踪迹。即使发生了基于密码分析的攻击,操作错误也常常使攻击变得容易得多,例如第二次世界大战 [1002] 期间对德国 Enigma trac 的攻击,或对密码学的政治干预。这可以是公开的,如出口控制(参见第 4.3.1 和 26.2.9 节),也可以是微妙的,如随机数生成器(参见第 2.2.1.5 节)和 VPN(第 2.2.1.7 节)的标准。这些活动被这些机构称为“加密货币支持”,他们的预算高达九位数。其他国家玩类似的游戏:冷战期间苏联情报的历史表明,美国的技术优势在很大程度上被苏联“在 Sigint 支持中使用 Humint”的技能所抵消 招募出售关键材料的叛徒,例如沃克家族 [118]。最近,第 2.2.2 节描述了中国对云服务提供商和人事管理办公室等关键资产的攻击 这让他们获得了几乎所有美国政府雇员的许可数据文件。

其次,对内容的访问往往不是想要的结果。在战术情况下,目标通常是检测和摧毁节点,或堵塞交通。

干扰不仅涉及噪声插入,还涉及主动欺骗。在第二次世界大战中,盟军使用讲德语的人作为伪造的控制器向德国夜间战斗机发送令人困惑的指令,并且在发明和击败验证技术时发生了一场斗智斗勇。我在前面的一章中提到了情报部门和作战单位之间的紧张关系:前者想听取对方的情报,而后者则拒绝使用 [150]。这些目标之间很难找到折衷方案。堵塞您无法阅读的轨道是不够的,因为它告诉敌人您可以阅读什么!

如果对手使用密码学,事情就可以简化 尤其是当他们有能力并且你看不到他们的踪迹时。这消除了 ops/intel 的紧张关系,因此您可以适当地切换到 RDF 或破坏受保护的链接。这可能涉及挖掘电缆或轰炸电话交换机的硬杀伤方法(盟军在第一次海湾战争期间都这样做了)、干扰的软杀伤方法,或任何有效的组合 。干扰在链路短时间中断时很有用,但通常代价高昂;它不仅占用设施,而且干扰器本身也成为目标。它比物理攻击更有效的案例包括卫星链路,其中上行链路通常可以使用来自隐藏位置的紧密光束干扰,仅使用适度的功率。

越来越多地使用民用基础设施,尤其是互联网,提出了系统性拒绝服务攻击是否可用于干扰通信的问题。 (在波斯尼亚战争期间,有传言称塞尔维亚信息战小组试图对北约网站进行 DDoS 攻击。)这种威胁仍然被认为是真实存在的,以至于许多西方国家都有单独的内部网供政府和军方使用。

23.3.3 保护技术

因此,通信安全技术不仅涉及保护真实性和机密性,还涉及防止流量分析、测向、干扰和物理破坏。如果在链路层应用加密可以扩展到其中的第一个,因此所有链路上始终都有一个恒定速率的伪随机比特流。但是由于同步和干扰之间的权衡 ,链路层加密在无线电上很棘手;并且仅靠它本身并不总是足够的,因为敌人捕获单个节点可能会使整个网络处于危险之中。

仅靠加密无法防止 RDF、干扰以及链路或节点的破坏。为此,需要不同的技术。显而易见的解决方案是:

- 冗余专线或光纤;
- 高度定向的传输链路,例如使用红外激光的光学链路或使用高度定向天线和极高频率的微波链路;
- 低拦截概率 (LPI)、低定位概率 (LPPF) 和
  抗干扰无线电技术。

这些选项中的前两个非常简单,并且在可行的情况下它们通常是最好的。有线网络很难被完全摧毁,除非敌人知道电缆在哪里并且有物理途径来切断它们。即使遭到大规模炮击,斯大林格勒的电话网络在整个围城期间(双方)仍在使用。

第三个选项本身就是一个实质性的主题,我现在将(简要地)描述一下。

许多 LPI/LPPF/抗干扰技术属于扩频通信的通用名称。它们包括跳频、直接序列扩频 (DSSS) 和突发传输。从第二次世界大战前后开始,扩频催生了一个庞大的行业,该技术（尤其是 DSSS)已应用于许多其他问题,从高分辨率测距（在 GPS 系统中)到蓝牙等无线电协议。我将依次查看这三种方法中的每一种。

23.3.3.1 跳频

跳频器是最容易理解和实施的扩频系统。他们的工作正如他们的名字所暗示的那样 他们从一个频率快速跳到另一个频率,频率序列由授权委托人已知的伪随机序列确定。著名的是,它们是在 1940 年晚餐时由女演员海蒂·拉玛 (Hedy Lamarr) 和编剧乔治·安泰尔 (George Antheil) 发明的,他们将这项技术设计为一种控制鱼雷的方法,而不会被敌人发现或干扰其传输 [1702]。大约在同一时间,德国人独立研制了跳频雷达[1682]。

跳跃者可以抵抗不知道跳跃顺序的对手的干扰。如果跳跃很慢并且附近的对手拥有强大的设备,那么一个选择可能是跟随干扰 观察信号并在频段内跟随它,通常用单音干扰每个连续的频率。然而,如果跳频足够快,或者传播延迟过大,对手可能不得不阻塞大部分频段,这需要更多的功率。输入信号的带宽与传输信号的带宽之比称为系统的过程增益;因此,分布在 10MHz 上的 100 位/秒信号的处理增益为107/102 = 105 = 50dB。干扰余量定义为干扰功率与信号功率的最大容忍比,本质上是过程增益模实现和其他损失（严格来说,过程增益除以最小比特能量噪声密度比）。对于无法预测或有效遵循跳变序列的对手,最佳干扰策略是部分频带干扰 干扰足够的频带以在信号中引入不可接受的错误率。

跳频用于一些民用应用,例如蓝牙,它以低成本提供了不错的抗干扰水平。在军事方面,尽管漏斗可以提供较大的干扰余量,但它们几乎无法防止测向。扫过感兴趣频带的信号分析接收器通常会拦截它们（并且根据相关带宽、扫描速率和驻留时间,它可能会多次拦截跳频信号）。

由于跳频器易于实现并提供有用的抗干扰水平,因此它们通常用于战斗网络,例如单兵无线电,跳频率为每秒 50-500 次。为了破坏这些通信,敌人需要一个快速或强大的干扰机,这在战场上是不方便的。快速跳跃者（理论上定义为跳跃率超过比特率;在实践中,跳跃率为每秒 10,000 或更高)甚至可以超过大型干扰机的限制。与我将要介绍的技术相比,料斗的“LPI”更少

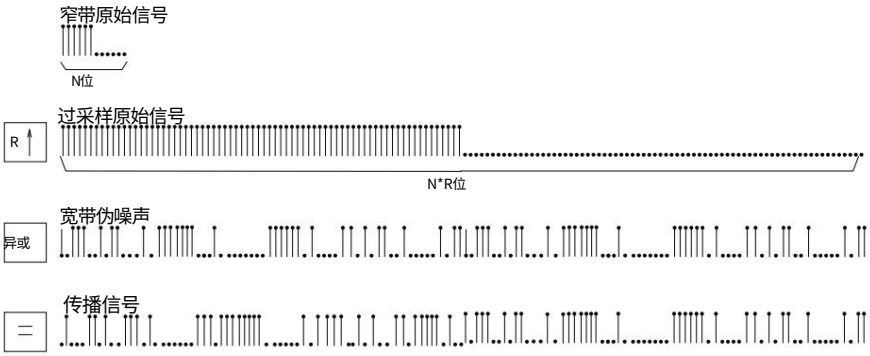

图 23.1：- 在 DSSS 中传播（由 Roche 和 Dugelay 提供）

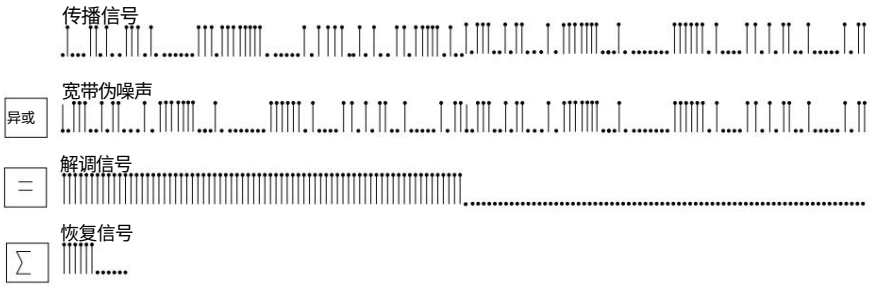

图 23.2：- 在 DSSS 中展开（由 Roche 和 Dugelay 提供）

接下来描述,作为具有扫描接收器的对手可以检测到信号的存在;慢速跳跃者在窃听和测向方面存在一定的脆弱性,因为拥有合适的宽带接收设备的对手通常可以跟踪信号。

23.3.3.2 DSSS

在直接序列扩频中,我们将信息承载序列乘以速率更高的伪随机序列,通常由某种流密码生成（见图 23.1 和 23.2）。这通过增加带宽来扩展频谱。该技术首先由瑞士工程师 Gustav Guanella 在 1938 年的专利申请 [1682] 中描述,并于 1950 年代在美国得到广泛发展。 1959 年,它在柏林的第一次愤怒部署。

与跳频一样,DSSS 可以提供可观的干扰余量（这两个系统具有相同的理论性能）。但它也可以使信号明显更难拦截。诀窍是安排事物,以便在拦截位置,信号强度非常低,以至于它在本底噪声中丢失,除非对手知道用于恢复它的扩展序列。当然,同时做到这两点比较困难,因为抗干扰信号应该是高功率而 LPI/LPPF 信号应该是低功率;通常的策略是在 LPI 模式下工作,直到被敌人检测到（例如,当进入雷达范围内时）,然后将发射机功率提高到抗干扰模式。

有大量关于 DSSS 的文献,该技术现在已被商业界采用,例如各种移动无线电和电话系统中的码分多址 (CDMA)。

DSSS 有时被称为“加密 RF”,它有多种变体。例如,当基础调制方案是 FM 而不是 AM 时,它被称为线性调频。底层数学和技术的经典介绍是[1525];由于各种原因,工程复杂性高于跳频。例如,同步尤为关键。一种策略是让您的用户轮流提供参考信号。如果您的用户可以访问参考时间信号(例如 GPS 或原子钟),您可能会依赖于此;但是如果你不控制 GPS,你可能会受到同步攻击,即使你控制了 GPS 信号也可能会被干扰。据报道,2000 年法国人干扰了希腊的 GPS,企图破坏英国向希腊政府出售 250 辆坦克的投标,而法国是该交易的竞争对手。这导致英国坦克在试验中迷路了。当诡计被发现时,希腊人发现这一切都很有趣 [1918]。现在 GPS 干扰器是商品,我将在本章后面更详细地讨论它们。

23.3.3.3 突发通信

顾名思义,突发通信涉及压缩数据并在敌人无法预测的时间以短突发传输数据。它们也被称为时间跳跃。它们通常不那么抗干扰(除非更高的数据速率扩展了频谱),但比 DSSS 更难检测;如果占空比很低,扫描接收器很容易错过它们。它们通常用于特种部队和情报人员的无线电中。

真正高档的房间虫子经常用爆破。

一个有趣的变体是流星爆发传输(也称为流星散射)。这依赖于每天撞击地球大气层的数十亿颗微陨石,每一颗都留下一条长长的电离轨迹,通常持续三分之一秒,并在母站和大约一百英里长的区域之间提供一条临时传输路径和几英里宽。母站连续发射;每当其中一个女儿在这样的区域内时,它就会听到妈妈的声音并开始高速发送数据包,妈妈会回复。在秘密行动中使用低功率电平,可以实现约 50 bps 的平均数据速率,平均延迟约 5 分钟,范围为 500-1500 英里。流星爆发通信被特种部队使用,也用于民用应用,例如监测第三世界偏远地区的降雨量。随着更高的功率水平和更高的纬度,平均数据速率可以上升到每秒几十千比特,阿拉斯加的美国空军使用这样的系统作为预警雷达的备用通信。在可以容忍低比特率和高延迟但设备尺寸和成本很重要的利基市场中,流星散射很难被击败。 [1661] 中描述了该技术。

23.3.3.4 结合隐蔽性和抗干扰性

在不同的 LPI、LPPF 和抗干扰特性,以及其他性能方面（例如抗衰落和多径以及可同时容纳的用户数量)之间存在一些相当复杂的权衡。它们在面对扫频干扰（干扰机重复扫描目标频段)和跟随器等专门干扰技术时也表现不同。某些类型的干扰在不同模式之间转换:例如,对手的功率不足以完全阻止信号,可以通过发射覆盖其使用的部分频谱的脉冲来对 DSSS 进行部分时间干扰,就像部分频带干扰一样的跳频。

还有工程权衡 。例如,就功率而言,DSSS 往往是跳频的两倍左右,但对于给定的设备复杂性,跳频提供了更多的干扰余量。另一方面,使用测向技术 [673] 很难定位 DSSS 信号。

系统生存能力要求可以施加进一步的限制。防止捕获一台无线电并提取其当前密钥材料的对手使用它来干扰整个网络可能是必不可少的。因此,典型的军事系统将使用紧束、DSSS、跳频和突发的某种组合。

- DSSS 和跳频都在链路 16 中与 TDMA 一起使用,这在北约是众所周知的;美军也将其称为战术数字信息链路 (TADIL),之前称为联合战术信息分发系统 (JTIDS) [1662]。 TDMA 将传输与接收分开,并让用户知道何时需要他们的时隙。它的 DSSS 信号具有 57.6KHz 的数据速率和 10MHz 的码片速率（因此干扰裕度为 36.5dB）,它在 255MHz 的频段内跳跃,最小跳跃为 30MHz。跳码适用于所有用户,而扩展码仅限于个别电路。理由是,如果设备捕获导致扩展码受损,这将只允许干扰单个 10MHz 频段,而不是整个 255MHz。开发始于 1967 年,戈登·韦尔奇曼 (Gordon Welchman) 也在第二次世界大战期间在布莱切利 (Bletchley) 破译了德国密码;在 1970 年代的试点项目之后,在 1980 年代开始认真发展,该系统从 2000 年左右开始全面部署,在阿富汗和伊拉克得到使用 [1956]。

- 美国武装部队得到了一系列卫星通信系统（MILSTAR 和DSCS)的支持,这些系统具有来自地球静止轨道的1 度波束。窄波束的效果是用户可以在距离敌人三英里的范围内操作而不被发现。干扰保护来自跳频:它的信道在 2GHz 的频带中每秒跳频数千次。

- 法国战术无线电有遥控器。士兵可以用手
  距离收音机一百码。这意味着对高功率发射器的攻击不必对部队造成如此大的危害 [514]。

还有一些系统级的技巧,比如干扰消除 你在一个你用你自己的无线电已知的波形干扰的频段中通信,这样他们就可以消除它或绕过它。这可以迫使敌人将可用功率分散到更大的带宽上,从而使敌人的干扰变得更加困难,并且也可以使信号情报变得更加困难 [1601]。

23.3.4 民用和军用之间的相互作用

民用和军用通信日益交织在一起。沙漠风暴行动(针对伊拉克的第一次海湾战争)广泛利用了海湾国家的民用基础设施:利用卫星、无线电链路和租用线路以及来自美国各军种的专家在短时间内创建了一个庞大的战术通信网络声称通信能力对战争的影响是决定性的 [942]。

相互依存度增加的另一个例子是全球定位系统 GPS。这开始于 o 作为美国军用导航系统,并具有选择性可用性功能,除非用户拥有相关的加密密钥,否则将精度限制在大约 100 码。在第一次海湾战争期间,由于没有足够的军用 GPS 设备,不得不使用民用设备,因此必须关闭它。随着时间的推移,事实证明 GPS 在民用航空中非常有用,以至于美国联邦航空局帮助找到了克服选择性可用性的方法,并提供了大约 3 码的精度,而标准军用接收器声称的精度为 8 码 [630]。最后,在 2000 年 5 月,克林顿总统宣布结束选择性可用性。

美国政府仍然保留关闭 GPS 或引入错误的权利,例如,如果恐怖分子被认为正在使用它。但现在有如此多的不同系统依赖于 GPS,从谷歌地图到优步,负责任的政府不太可能这样做。然而,有许多应用程序有动机的对手。正如我在第 14.4 节中讨论的那样,一些国家/地区使用 GPS 进行道路收费,或通过电子脚踝标签对释放的囚犯执行假释条款。因此,GPS 干扰器在 2007 年以 700 美元的价格出现在汽车杂志上,现在成本不到 100 美元;它们被卡车司机用来欺骗道路收费系统,公司的汽车司机想要阻止他们的老板知道他们要去哪里,以及偷车贼。廉价设备的射程较短,通常为 5-10 米。

GPS 欺骗需要更多的工作。一个例子是 meaconing,您在位置 A 对信号进行采样并在位置 B 重新传输它们(这也称为虫洞攻击)。结果是 B 附近的任何人都认为他们在 A 附近。这被用作一些政府首脑的豪华轿车的防御机制(老练的刺客可以用它来瞄准导弹)。一些国家进行系统的 GPS 干扰,例如俄罗斯与挪威的边界。可以使用差分 GPS 在很大程度上检测欺骗,您可以在已知位置使用另一个接收器作为参考点(FAA 的技巧),也可以使用干涉 GPS(也称为 S-GPS)使用连续捕获的信号同一接收器的读数以产生合成孔径。这也增加了灵敏度并处理城市峡谷中的多径问题,这是大误差的主要来源

现有设备 1.

除了美国的 GPS 系统,俄罗斯、中国和欧洲都有使用相同原理的独立导航卫星系统;这些系统统称为 GNSS。

23.4 监视和目标获取

电子战中与目标获取和武器制导有关的那些方面是干扰和欺骗技术得到最高度发展的地方。（事实上,尽管公开文献中关于电子攻击和防御在雷达上的应用比在通信上的应用要多得多,但很多相同的科学都适用于两者。）

用于探测敌对目标并将武器引导至目标的主要方法是声纳、雷达和红外线。第一个被开发的是声纳,它是在第一次世界大战中发明和部署的（以“Asdic”的名义）,并且仍然主导着潜艇战争 [846]。在其他地方,关键传感器是雷达。

虽然它是作为海上防撞装置于 1904 年发明的,但其真正的发展只发生在 1930 年代,并被第二次世界大战的所有主要参与者使用 [855, 990]。为它开发的电子攻击和保护技术往往比使用其他传感器的系统发展得更好,而且经常会转向使用其他传感器的系统。

23.4.1 雷达类型

广泛部署的系统包括搜索雷达、火控雷达、地形跟踪雷达、反轰击雷达和气象雷达。它们具有各种各样的信号特性。例如,具有低 RF 和低脉冲重复频率 (PRF) 的雷达更适合搜索,而高频、高 PRF 设备更适合跟踪。关于该技术的经典教科书是 Schleher [1662]。

用于搜索应用的早期雷达设计可能有一个旋转天线,它会发射一系列脉冲并检测回波。在数字电子技术出现之前,显像管中的扫描可以与天线同步机械旋转。火控雷达通常使用锥形扫描:光束将在目标位置周围的一个圆圈中进行跟踪,返回的幅度可以直接驱动定位伺服系统（和武器控制）。现在,波束是使用多个天线元件以电子方式生成的,但跟踪环路仍处于中心位置。许多雷达都有一个距离门电路,该电路专注于距天线一定距离范围内的目标;如果雷达必须跟踪（比如说）0 到 100 英里之间的所有物体,那么它的脉冲重复频率将受到无线电波传播 200 英里所需时间的限制。

这通常会对角分辨率和跟踪性能产生影响。

1全面披露:开发 S-GPS 的公司 Focal Point Positioning 是由我的一位博士后创办的,我是该公司的投资者。

多普勒雷达通过返回信号的频率变化来测量目标的速度。这对于区分移动目标和杂波（从地面反射的回波）非常重要。多普勒雷达可能有速度闸门，将注意力限制在相对于天线的径向速度在一定限度内的目标上。

非军事应用中门控的一个例子是汽车中的自适应巡航控制。这使用雷达，门控忽略相对速度太大的车辆（因此它不会对迎面而来的车辆感到恐慌）以及太近或太远的车辆。您可能会注意到，如果另一辆车在您前方靠近，距离不到 20 米，您的巡航控制不会注意到它，也不会减速。

23.4.2 干扰技术

电子攻击可以是被动的也可以是主动的。

最早被广泛使用的反制措施是 cha – 将导电箔的细条切成目标信号波长的一半，然后散开以提供错误返回。第二次世界大战快结束时，盟军飞机每天投放 2000 吨的弹药以削弱德国的防空能力。 Cha 可以由试图穿透防御系统的飞机直接投掷（这并不理想，因为它们将处于拉长信号的顶点），或者由支援飞机投掷，或者使用火箭或炮弹向前发射到合适的模式。针对 cha 的主要反制措施是多普勒：由于 cha 非常轻，它几乎立即停止，并且可以很容易地与移动目标区分开来。

其他技术包括带有主动中继器的小型诱饵，可以重新传输雷达信号，以及较大的诱饵，可以简单地反射雷达信号；有时，一辆车（如直升机）充当另一辆更有价值的车（如航空母舰）的诱饵。这些原则是很普遍的。使用无线电测向 (RDF) 追踪目标的武器被发射射频信号的特殊无人机诱骗，而红外制导导弹则使用照明弹转移。

投入最多资金的被动对抗措施是隐身 减少车辆的雷达横截面 (RCS)，使其只能在非常短的距离内被检测到。这迫使敌人将他们的防空雷达靠得更近，所以他们不得不购买更多的雷达。Stealth 包括范围广泛的技术，适当的讨论远远超出了本书的范围。有些人认为它是“极其昂贵的黑漆”，但它的意义远不止于此。由于飞机的 RCS 通常是其方位角的函数，因此它可能有一个电传飞行系统，该系统会持续显示低 RCS 方位角以识别敌方发射器（F117 被其飞行员称为“摇摇晃晃的妖精”）。

积极的反制措施更加多样化。早期的干扰机只是在目标雷达使用的频率范围内产生大量噪声。这被称为噪声干扰或弹幕干扰。一些系统使用系统频率模式，例如脉冲干扰器或横穿感兴趣频率范围的扫描干扰器（也称为 squidging 振荡器）。但是这样的

一个信号相当容易被阻塞 一个技巧是使用一个保护带接收器,一个频率与正在使用的接收器相邻的接收器,并在该接收器接收到干扰信号时消隐信号。干扰不仅限于一侧;除了被目标使用外,雷达本身还可以从辅助天线发送杂散信号以掩盖真实信号或简单地使防御系统过载。

天平的另一端是硬杀伤技术,例如反辐射导弹 (ARM),通常由支援飞机发射,它们会追踪敌方信号。防御此类武器的方法包括使用诱饵发射器、闪烁发射器开启和关闭 ,以及无源雷达 它们利用现有发射器 (如电视和广播电台)弹回目标时发出的信号。

中间是一个大型的欺骗干扰技术工具包。大多数用于自我保护的干扰器都是一种或另一种欺骗性干扰器。弹幕和 ARM 技术往往更适合支援车辆使用。

自我保护干扰机的通常目标是拒绝向攻击者提供射程和方位信息。基本技巧是反向增益干扰或反向增益幅度调制。这是基于攻击者天线的方向性通常并不完美的观察;除了主波束,它还有旁瓣,通过旁瓣也可以传输和接收能量,尽管效率要低得多。旁瓣响应可以通过观察发射信号来映射,并且可以生成干扰信号,使得净发射是天线方向响应的倒数。就攻击者的雷达而言,效果是信号似乎无处不在;在雷达屏幕上,您看到的不是一个“光点”,而是一个以您自己的天线为中心的圆圈。

反向增益干扰对较旧的锥形扫描火控系统非常有效。

更一般地,该技术是通过延迟和/或频率的系统变化来重新传输雷达信号。这可以是非相干的,在这种情况下,干扰机称为转发器,或者是相干的 即具有正确的波形 当它是中继器时。现代设备将接收到的波形存储在数字射频存储器 (DRFM) 中,并使用信号处理来操纵它们。

一个基本的对策是烧穿。通过降低脉冲重复频率,驻留时间会增加,因此返回信号会更强但精度会降低。更复杂的对策是距离门拉动 (RGPO)。在这里,干扰机发射许多比真实脉冲更强的假脉冲,从而捕获接收器,然后将它们移出相位,使目标不再位于接收器的距离门内。类似地,多普勒雷达的基本技巧是速度门拉动 (VGPO)。对于较旧的雷达,成功的 RGPO 会导致雷达解锁并且目标从屏幕上消失。现代雷达可以非常快速地重新获取锁定,因此 RGPO 必须重复执行或与另一种技术结合使用 通常是使用反向增益干扰来同时中断角度跟踪。

一个基本的反对策是抖动脉冲重复频率。每个传出脉冲要么延迟,要么不延迟,具体取决于延迟 se

由随机数生成器生成的序列,因此干扰机无法预测下一个脉冲何时到达并且必须跟随它。这样的跟随干扰只能制造看起来更远的虚假目标。所以反反制,或（反）三措施,是让雷达有一个前沿跟踪器,它只响应第一个返回脉冲;并且（反）4 措施可以包括以如此高的功率进行干扰,以捕获接收器的自动增益控制电路。另一种方法是覆盖干扰,其中干扰脉冲足够长以覆盖最大抖动周期。

螺丝的下一个转折点可能涉及战术。 Cha 通常用于强制雷达进入多普勒模式,这使得 PRF 抖动变得困难（因为对于多普勒来说,连续波形比脉冲更好）,而前沿跟踪器可以与频率捷变和智能信号处理相结合。例如,真实的目标返回波动,并具有真实的加速度,而简单的转发器和中继器发出或多或少稳定的信号。当然,设计师总是有可能太聪明； Mig-29 可以通过快速拉升在水平飞行中减速得比一些雷达设计师预期的要快,因此飞行员可以使用这种机动来打破雷达锁定。现在 CPU 的功能强大到足以制造真实的错误回报。

23.4.3 先进雷达和对抗措施

许多先进的技术被用来抵御干扰。

脉冲压缩是在第二次世界大战期间首先在德国开发的,它使用一种直接序列扩频脉冲,在返回时通过匹配滤波器进行滤波以再次压缩它。这可以提供 10–1000 的处理增益。脉冲压缩雷达可以抵抗转发器干扰,但容易受到中继器干扰,尤其是那些具有数字射频存储器的雷达。但是,如果您不希望目标在您检测到它之前很久就检测到您,那么使用 LPI 波形很重要。

脉冲多普勒与多普勒非常相似,发送一系列相位稳定的脉冲。它已经主宰了许多高端市场,并被广泛用于,例如,用于防空低空入侵者的俯视击落系统。与基本脉冲跟踪雷达一样,不同的 RF 和脉冲重复频率具有不同的特性:我们需要低频/PRF 以获得明确的距离/速度并减少杂波 但这会留下许多盲点。必须应对许多威胁的机载雷达使用高 PRF,并且只寻找超过某个阈值的速度,比如 100 节 但在追尾方面很弱。通常的折衷方案是中等 PRF 但这会受到机载操作中严重的距离模糊的影响。此外,搜索雷达需要长而多样的脉冲串,而跟踪只需要短而调谐的脉冲串。一个优势是脉冲多普勒可以区分一些非常具体的信号,例如喷气发动机中涡轮叶片提供的调制。用于对抗脉冲多普勒的主要欺骗策略是速度门 pull-o ,尽管现代变体是用欺骗性回报激发多个速度门。

单脉冲成为最流行的技术之一。例如,它被用于事实证明很难在福克兰群岛干扰的飞鱼导弹

战争。这个想法是有四个链接的天线,以便可以使用干涉测量技术从每个返回脉冲计算方位角和仰角数据。
除非可以利用设计缺陷,否则单脉冲雷达难以干扰且成本高昂;通常的技术包括编队干扰和地形弹跳等技巧。通常首选的防御策略只是使用拖曳诱饵。

一种强大的技巧是被动相干定位。洛克希德的“Silent Sentry”系统根本没有发射器,而是使用商业无线电和电视广播信号的反射来检测和跟踪空中物体[164]。接收器是被动的,很难定位和攻击;摧毁该系统需要摧毁主要的民用基础设施,出于法律和宣传的原因,反对者往往不愿这样做。被动相干定位可有效对抗某些类型的隐身技术,尤其是那些需要操纵飞机的隐身技术,以便将其雷达横截面中的零位呈现给可见发射器。被动定位实际上可以追溯到 1930 年代的雷达先驱 Robert Watson-Watt,并且似乎从 1942 年开始被德国人首次使用,当时他们的 Klein Heidelberg 站利用英国 Chain Home 雷达信号跟踪英国皇家空军的飞机(用 EW 的说法,这是一个“搭便车的人”)。

当英国在 1944 年意识到这正在发生时,Chain Home 信号开始紧张 [824]。

2020 年的一个研究前沿是认知雷达。自数字射频存储器和其他软件无线电技术问世以来,攻击和防御变得更加复杂。雷达和干扰机波形都可以比以前更灵活地适应战术情况。西蒙·海金 (Simon Haykin) 及其同事研究了蝙蝠使用的战略和战术,蝙蝠在捕食昆虫时会智能地调整声纳,并首先将其应用于无线电以有效利用频谱,然后在 2006 年的一篇开创性论文 [872] 中将其应用于雷达。从雷达(或声纳)开启的那一刻起,它就开始了解其环境,其中有趣的方面大多是动态的。基本思想是认知雷达对其环境模型进行递归更新,并使用学习机制对其进行智能照明。这与非合作目标变得敌对。现在对人类视觉系统和更普遍的神经网络、贝叶斯目标跟踪和信号处理的思想融合进行了积极的研究。

23.4.4 其他传感器和多传感器问题

我所说的关于雷达的大部分内容也适用于声纳,还有相当一部分适用于红外线。被动诱饵 照明弹 对早期使用机械旋转探测器的热跟踪导弹非常有效,但对包含信号处理的现代探测器效果较差。耀斑就像 cha ,因为它们相对于目标迅速减速,因此攻击者可以过滤速度或加速度。它们也像中继干扰机,因为与真实目标相比,它们的信号相对较强且稳定。

主动红外干扰不如雷达干扰广泛,因为它更难;它倾向于通过以引起混淆的速率或模式发出脉冲来利用敌对传感器的功能。一些红外防御系统开始使用激光来禁用来袭武器的传感器;它出现了

许多“不明飞行物”目击事件实际上是由于各种干扰（雷达和红外)[175]。

一个增长领域是多传感器数据融合,来自雷达、红外传感器、摄像机甚至人类的输入被组合起来,以提供比单独任何一个都更好的目标识别和跟踪。例如,Rapier 防空导弹使用雷达获取方位角,同时在视觉条件下进行光学跟踪。数据融合可能比看起来更难。正如我在 17.8 节中讨论的那样,结合两个警报系统通常会导致误报率或漏报率提高,同时使另一个更糟。如果你在雷达或红外线中看到一个光点时紧急起飞你的战斗机,你就会有更多的误报;但是,如果您仅在看到两者时才进行争夺,那么敌人将更容易干扰您或偷偷溜走。

如果攻击者位于容易受到反击的平台（例如船只或飞机)上,事情就会变得更加复杂。它将拥有威胁识别、测向和导弹接近警告系统,其接收器将被其干扰器震聋。通常的技巧是在随机时间关闭干扰器进行短暂的“透视”。

有了多个友好和敌对的平台,事情变得更加复杂。
冷战期间,你期望双方都有配备大功率专用设备的专业支援车辆,这在某种程度上使之成为一场能源战 “瓦数多者胜”。 SAM 腰带将有多个不同频率的雷达,以增加干扰难度。干扰（隐身)的总体效果是减少雷达的有效范围。但干扰余量也很重要,谁拥有最多的车辆,以及采用的战术;向认知系统的转变改变了条令,以“巧妙地破坏敌人的通信和雷达网络,而他们没有意识到自己被欺骗了”[721]。

23.5 敌我识别系统

在多辆车交战的情况下,还需要有一种可靠的方式来区分敌友。敌我识别 (IFF) 系统既重要又具有争议性,伊拉克发生的大量“蓝对蓝”事件是由于美国和盟军之间的设备不兼容造成的。

美国飞机轰炸英国士兵的事件极大地导致了英国公众对这场战争的支持的丧失,尤其是在两国当局出于既维护技术安全又尽量减少破坏的希望而试图掩盖此类事件但未能成功之后。政治尴尬。

IFF 以其非技术形式追溯到古代。例如,参见士师记 12:5-6（我在生物识别学一章的开头引用）：以色列人通过无法发音“Shibboleth”来识别敌方士兵。第二次世界大战见证了法国的抵抗运动,要求人们发音为“grenouille”,任何不会发音的人都被假定为德国人。在那场冲突的早期,空中身份识别是程序性的:盟军轰炸机预计会在特定时间和地点飞越海岸,而掉队者会宣布他们

预先安排的机动没有敌意,例如在穿越海岸之前飞行等边三角形。当无线电操作员挑战德国飞机时,它们会翻滚,从而在它们的雷达横截面中产生一个“光点”。

然后有一些早期的自动化尝试:当盟军飞机开始携带敌我识别信标时,德国防空发现他们可以通过触发它们来检测飞机 [824]。

朝鲜战争见证了双方喷气式飞机和导弹的到来,这使得目视识别目标变得不切实际。早期的敌我识别系统只使用一个序列号或“每日代码”,但这很容易受到欺骗,因此世界各国的空军开始着手进行密码验证。

北约遗留系统是 Mark XII,于 1960 年代推出,旨在解决第 4.3.3 节中讨论的协议问题。Mark XII 安全模式使用 32 位质询和 4 位响应。如果挑战或响应太长,则雷达的脉冲重复频率(及其精度)会降低。它连续发送 12-20 个挑战,在最初的实现中,响应显示在屏幕上的位置由实际响应和预期响应之间的算术差异 偏移。效果是,当敌人的反应为空或随机时,“朋友”的反应会聚集在中央屏幕附近,屏幕会亮起。反射攻击被阻止,MIG-in-the-middle 攻击变得更加困难,因为挑战使用聚焦天线,而接收器是全向的。 (用于挑战的天线通常是火控雷达,在旧系统中它是圆锥形扫描的。)

这在很大程度上已被具有向后兼容模式的 Mark XIIA 所取代,但在新的模式 5 中使用扩频波形,这一直是 2010 年代美国军种和北约武装部队发展努力的重点。此类系统还具有与民用飞机使用的系统兼容的模式,可将其 ID ‘叫’到二次监视雷达。然而,现在真正的问题是空对地。北约的敌我识别系统是为铁幕两侧数千架战术飞机的冷战情景而发展的;他们在伊拉克或阿富汗这样的现代冲突中表现如何?

从历史上看,大约 10-15% 的伤亡是由于“误伤”造成的,但在第一次海湾战争中,这一比例上升到 25%。由于各军种的做事方式不同,此类伤亡更有可能发生在空战和陆战交界处;因此,联合行动特别危险。

由于不同的国家系统,联合行动也增加了风险。
根据这一经验,开发了几个实验系统以将 IFF 扩展到地面部队。但是当第二次海湾战争出现时,并没有部署任何像样的东西。英国国家审计署的一份报告描述了问题所在 [1389]。在这样一个世界里,国防不仅由民族国家购买,也不仅仅是由军种购买,而且由这些军种中的派系购买,立法者试图通过阻止与盟国的技术合作来向受教育程度较低的选民表明他们的“爱国主义”(“为了阻止他们窃取我们的工作和我们的秘密”),体制和政治结构不利于提供国防“公共产品”,例如可以在整个北约运作的体面的敌我识别系统。北约是一个广泛的联盟;正如一位内部人士告诉我的那样,“试图制定一种解决方案,既满足美国的一个极端愿望,又满足希腊(例如)另一个极端的愿望,这是一项近乎无望的任务。”

项目的复杂性是一个问题:阻止你的空军飞机互相射击并不难,阻止它们向你的船只或坦克射击要复杂得多,而且当涉及十几个国家时更难。伊拉克的少数部队使用了一些性感的系统,让所有士兵看到彼此的位置实时叠加在头盔上的单片眼镜上的地图显示上。它们极大地提高了运动战中的部队能力,使部队能够执行危险的机动,例如驶过彼此的杀伤区,但并不是 2000 年代末和 2010 年代初伊拉克等复杂战争中的灵丹妙药:在那里,关键网络是社交网络,不是电子的,并且很难使具有未知可信度节点的网络自动化 [1659]。

尝试过大爆炸方法,但失败了;联合战术无线电系统（JTRS,发音为“抖动”)着手为所有美国军种配备可互操作并至少执行两种敌我识别模式的无线电。然而,这是五角大楼最大的采购失败案例之一,因为他们在 15 年内花费了 60 亿美元,却没有交付一台可用的无线电设备 [1983 年]。

经验告诉我们,即使是“硬核”敌我识别,即舰船和飞机相互识别,最困难的问题也不是技术问题,而是经济、政治和学说方面的问题。北约内部经过二十多年的争论,美国想要一个昂贵的高科技系统,其国防工业正在努力游说,而欧洲国家想要更简单、更便宜的东西,他们也可以自己建造,例如通过正常指挥跟踪单位-和控制系统,并在国家之间拥有良好的接口。但出于“安全”原因,美国拒绝向任何其他人透露其单位的位置。美国在国防上的支出超过其盟友的总和,并认为它应该领先;盟国不希望自己的能力因更加依赖美国供应商而进一步边缘化。

潜在的教义紧张加剧了这一点。美国学说,由唐纳德·拉姆斯菲尔德 (Donald Rumsfeld) 提倡并基于电子系统系统的“军事航空革命”(RMA),不仅超出了盟国的预算,而且不受信任,因为它基于最小化自己的预算巨大的材料和技术霸权造成人员伤亡。欧洲人争辩说,人们不应该通过轰炸村庄来自动对村庄的狙击火力做出反应;除了杀死 10 名叛乱分子,您还杀死了 100 名平民,并将他们的数百名亲属招募到另一方。美国人对此的反驳是,欧洲太虚弱且分裂,甚至无法应对波斯尼亚的种族灭绝。结果陷入僵局;各国决定寻求国家解决方案,自冷战以来在互操作性方面没有取得真正进展。驻扎在伊拉克和阿富汗的盟军只好在车辆的车顶上涂上大片彩色补丁,并希望空袭能够绕过他们。美国飞机适时轰炸并杀死了一些盟军军人,削弱了联盟。鉴于去全球化和特朗普总统对外国盟友的不耐烦,现在会发生什么是任何人的猜测。

23.6 简易爆炸装置

在电子战措施方面做出了重大努力,以对抗简易爆炸装置 (IED),这是叛乱分子选择的武器

伊拉克和阿富汗。第一次针对美军的简易爆炸装置袭击发生在 2003 年 3 月,2007 年达到 25,000 次的峰值,总数超过 100,000 次。
这些炸弹成为伊拉克战争的“标志性武器”,就像第一次世界大战的机枪和第一次海湾战争的激光制导炸弹一样。现在,业余爱好者可以用不到 1000 美元的价格制造无人驾驶飞行器,我们开始看到在叙利亚和其他地方使用简易巡航导弹,包括企图暗杀委内瑞拉总统马杜罗。

无论如何,制造了超过 33,000 台干扰机并运送给了联军。
2006 年,国防部在他们身上花费了超过 10 亿美元,据内部人士称,这项行动“证明是国防部在战争中面临的最大技术挑战,其规模是第二次世界大战的最后一次经历”[140]。其效果是无线电控制的 IED 的比例从 70% 下降到 10%,而由指令线触发的比例增加到 40%。

至少自盖伊·福克斯 (Guy Fawkes) 以来,叛军一直在制造简易爆炸装置,他在 1605 年试图炸毁英格兰议会大厦。许多其他民族主义和叛乱团体都使用过简易爆炸装置,从无政府主义者到第二次世界大战中的俄罗斯抵抗运动、伊尔贡、埃塔和越共对爱尔兰民族主义者。爱尔兰共和军非常擅长将简易爆炸装置隐藏在排水沟和涵洞中,以至于在 1980 年代和 1990 年代初期,英国军队不得不在爱尔兰边境附近的“强盗国家”使用直升机而不是公路车辆。在二十世纪,他们还多次对英国进行轰炸。在最后一次事件中,从 1970 年到 94 年,他们炸毁了布莱顿的大酒店,当时玛格丽特·撒切尔 (Margaret Thatcher) 正在那里参加一个党派会议,炸死了她的几位同事;后来,伦敦发生了两起事件,其中 IRA 提供了卡车装载的自制炸药,造成了广泛的破坏。与 IRA 的战斗总共涉及大约 7,000 个简易爆炸装置,并为英国国防科学家提供了很多干扰经验:弹幕干扰器安装在贵宾车上,这会导致简易爆炸装置过早或过晚熄火。这些已提供给盟友； 2005 年基地组织试图炸毁巴基斯坦总统穆沙拉夫的车队时,这种干扰器救了他一命。

事实证明,伊拉克的电子环境比贝尔法斯特或巴基斯坦要复杂得多。轰炸机可以使用任何可以在远处翻转开关的设备,并且可以使用从遥控钥匙到手机的所有设备。与此同时,伊拉克的射频环境变得复杂而混乱。数百万伊拉克人使用不受管制的手机、对讲机和卫星电话,因为大部分光纤和铜线基础设施在 2003 年战争中被摧毁或在战后被洗劫一空。 15万联军也发出了种类繁多的无线电波,随着单位的轮换而不断变化。超过 80,000 个无线电频率在使用中,并使用 300 个数据库进行监控 其中许多无法互操作。当数百名海军电子战专家部署在巴格达时,盟军才开始解决这个问题;在那之后,联盟的干扰工作得到了更好的协调,并开始减少由无线电引爆的简易爆炸装置的比例。

但电子战的“成功”并没有转化为盟军伤亡的减少。简易爆炸装置制造商只是简单地从无线电控制炸弹切换到由压力板、指令线、被动红外线或志愿者引爆的装置。国防重点转向混合策略：“繁荣右翼”措施,例如更好的车辆装甲和自动驾驶车辆,以及“左翼”

boom”措施,例如破坏炸弹制造网络。更好的装甲起到了一定的作用:虽然在 2003 年几乎每个简易爆炸装置都造成联军伤亡,但到 2007 年平均有四个装置造成伤亡 [140]。装甲车也是其他叛乱中的关键策略,而 DARPA 对自动驾驶汽车的投资在十年后以 Waymo 和特斯拉等商业公司对驾驶员辅助甚至自动驾驶车辆的工作激增的形式得到了回报.

不过,网络中断是一项长期举措,因为它取决于建立良好的人类情报来源;英国和以色列多年来分别针对爱尔兰和黎巴嫩的炸弹制造者。

23.7 定向能武器

在 20 世纪 30 年代后期,有传言称纳粹已经开发出一种可以烧毁车辆点火系统的高功率无线电波束,英美对此感到恐慌。英国科学家研究了这个问题并得出结论认为这是不可行的[990]。他们是正确的 考虑到 1930 年代相对低功率的无线电发射器和简单但坚固的汽车电子设备。

随着原子弹的到来,情况开始发生变化。核装置的爆炸会产生大量伽马射线光子脉冲,进而通过康普顿散射将电子从空气分子中置换出来。大的感应电流会产生电磁脉冲 (EMP),它可以被认为是具有非常短上升时间的非常高振幅的无线电波脉冲。

在地球大气层内发生核爆炸的地方,EMP 能量主要在 VHF 和 UHF 波段,尽管较低频率的能量足以让无线电闪光在数千英里外也能被观察到。在爆炸的几十英里范围内,射频能量可能会感应出大到足以损坏大多数未加固电子设备的电流。据信,地球大气层外爆炸的影响要严重得多(尽管从未进行过测试)。伽马光子在撞击地球大气层之前可以传播数千英里,地球大气层可以电离形成大陆尺度的天线。据估计,在北海 250 英里的高度,1 兆吨级的爆炸可能会烧毁北欧的大多数电子设备。就此而言,美国西海岸(从西雅图到圣地亚哥)的大多数电子设备都可能被盐湖城上空 250 英里的爆炸摧毁。

这种攻击不会直接杀死任何人,但可能造成冠状病毒大流行规模的经济损失 [122]。卡灵顿事件 天文学家理查德·卡灵顿 (Richard Carrington) 在 1859 年观测到的巨大太阳耀斑 会造成类似的破坏;导致极光南至加勒比海。

整个欧洲和北美的电报系统都发生了故障,有时电报员会因此受到电击。 Lloyd s of London 后来估计,这种事件仅对美国造成的损失就可能达到数万亿美元,而且这种事件每一代或两代人都不可避免 [917]。较小的地磁风暴经常发生,例如在 1989 年和 2003 年。出于这个原因,关键的军事系统受到仔细保护,大型 IT 服务公司将其数据中心分散在全球各地,我们有预警卫星,并且运行良好的公用事业支出

保护大型变压器等重要资产的资金。

在苏联于 80 年代中期启动非核武器 EMP 武器的研究计划后,西方对 EMP 的担忧有所增加。当时,美国正在欧洲部署“中子弹” 增强型辐射武器,可以在不拆除建筑物的情况下杀死人。苏联人将其描述为“资本主义炸弹”,它会在不破坏财产的情况下摧毁人,并威胁要用“社会主义炸弹”来摧毁财产(以电子形式),同时不伤害周围的人。

到第二次世界大战结束时,空腔磁控管的发明使制造雷达成为可能,雷达的威力足以在数百码范围内损坏未受保护的电子电路。从阀门到晶体管和集成电路的转变增加了大多数商业电子设备的脆弱性。理论上,恐怖组织可以在卡车上安装雷达,绕过城市的金融部门,摧毁银行。事实上,银行的地下服务器群可能不会受到影响 ;真正的损害是对日常电子设备造成的。更换城市生活所依赖的数以百万计的小工具将非常令人厌烦。

对于战场使用,EMP 武器最好装入标准炸弹或弹壳中,而不必安装在卡车上。然而,它们的军事用途是有限的。美国在伊拉克尝试了一种称为 Blow Torch 的装置来炸毁简易爆炸装置中的电子设备,但效果不佳[140]。 [1082] 中有一项可用技术的调查,描述了如何使用爆炸式泵浦通量压缩发生器和磁流体动力装置以及高功率微波发射器生成太瓦级功率脉冲。但从飞机上投下的电磁脉冲炸弹需要在引爆前部署天线以获得良好的耦合,即便如此,对于半径只有几百米的普通电子设备来说也是致命的。已经为核 EMP 加固的军事指挥和控制系统应该不会受到影响。

EMP的真正意义可能是给伊朗、朝鲜等核技术原始的国家敲诈勒索的武器。当朝鲜向日本附近海域发射导弹时,它发出了一个信号:“我们可以随时关闭你们的经济,而且不会直接杀死一个日本平民。”日本现在正在发展反导弹防御系统。对电子通信的大规模攻击对美国和日本等依赖电子通信的国家的威胁要大于对朝鲜(或伊朗)等不依赖电子通信的国家的威胁。

这种观察也适用于对互联网的攻击,所以现在让我们转向“信息战”。

23.8 信息战

信息战这个词大约从 1995 年开始使用。第一次海湾战争的作战经验推动了它的流行。在那里,空中力量被用来削弱伊拉克的防御,然后发动地面攻击,美国国家安全局人员支持盟国的一个目标是为了启用初始攻击

在没有人员伤亡的情况下进行 尽管当时伊拉克的防空系统完好无损且处于警戒状态。这次攻击涉及标准电子战技术的混合,例如干扰机和反辐射导弹;对指挥中心的巡航导弹攻击;潜入伊拉克并从沙漠中挖出长长的通信电缆的特种部队的袭击;据称,使用黑客手段使计算机和电话交换机瘫痪。 （到 1990 年,美国陆军已经开始招标生产病毒 [1206]。）该行动在空袭的第一个晚上就实现了确保盟军伤亡为零的目标。军事规划者和智囊团开始考虑如何在成功的基础上再接再厉。

2007 年 4 月,爱沙尼亚发生的事件将信息战推回了议程。在那里,政府通过移动一座旧的苏联战争纪念馆激怒了俄罗斯,不久之后该国遭受了一些似乎来自俄罗斯的分布式拒绝服务攻击 [525]。

爱沙尼亚的计算机应急响应小组以冷静的专业精神解决了这个问题,但他们的国家领导人却援引北约条约,呼吁美国对俄罗斯提供军事帮助。俄罗斯有可否认性:数据包风暴是由俄罗斯僵尸网络牧民发起的,对来自爱沙尼亚的消息做出反应并通过聊天室相互怂恿;被定罪的一名男子是爱沙尼亚本土的一名俄罗斯族少年。以色列和巴勒斯坦黑客之间,以及印度和巴基斯坦黑客之间也发生过类似的争斗。爱沙尼亚也发生了一些小的街道骚乱,原因是吵闹的俄罗斯族人反对拆除雕像。尽管如此,北约确实做出了回应,在塔林设立了一个信息战中心,而且正如我在第 2.2.3 节中所描述的,一个成果是塔林手册,它规定了适用于在线行动的军事和国际法,旨在让现实世界的电子影响国家之间的冲突 [1664]。

国家必须出于自卫或其他合法理由并根据武装冲突法采取行动。攻击是合理预期会造成人员伤害或财产损失的操作;它们只能针对战斗人员及其后勤人员,而不是平民;攻击必须在地理上受到限制,而不是不分青红皂白;有些目标是禁区,从医院和礼拜场所到核电站。不过,口译可能会让律师忙个不停。军事和民间组织使用的基础设施都是公平的游戏,虽然“背叛”是被禁止的,但“战争诡计”却不是。

在第 2.2.3 节中,我描述了爱沙尼亚如何只是俄罗斯后来在乌克兰的行动的热身,俄罗斯人在那里摧毁了电力基础设施,并通过 NotPetya 蠕虫对在那里运营的公司造成了重大损害,这对一些公司造成了重大的附带损害在该国设有办事处的国际公司。

但到底什么是信息战?传统观点从
2000 年代中期,源于第一次海湾战争,Whitehead [1977] 表示:

> 战略家……应该使用（信息武器）作为先导武器,在常规攻击和行动之前致盲敌人。

愤世嫉俗者认为,这只是对这些机构几十年来一直在做的事情的再营销,目的是维持冷战后的预算。

然而,当时最有远见的分析家是海军研究生院的多萝西·丹宁 (Dorothy Denning),她 1999 年关于该主题的著作将信息战定义为“以信息媒体为目标或利用信息媒体以赢得对对手的优势的行动”[539]。这非常广泛,不仅包括黑客攻击,还包括所有电子战和所有现有的情报收集技术(从 Sigint 通过卫星图像到间谍),还包括宣传。

在后来的一篇文章中,她讨论了网络在围绕科索沃战争的宣传和激进主义中的作用[540]。

Edward Waltz [1977] 的一位背景是国防规划而不是计算机安全的作家对信息战提出了类似的观点。他将信息优势定义为“收集、处理和传播不间断信息流的能力,同时利用或阻止对手这样做的能力”。这种优势的目的是在没有有效反对的情况下开展行动。该书在计算机安全问题上的技术细节不如丹宁,但它首次尝试制定信息作战的军事学说。

23.8.1 对控制系统的攻击

如果你想利用计算机开发对敌对国家造成真正的破坏,也许首先要看的是发电和配电。摧毁电网相当于网络核打击;一旦电力供应出现故障,那么现代经济中的其他一切也都将关闭。例如,1996 年新西兰奥克兰中央商务区的电力供应中断了五周,导致 74,000 名员工中的 60,000 人不得不在家或搬迁办公室工作,而该地区 6,000 名公寓居民中的大多数在[839]期间搬出。也许最近历史上最严重的恐怖分子“险些失手”是爱尔兰共和军在 1996 年企图炸毁为伦敦供电的大型变电站的变压器 [231]。这失败了,因为爱尔兰共和军的一名高级指挥官是一名英国特工;如果成功的话,伦敦大部分地区的电力供应将中断数月之久,数以百万计的人和企业停电,这可能占英国 GDP 的三分之一。最后,在从塞尔维亚到伊拉克的战争中,对输电和配电的攻击一直是美国的标准战术。 (事实上,2003 年之后的伊拉克叛乱是由于延迟恢复电力供应而火上浇油,这让数百万伊拉克人在没有空调的情况下在酷暑中闷热难耐。)

一旦注意到用于管理电网和石化厂等资产的协议(即 Modbus 和 DNP3)不支持身份验证,安全研究人员便在 2000 年代中期开始关注控制系统,因为这些系统已经在专用网络 在设施内使用固定局域网,租用线路将它们连接到控制中心。公司从 1990 年代后期开始转向 IP 网络,因为它更便宜,但这意味着,如果没有身份验证,任何知道传感器 IP 地址的人都可以读取它,并且任何知道执行器地址的人都可以操作它。恶作剧造成一两次事故后,

2000 年,一家水务公司 IT 承包商的一名心怀不满的员工在澳大利亚马鲁奇 (Maroochy) 造成 800 吨污水泄漏 [7],随后,控制系统安全研究团体开始兴起。

政府试图帮助监管。美国能源部和国土安全部于 2006 年发起一项倡议,为大容量电力系统制定标准的北美电力可靠性公司 (NERC) 在其关键基础设施保护 (CIP) 标准中规定,任何具有黑启动能力需要具备基本的信息安全合规性。黑启动是即使电网掉电也能启动的能力;水电站可以做到这一点,核电站不能,而燃煤电站通常只有在有辅助柴油发电机的情况下才能进行黑启动。该行业的反应是一些燃煤电厂废弃了他们的柴油电厂,因为信息安全不能添加到他们的监管成本基础中,因此超出了底线 [104]。

还尝试扩展控制系统协议以支持加密和身份验证,但这非常困难。变电站主要有三个供应商,如果一个成为项目的主承包商,它通常会从另外两个购买组件,因此兼容性至关重要。变电站的设计寿命通常为 40 年,并附带维护合同,因此变化率非常低。威胁模型也很有趣。任何可以物理访问的人都可以通过按下红色按钮来关闭电源;他们甚至可以通过引起内部短路来破坏变压器,而这只需要一颗子弹。因此,在变电站 LAN 上加密甚至只是验证 trac 意义不大,而且这样做很难,因为一些控制 trac 有 4ms 的延迟要求 [731]。唯一实际的结果是保护逻辑边界 从变电站到网络控制中心的通信 就像人们通过使用笼子或建筑物物理保护资产一样。因此,这项研究计划的一个实际成果是初创公司,其重点是使能源公司和其他公用事业公司能够通过重新划分网络来保护他们的网络。他们设计的专业防火墙和网关现已成为主流产品,并被能源公司广泛使用。

第二个成果是提高了对国家电力供应的间接威胁的认识。我在第 14.2.4 节中描述了大多数欧洲政府如何在电表行业游说后决定安装智能电表,以及我们如何发现建议的英国安装是不安全的;这相当于在英国的每个家庭中都放置了一个可远程控制的 o 开关,甚至没有使用适当的加密身份验证来保护它。 GCHQ 参与了设计,但即使在七年后,也只有少数英国智能电表遵循“改进”的规范。正如我们在第 14.2.4 节中讨论的那样,该项目在财务和节能方面都是一个明显的失败。

第三个成果是一套研究工具。 Shodan 搜索引擎于 2009 年推出,通过互联网抓取来定位和索引连接的设备,使研究人员能够从其软件更新状态中了解哪些设备容易受到攻击; 2011 年,Eireann Leverett 使用它定位了数千个易受攻击的控制系统 [1147]。 Ariana Mirian 及其同事在 2016 年进行的一项扫描发现,全球约有 60,000 台易受攻击的设备,从变电站不等

政府大楼的暖通空调;他们还使用蜜罐来跟踪扫描此类设备的行为者,尽管超过一半来自知名安全公司,但也有相当一部分来自中国或受保护的主机 [1321]。最近,我们的小组参与开发更好的蜜罐来检测对网络连接设备进行扫描和发起攻击的人 [1955];通过在现实的网络位置部署现实的蜜罐,有可能引发敌对行动 [573]。我们对地下犯罪论坛的监测可以追溯到控制系统安全研究的早期阶段,没有发现犯罪集团对控制系统黑客攻击有持续的主管利益,因此有理由假设绝大多数此类活动是由国家发起的演员或其代理人。

控制系统安全研究的爆发与国家行为者对潜力的日益增长的认识同时进行。据报道,参与美国监管推动并在当时主办了一些 Scada 安全会议的爱达荷国家实验室帮助美国国家安全局及其以色列同行开发了 Stuxnet 蠕虫,该蠕虫破坏了伊朗的铀浓缩能力2008-2010 年期间;我在 2.2.1.11 节中对此进行了描述。

最后,正如我在第 2.2.3 节中所描述的,2015 年俄罗斯通过网络攻击对克里米亚（俄罗斯吞并的乌克兰领土)的配电进行了一次常规的乌克兰攻击,该攻击摧毁了 30 个乌克兰变电站,使 230,000 人丧生在黑暗中几个小时 [2067]。然而,这似乎是一种警告,而不是试图造成严重的经济损失,而且从那以后似乎没有对配电进行严重的网络攻击。其他控制系统受到攻击;值得注意的是,伊朗在 2020 年 4 月试图入侵以色列的供水系统,以期将有毒水平的氯引入农村供水系统,但以色列人发现并阻止了这一行为。他们在接下来的一个月进行报复,关闭了伊朗阿巴斯港的一个港口,导致卡车尾随数英里 [229]。

但主要行动已转移到别处。

23.8.2 对其他基础设施的攻击

Stuxnet 事件爆发后,全球各国政府对网络冲突的兴趣激增。地下市场为可利用漏洞支付的价格飙升,除了漏洞的公开市场外,还开发了灰色市场,安全研究人员可以将他们的想法转售给网络武器制造商。除了政府可以用来利用国内外敌人的 PC 或电话的漏洞能力外,人们还担心对信息基础设施（如互联网本身)的攻击。 2007 年俄罗斯对爱沙尼亚和 2008 年对格鲁吉亚的攻击引起了人们的注意,2008 年巴基斯坦对 YouTube 的攻击也是如此（巴基斯坦原本计划只在国内阻止该服务,但它发起的 BGP 攻击导致了全球中断）,以及 2010 年发生的一起事件,当时中国电信劫持了 15% 的互联网地址长达 18 分钟,一些观察家将此解读为“网络核武器”试验。

欧洲网络和信息安全局 (ENISA) 委员会

建议我们写一份关于互联网互连的报告,该报告发表于 2011 年 [1906 年]。我在第 21.2.1 节中讨论了关于 BGP 安全性的主要发现。
通过发布大量虚假路由来破坏 Internet 的路由基础设施当然是可能的;许多事件（包括巴基斯坦和中国的事件)告诉我们这一点。同样真实的是,如果对手能够在发达国家将互联网搞垮几天,结果将是一片混乱（尤其是自从冠状病毒大流行以来,更多的人类活动被迫在线进行）。这种行动的主要技术限制之一是,鉴于大多数国家/地区使用的在线服务是全球化的,最有能力的对手自己也会遭受巨大的伤害。然而,中国在很大程度上是免疫的,因为它的政策是使用长城防火墙将其基础设施与互联网的其他部分分开,并将谷歌、Facebook 和 Twitter 等美国服务提供商排除在外,以支持本地冠军。朝鲜更加孤立。俄罗斯一直试图效仿中国,由于 Vkontakte 等服务提供商与欧美基础设施的关系更加密切,普京总统于 2019 年 5 月通过了一项法律,要求俄罗斯互联网服务提供商在 11 月之前能够独立于外国互联网基础设施运营。 12 月,宣布测试成功,但没有人注意到发生了什么;由于冠状病毒,原定于 2020 年 3 月进行的第二次测试显然被推迟了 [159]。如果这要奏效,那么俄罗斯将像中国一样,能够对世界其他地区的互联网发动大规模破坏攻击。

23.8.3 对选举和政治稳定的攻击

2011-16 年期间,信息作战的重点从攻击基础设施转向政治冲突。这一时期始于阿拉伯之春,我将在第 26.4.1 节中更详细地讨论。在那里,社交媒体被用来推动阿拉伯世界反对专制政权的起义;尽管突尼斯人推翻了他们的独裁者并实现了民主,但其他地方的结果从叙利亚和也门的内战到利比亚的政府失败以及其他地方的统治者的镇压。我在第 2.2.4 节中描述了阿拉伯政府如何从西方和以色列大力购买监控技术,并雇佣前 NSA 雇佣军来追踪和骚扰他们在国内外的对手。

到 2016 年,我们已经看到俄罗斯对英国退欧公投和美国总统大选进行了大量干预。俄罗斯在管理选举方面有着悠久的历史。我在2001年的第一版中讽刺地写道：“我衷心希望弗拉基米尔·普京（Vladimir Putin 1991年接任克格勃第8、16局。据报道,它的负责人斯塔罗沃伊托夫将军是克格勃的旧类型;他的机构直接向叶利钦总统汇报,叶利钦总统选择普京作为他的继任者。” [733, 1003] By the time Putin s party was re-elected in 2007, the cheating had become so blatant – with gross media bias and state employees ordered to vote for the ruling party – that the international community would not accept the result as free和公平。

到 2012 年大选时,正如我在第 2.2.3 节中指出的那样,俄罗斯民众已经变得非常抗拒,以至于普京觉得需要外部敌人来争取公众的支持。他于 2014 年入侵乌克兰,声称同时保卫它免受法西斯分子、同性恋者和犹太人的侵害,并吞并了克里米亚 解除了国际制裁。这场运动涉及“混合战争”战术,结合了“小绿人” 身着制服但没有徽章、自称是乌克兰反法西斯分子的俄罗斯士兵 与各种网络攻击、宣传,甚至攻击乌克兰媒体,谎称一位亲俄候选人赢得了选举。在欧洲对俄罗斯实施制裁作为对入侵乌克兰的惩罚后,克里姆林宫成为整个欧洲极右翼团体的主要资助者,支持英国的脱欧运动和德国 AfD 等政党的崛起。在公开宣扬法西斯思想(包括国内伊万·伊林的意识形态)的同时,普京也设法赢得了欧洲反法西斯左派的支持。自制裁以来的总体战略一直是通过一切可用手段扰乱和削弱美国和欧盟。

这种信息战中使用的战术与电子战有很多共同点。普京和其他专制领导人经常用假新闻淹没国内外的目标受众;这种干扰破坏了对更可靠媒体的信任 这些媒体反过来被指责为“假新闻”。如果你不能阻止你的民众阅读《纽约时报》,你只要确保他们不相信就可以了 [474]。有散装诱饵,如 cha ; 2014 年俄罗斯人在乌克兰击落马来西亚航空公司的 MH17 航班后,他们同时推出了许多不同的阴谋论 [1593]。许多政客使用其他诱饵来分散媒体对可能损害他们的新闻的注意力;特朗普使用了从世界卫生组织到羟氯喹 [1710] 的一切。欺骗 IFF 的等价物可能是三角测量 窃取对手品牌关键方面的艺术(就像鲍里斯约翰逊在英国退欧公投中将 NHS 置于他的宣传中心一样)。相当于反辐射导弹可能会阻止对手的网站或扼杀他们的资金。腐败的领导人指责他们的对手腐败,而将国家的困境归咎于同性恋者和犹太人的独裁者会高兴地指责他们的对手是法西斯主义。

因此,认为选举的安全性仅限于匿名但可核实的计票本身是错误的。正如简易爆炸装置可以在爆炸前(通过情报或干扰)或之后(通过装甲)被击败,选举也可以在投票前或投票后被颠覆。即使在成熟的民主国家,政客们也一直在试图操纵选举权和竞选规则,例如竞选资金限制。例如,俄罗斯人为英国脱欧公投中的两次“脱欧”运动捐款,这是非法的,并且两次运动分别违反了总体财务限制,因此被罚款 [1265]。这些罪行的披露并没有导致重新进行投票;它只是帮助使英国政治瘫痪了三年。英国首相大卫卡梅伦早些时候改变了选举规则,要求所有选民单独登记,而不是按家庭登记,以减少选民名册上的年轻人数量(这本应该帮助他的保守党,但在公投中适得其反) .结果更多是由于选民的不满和自满的支持留欧的政客的失误,而不是敌人的行动,但积极推动有害结果的敌人的存在无济于事。时至今日,仍有许多人支持

不要认为公投结果是有效的 从俄罗斯人的角度来看,这是一个真正美妙的结果。

对当年晚些时候的美国总统大选也可以做出类似的评论;我在第 26.4.2 节讨论了政治学家 Yochai Benkler 对假新闻选举影响的分析。同样,俄罗斯人扮演的角色是利用现有的两极分化,在可能的情况下火上浇油(例如,通过泄露来自克林顿阵营的被黑电子邮件,如第 2.2.3 节所述)并尽可能地购买影响力 [385]。Had Clinton won the election, I expect evidence of hacked election systems would have emerged to enable Trump to refuse to accept defeat.事实上,美国有 6,000 种不同的投票系统,这使得总统选票很难通过技术手段窃取,但其可信度面临挑战。选举制度就像一个警报器;正如我们在 13.3 节中讨论的那样,您可以通过破坏对它的信心来消除警报,从而忽略警报。选举的真正客户是失败的一方,如果其中一方没有真正准备好接受失败,那么他们所需要的可能就是一个借口。无论特朗普在 2020 年 11 月是赢还是输,我们都可以预期美国选民的两极分化会加剧,美国在世界上的地位会下降 这又是俄罗斯的胜利。

中国在很大程度上避免干涉别国内政;正如我在第 2.2.2 节中所述,他们长期以来一直认为,未经审查的互联网相当于美国颠覆共产党的统治,但他们在这方面的立场一直是防御性的。他们的重点是建设自己的经济、技术和情报能力,而不是对其他国家进行破坏性或政治性攻击。正如我在第 2.2.2 和 22.2.4 节中讨论的那样,这种能力建设产生了政治后果,最显着的是美国为防止华为主导 5G 基础设施所做的努力。随着中国寻求成为美国的竞争对手,这似乎将成为新冷战的前沿。有迹象表明,2020 年中国将采取更积极的外交手段,因为中国试图巩固其围绕冠状病毒的说法,并利用美国对这一流行病的混乱反应。

23.8.4 学说

早在 1999 年,丹宁和华尔兹就将宣传和其他心理战纳入信息战,这在当时只是少数人的观点,但此后的事件已经证实了这一点。它确实有历史先例。从罗马人和蒙古人努力宣传无敌神话,通过双方在第二次世界大战和冷战期间使用宣传电台,到在科索沃战役期间轰炸塞尔维亚电视台和拒绝服务攻击在俄罗斯机构的车臣网站上 工具可能会改变,但游戏内容保持不变。

在其间的二十年中,名称发生了变化:五角大楼于 1998 年采用“信息战”,2006 年改为“信息作战”,2013 年改为“网络空间作战”[1164]。存在一些很大的盲点:2016 年五角大楼的任何人都没有工作要担心圣彼得堡的人假装来自 Black Lives Matter [1221]。

与此同时,许多错误的观念也逐渐被摒弃。它曾经是

说归因太难了;这还没有被证实。其他人过去曾表示,信息战提供了一种无人员伤亡的取胜方式:“只需入侵伊朗电网,然后看着他们求和”。然而,越是发达国家,暴露的风险就越大,如果网络攻击针对平民的程度比其他方式更大,那么攻击者很可能会被描绘成战争罪犯。更重要的是,如果北约国家是侵略者,塔林手册将支持起诉。

在本书的第二版中,我想知道网络攻击是否会在公开冲突或游击战中找到一席之地。到目前为止,我们已经看到俄罗斯将它们发展成为在格鲁吉亚和乌克兰磨练的混合战争战略的一个组成部分。我们不仅在英国和美国,而且在德国、法国和其他地方都看到了对民主机制的攻击。这是否也是未来十年的未来,因为美国、俄罗斯和中国继续对着联合国甜甜地微笑,同时在桌子底下互相踢打?

或者还有其他的可能性吗?我们已经看到和平示威者在阿拉伯之春以及中东的暴力极端分子使用网络策略,但大多没有成功。那里还有什么?还是国家会继续扮演主要角色?

23.9 总结

电子战在冷战期间蓬勃发展,并发展出许多有趣的技术,其中一些技术已进入主流信息安全领域。在多年缺乏关注和资金之后,它开始重新回到议程上,因为中国旨在与美国竞争,而俄罗斯人也在对其武装部队进行现代化改造。人工智能革命可能会改变游戏的玩法,因为认知雷达和声纳,加上更好的多传感器数据融合技术,将优势从拥有最多兆瓦的平台转移到拥有最智能软件的玩家身上。不过,胜利很可能需要物理力量和巧妙欺骗的有效协调。

十年前,人们已经在谈论电子战变成信息战。我们偶尔会看到网络武器的使用,从 2010 年针对伊朗铀浓缩设施的 Stuxnet 攻击到俄罗斯对乌克兰的 NotPetya 攻击。很容易观察到民族国家行为者正在准备攻击其他国家的关键国家基础设施。

然而,在 2010-20 年实际开展的绝大多数信息行动都是心理战和宣传,旨在散布不和、扰乱选举等政治制度并加深政治两极分化。用于操纵敌方雷达的诱饵、干扰和其他技术与用于操纵舆论的技术之间存在一些有趣的相似之处。

研究问题

我自己的研究小组有两个相关的兴趣。首先,我们一直在研究对抗性机器学习。例如,如果导弹使用神经网络

寻找它的目标,那么我们能否从观察中足够好地近似该模型以确定是否存在比随机机动更好的规避策略[2071]?我们能否设计出需要大量计算才能理解的伪装?我们能否在神经网络中添加密钥,使它们的不同实例容易受到不同对抗样本的攻击,从而限制对手的学习能力 [1732]?

其次,通过剑桥网络犯罪中心,我们收集了大量关于垃圾邮件、网络钓鱼、恶意软件、僵尸网络命令和控制trac 以及其他在线恶意行为的数据。我们开发了更好的蜜罐来捕获攻击轨迹,包括针对嵌入式系统的攻击。我们将我们的数据集授权给全球一百多名研究人员。他们现在开始包括政治极端主义和网络犯罪的地下论坛。

进一步阅读

Curtis Schleher [1662] 提供了从雷达到隐身再到 EMP 武器的电子战技术方面最好的全面参考； Doug Richardson [1601] 写了一个很好的总结。 Andrew Viterbi [1964] 对扩频序列的抗干扰特性进行了经典介绍； Robert Scholtz [1682] 巧妙地讲述了扩频的历史； Raymond Pickholtz、Donald Schilling 和 Lawrence Milstein 对扩频数学的经典介绍 [1525];而标准教科书是由 Robert Dixon [567] 编写的。关于通信干扰最详尽的参考文献是 Richard Poisel [1530]。休·格里思 (Hugh Griths) 和尼古拉斯·威利斯 (Nicholas Willis) 描述了第二次世界大战中英国皇家空军和德国空军之间的电子战 [824],而 RV 琼斯关于英国电子战和科学情报的整体历史提供了很多见解,而不仅仅是技术如何发展但也发展成战略和战术欺骗[990, 992]。 Santiago Figueroa-Lorenzo、Javier A~norga 和 Saioa Arrizabalaga 在 [684] 中调查了工业控制系统中使用的各种协议,并讨论了它们的漏洞。

Matthew 和 Martin Weiss [2005] 讨论了美国电网针对卡林顿事件和 EMP 的不足之处。关于信息操作的读物,我推荐我在心理学和监视章节末尾列出的读物;对于俄罗斯对美国和欧洲民主的攻击,一个起点是向美国参议院外交关系委员会提交的一份报告[385]。