HM Government

2022年国家网络战略

与全英国一起开创网络未来

2022年
国家网络战略

与全英国一起开创网络未来

目录

附加目录

前言

英国是一个开放和民主的社会，在合作和创新方面的成就支撑着我们成为成功的外向型全球化国家。而这一点已经在我们应对国际卫生突发事件和推广净零目标上就已经有所体现。但是这种做法的优势在网络事务上表现得最为明显。

无论是在我们均衡发展和团结整个国家的过程中，实现网络给我们公民和经济带来的广泛利益，还是与伙伴一起努力建设一个反映我们国家价值观的网络空间，又或是充分利用我们的网络能力来影响全球事件，英国都将网络视为一种可以在受到技术塑造的环境中，保护和促进英国利益的方式。

此次全新的《国家网络战略》就是我们的规划。保证英国在这个快速发展的数字世界中保持其自信、实力和韧性。我们也将继续适应、创新和投资，用于保护和促进我们在网络空间的利益。

在2016年开创性的《国家网络安全战略》的基础上，本章节将带领我们进入一个对网络攻击更具韧性的英国的未来。作为主管部长，我非常清楚它有个核心目标。第一，我们应该加强对网络至关重要的技术。其次，我们应该限制对个别供应商或技术的依赖，这些供应商或技术是在与我们价值观不同的制度下开发的。

英国的科学和技术将成为驱动这一变化的引擎，保证网络继续作为国家的经济和战略资产，让我们的技术更加值得信赖，能够更好地抵御各种网络对手，而这些对手的能力直到最近仍是其国家专属的。

作为政府，我们承诺在研发上投入220亿英镑，并将技术置于我们国家安全计划的核心。我们都看到了数字技术的变革潜力，但正如5G一样，它们也有造成破坏的潜力。我们的人工智能和数据政策计划将有助于确保我们处于这些技术的前沿。而我们根据网络战略采取的措施，也将确保我们对供应商和伙伴的安全性和韧性充满信心。

去年国家网络部队的建立标志着我们在攻击性网络能力上取得了重大进步。但是，即使我们加强回应针对英国和我们公民的攻击，基本的网络安全仍然是我们努力的核心。我们的重点也是让公共部门更有韧性，帮助地方议会保护他们的系统和公民的个人数据免受勒索软件和其他网络攻击的影响。

作为一个社会，网络是每个人享有的。通过这一战略，政府正在广泛开展工作，保护英国公民和公司及其国际伙伴，帮助其实现愿景，使网络空间成为一个可靠和有韧性的地方，让人和商业在此蓬勃发展。

兰开斯特公爵领地事务大臣兼内阁办公室部长史蒂夫·巴克利（Steve Barclay）议员阁下

引言

数字时代的机遇和挑战

1. 技术呈指数级的进步，加上不断降低的成本，使世界的联系比以往任何时候都要紧密，带来非凡的机遇、创新和进步。新冠肺炎疫情加速了这一趋势，但我们很可能仍处于长期结构性转变的早期阶段。网络空间的全球性扩张正在改变我们的生活、工作和交流方式，并转变着我们在金融、能源、食品配送、医疗卫生和交通等领域所依赖的关键系统。简而言之，网络空间已成为我们未来安全和繁荣不可或缺的一部分。这为像英国这样技术先进的国家提供了绝佳机会，以新的方式来实现国家目标。

2. 这一变化的规模和速度往往超过我们的社会规范、法律和民主制度的变化速度，也正在释放出前所未有的复杂性、不稳定性和风险。过去一年，医院和输油管道、学校和企业遭到了网络攻击，其中一些因勒索软件而陷入停顿，而商业间谍软件则被用于攻击活动人士、记者和政界人士。网络空间的跨国性质意味着没有国际合作就无法应对这些挑战，但它也是对于系统性竞争，以及利益、价值观和我们全球未来愿景之间诸多冲突而言日益重要的舞台。

我们的愿景：
支持国家目标的网络力量

3. 在此背景下，网络力量正在成为一个日益重要的国力手段和战略优势来源。**网络力量是在网络空间内和通过网络空间保护和促进国家利益的能力。**最有能力驾驭数字时代机遇和挑战的国家，未来将更为安全、更具韧性、更加繁荣。英国是世界上数字技术最发达的国家之一，政府在国内外都有雄心勃勃的技术议程。这意味着我们尤其面临网络空间的挑战，但同时也处于独特的有利地位，能够为我们的公民和人类的共同利益抓住机遇。

4. 在接下来的十年里，互联网、数字技术以及支撑这些的基础设施对我们、以及我们的盟友和对手的利益将变得越来越重要。随着我们在一个竞争更加激烈的时代为英国打造新的角色，加强我们的网络力量将使我们能够为行业和其他国家引领道路，领先于未来的技术变革，减轻威胁，并获得相对于对手和竞争者的战略优势。这将使英国成为最安全、最具吸引力的数字经济体之一，适宜生活、营商和投资。

5. 我们的愿景是，**到2030年，英国将继续作为一个负责任的民主网络大国，能够在网络空间内和通过网络空间保护和促进我们的利益，支持实现国家目标**：

- 一个更安全、更具韧性的国家，更好地应对不断变化的威胁和风险，并利用我们的网络能力保护公民免受犯罪、欺诈和国家威胁的影响
- 一个创新、繁荣的数字经济体，机会更加均衡地分布在整个国家和我们多样化的人口中
- 一个科技超级大国，安全地利用变革性技术支持建立一个更绿色、更健康的社会
- 一个在全球舞台上更有影响力和价值的伙伴，塑造未来开放和稳定的国际秩序的边界，同时维护我们在网络空间的行动自由

6. 在过去的十年里，我们已经把英国建设成了一个网络强国，建立了尖端的网络安全和运营能力，以及领先的网络安全部门。本战略基于通过《2016-2021年国家网络安全战略》(National Cyber Security Strategy 2016-2021) 取得的重大进展，以及政府在《安全、国防、发展和外交政策整合评估》(Integrated Review of Security, Defence, Development and Foreign Policy) 中提出的三项重要结论。首先，在数字时代，英国的网络力量将成为实现我们国家目标的一个越来越重要的手段。第二，考虑到所有全部网络目标和能力，维持我们的网络力量需要一个更加全面和综合的战略。第三，这必须是一种全体社会的方法，在会议室或教室里发生的事情对我们的国家网络力量的重要性不亚于技术专家和政府官员的行动，合作对于我们的成功至关重要。


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

战略的五大支柱

7. 《整合评估》为此战略制定了五项“优先行动”作为我们战略框架的支柱，**指导和组织我们将采取的具体行动以及我们希望在2025年前取得的成果**：

- **支柱一：加强英国网络生态系统**，对人才和技能进行投资，并深化政府、学术界和产业界之间的合作关系
- **支柱二：建设一个富有韧性和繁荣的数字英国**，降低网络风险，让企业能够最大限度地获得数字技术带来的经济效益，让公民在网上更安全，对自己的数据受到保护更有信心
- **支柱三：引领对网络力量至关重要的技术**，发展我们的产业能力并建立框架以保护未来技术
- **支柱四：提升英国的全球领导力和影响力，建立更加安全、繁荣和开放的国际秩序**，与政府和行业伙伴合作，分享支撑英国网络力量的专长
- **支柱五：侦测、瓦解和威慑我们的对手，以在网络空间内和通过网络空间加强英国的安全**，更加整合性地、创造性地和常规性地利用英国的各种手段

8. 本《战略》的第一部分将阐述我们的战略背景、战略目标以及未来十年我们将采取的战略方法。第二部分将阐述为了实现我们到2025年的目标索要采取的具体行动，这些行动围绕这五大支柱展开。

愿景

到2030年，英国将继续作为一个负责任的民主网络大国，能够在网络空间内和通过网络空间保护和促进我们的利益，支持实现国家目标。

支柱和目标

支柱一

加强英国网络生态系统

1. 强化必要的结构、合作关系和网络，对网络采取全社会的方法并予以支持。
2. 在各个层级提升和扩大国家的网络能力，包括创造世界一流的多元网络专业，启发和培育未来人才。
3. 培育可持续、创新和具有国际竞争力的网络和信息安全行业，交付高质量的产品和服务，满足政府和广大社会的需求。

支柱二

建设一个富有韧性和繁荣的数字英国

1. 增进对网络风险的理解，以驱动更有效的行动增强网络安全和韧性
2. 通过改善英国组织内部对网络风险的管理以及为公民提供保护，更有效地预防和抵抗网络攻击。
3. 强化国家和组织韧性，以准备、响应网络攻击和从中复原。

支柱三

引领对网络力量至关重要的技术

1. 改善我们预期和评估的能力，并基于网络力量关键的科技发展采取行动。
2. 培养和维持国家和同盟在网络空间关键技术安全性方面的优势。
2a. 保持强健且具有韧性的国家层面的加密关键能力，以满足英国政府的客户、伙伴和盟友的需求，相关工作也适当地减缓了我们所面临的重大风险，包括来自最强大对手的威胁
3. 巩固下个世代的互联技术和基础设施、缓解依赖全球市场的网络安全风险，并确保英国的使用者能获取值得信赖且多元的供给。
4. 与多利益相关方的社群合作，塑造优先领域的全球技术标准制定，这些优先领域对于维系我们的民主价值、确保网络安全，和通过科技推进英国的战略优势等工作至关重要。

支柱四

提升英国的全球领导力和影响力

1. 加强国际合作伙伴的网络安全和韧性，增加破坏和威慑对手的集体行动。
2. 塑造全球治理，促进自由、开放、和平且安全的网络空间。
3. 运用和输出英国的网络能力和专业技能以增强我们的战略优势，并促进更广泛的对外政策和繁荣利益。

支柱五

侦测、瓦解和威慑我们的对手

1. 对国家、罪犯和其他恶意网络行动者与活动进行侦测、调查和信息共享，以保护英国的利益与公民。
2. 威慑和瓦解攻击英国利益和公民的国家、罪犯和其他恶意网络行动者。
3. 在网络空间内和通过网络空间采取行动支持我们的国家安全，并预防和侦测重大犯罪。

支持国家目标

- 安全和韧性
- 科学和技术大国
- 经济繁荣
- 塑造国际秩序

第一部分：
战略


CyberFirst Girls' Competition 2020
1 The Tiffin Girls' School 805
2 The Castle School 760
3 Herschel Grammar School 665
4 The Cathedral School 660
5 King Edward's School 635
6 Stretford Grammar School 580
7 Greenwood Academy 520
8 Loughborough High School 455

战略背景

竞争时代的全球化英国

9. 2021年3月发布的《安全、国防、发展和外交政策整合评估》描述了英国政府对英国未来十年在世界舞台上的愿景，以及我们将在2025年前采取的行动。《整合评估》认识到，为了让英国做好准备迎接更具竞争力的世界，我们必须接受科学和技术创新，以促进我们的国家繁荣和战略优势。《国家网络战略》正是基于这种方法制定的，它的发布是《整合评估》战略目标下"通过科学技术保持战略优势"的承诺之一。

网络格局

10. 网络空间对政策带来的挑战不仅仅是技术性质的。网络领域是一个人造的环境，从根本上说是由人类行为塑造的。网络会放大人类行为，不管是好是坏，其影响通常在物理世界也能感觉到。网络空间由私营企业、政府、非营利组织、公民个人甚至罪犯所拥有和运作。这意味着对这一背景的任何回应都必须将地缘战略与国家安全、刑事司法与民事监管、经济与产业政策联系起来，并要求对不同的文化或社会背景以及在线互动的价值体系有深刻的理解。

11. 网络空间也超越国界。技术供应链和关键的依赖性日益全球化，网络罪犯和基于国家的行动者在世界各地活动，强大的技术公司出口产品并制定标准，治理网络空间和互联网的规则和规范在国际论坛上制定。随着技术和人们使用技术的方式发生变化，网络空间也在不断演变，这要求我们采取敏捷和迅速反应的方法。

网络空间的各个层面

什么是网络空间?

对我们许多人来说,网络空间是我们在网上交流、工作和处理日常事务时体验的虚拟世界。从技术角度来说,网络空间是相互依存的信息技术网络,包括互联网、电信网络、计算机系统和互联网连接设备。对于军方来说,当考虑我们努力应对网络空间威胁时,它是一个行动领域,与陆地、海洋、空中和太空一样。

网络空间是如何体验的?根据定义,网络空间是一个"共享"空间,其规模和复杂性意味着每个人的体验都是独一无二的。当公民在网上查看银行账户或在家观看电影时,就会进入网络空间。企业使用网络空间将员工与他们需要的资源连接起来,无论是获取信息还是控制制造流程。政府利用在线门户网站向公民提供公共服务。网络专业人士则在后台研究技术、标准和协议,让它们为用户"服务"。所有这些群体都以不同的方式和出于不同的目的使用网络空间,而且使用得越来越多。

线上体验

- 电子邮箱账户
- 游戏个人档案
- 社交媒体账户
- 银行账户登入信息
- 感应式交通卡ID
- 健身追踪器个人档案

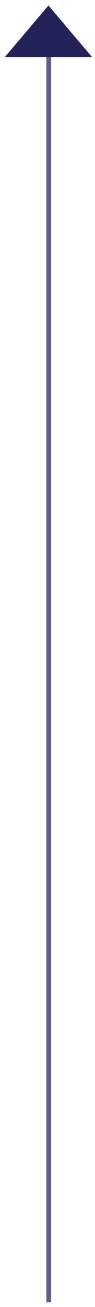
软件、系统和数据

- 企业IT系统
- 数据库,例如:英国税务海关总署的税务记录
- 工业控制系统
- Windows/OS
- 应用程序,例如:WhatsApp、Facebook、抖音
- 编程语言,Python、C++

实体设备和通讯

- 路由器、集线器
- 服务器
- 无线网络、以太网
- 无线电天线
- 智能冰箱
- 感应式交通卡读取器
- 手机、个人电脑和其他个人设备

网络空间可以分为三个层面来描述：



虚拟层

这是大多数人体验到的网络空间。这包含在共享虚拟空间中代表个人或组织的虚拟身份。虚拟代表可能是电子邮箱地址、用户身份识别、社交媒体账户或是一个化名。一个个人或组织可以在网上有多个身份。同样的，多个个人或组织也可以共同创造一个共享的身份。

逻辑层

网络空间的这个部分由代码和数据组成，例如操作系统、协议、应用程序和其他软件。逻辑层需要物理层才能运作，信息的流动需要通过有线的网络或是电磁频谱。逻辑层结合物理层让虚拟身份可以沟通和行动。

物理层

网络空间的物理层包括所有传输数据的硬件，包括从家中的路由器、电线、集线器，到大型技术公司所运营的复杂电信系统。物理基础设施以外，数据传输所经过的电磁频谱也算，例如：无线网络和无线电。

网络空间经验

网络力量

12. 网络力量的概念是我们战略的核心，我们将其定义为一个国家在网络空间内和通过网络空间保护和促进其利益的能力。我们指出了网络力量的五大维度，它们与该战略的支柱相一致:

- 人才、知识、技能、结构和伙伴关系是我们网络力量的基础，支撑着所有其他组成部分，并将它们整合到一个国家方案中
- 通过网络安全和韧性保护我们资产的能力，以充分实现网络空间为我们的公民和经济提供的效益
- 保持关键网络技术发展的技术和产业能力，并为社会利益部署取得新的进步
- 全球影响力、关系和道德标准，根据我们的价值观和利益塑造网络空间的规则和规范，促进国际安全和稳定
- 在网络空间内和通过网络空间采取行动以支持国家安全、经济福祉和预防犯罪的能力。这包括在真实世界取得效果并帮助实现战略优势的网络行动，以及通过对执法行动和网络制裁的应用将恶意网络行动者罪犯绳之以法并破坏他们的活动

13. 网络力量不同于更为传统的力量形式。它包括无缝融合硬实力和软影响力手段。它更加分散，各国政府必须与伙伴合作，以获取和利用这一实力。随着以前的尖端能力被新的进步淘汰，技术变化的速度意味着实力的得失都会发生得更快。

14. 我们的战略反映了这一点。战略描述了作为全社会一份子的我们将如何尽可能地与合作伙伴合作。我们将开展更多的工作来解决上游问题和根本原、，预测未来趋势和制定长期对策、且更加积极地塑造而不是应对有争议的地缘政治环境。

作为当今网络强国的英国

15. 英国已经是领先的网络强国。[1] 在过去十年中，政府领导国家持续作出努力，不断加强英国的网络安全，提高公众对网络风险的意识，发展网络安全行业，并通过网络空间发展广泛的能力，以应对来自敌对行动者的威胁。虽然我们已经取得了巨大的进步，并使自己处于强有力的地位，但在当前战略的五大支柱方面，我们仍然面临着巨大的挑战。

[1] 英国在国际电信联盟 (International Telecommunication Union) 的全球网络安全指数 (Global Cyber Security Index) 中排名第二，在哈佛贝尔弗中心 (Harvard Belfer Center) 的网络力量指数 (Cyber Power Index) 中排名第三，在国际战略研究所 (International Institute of Strategic Studies) 的网络力量能力评估 (Cyber Power capability assessment) 中处于第二级。

英国的网络生态系统和技术领导力

16. 英国建设其网络力量的方法包括共同努力发展本国的网络技能基础和商业能力，英国政府与北爱尔兰、苏格兰和威尔士的分权政府合作并相互学习。英国网络安全行业发展快速，去年有1400多家企业创造了89亿英镑的收入，支持了46700个技术工作岗位，并吸引了大量海外投资。这个行业对我们的网络力量至关重要，它为我们的安全、国际影响力和经济增长提供了支持。我们巩固了英国作为网络安全研究全球领军者的声誉，有19个学术卓越中心和4个研究所负责解决我们最紧迫的网络安全挑战。

17. 网络安全领域的劳动力在过去四年中增长了约50%，技能经常供不应求。我们与产业、专业组织、学生、雇主、现有网络安全专业人士和学术界进行了广泛接触，以更好地了解网络安全技能挑战的性质。我们提供了广泛的课外活动来激励年轻人从事网络安全职业。从2019年到2020年，我们让近57000名年轻人参与了我们的“网络优先和网络发现”（CyberFirst and Cyber Discovery）学习计划。我们扩展了课程以覆盖更年轻的学生，“网络优先”女子在线竞赛吸引了11900名女孩参加，排名靠前的团队在英国的18个场地同时比赛。我们的“网络优先”助学金计划吸引了非常积极、有才华的本科生。去年，该计划有750名学生，所有56名毕业生都从事了全职网络安全工作。

18. 尽管我们有这些干预措施，但更广泛的技能储备仍然是一个重大挑战。在整个经济中的132万家企业中，约50%仍然报告存在基本技术的网络安全技能缺口。[2] 虽然英国网络安全领域发展迅速，但大多数公司都是初创企业，面对国际整合，建立大规模国内供应商仍具有挑战性。发展5G的经验表明，英国和我们的盟友在更广泛的技术行业的一些关键领域并不处于领先地位。能够在对网络力量至关重要的技术领域确立领先地位的国家将更有优势，影响这些技术的设计和部署方式，更有能力保护其安全和经济优势，并更快地利用机会，在网络能力方面取得突破。

英国的网络韧性

19. 在过去十年，我们实施了广泛的干预措施，旨在加强英国的网络韧性。这要归功于我们在一些核心网络能力方面的大量持续投资，包括国家网络安全中心（NCSC）、执法部门、政府各部门的安全和政策专业人员，以及我们不断扩大的国内和国际合作伙伴关系。

[2] 数字化、文化、媒体和体育部，《2021年英国劳动力市场的网络安全技能》（Cyber security skills in the UK labour market 2021）（2021年）

20. 我们最具创新性和突破性的努力是采取大规模行动，包括制定和不断推广积极网络防御（Active Cyber Defence，ACD）计划。去年ACD挡下了230万件恶意行动，其中包括442件冒用NHS（英国国民保健服务）名义的钓鱼式攻击和80个在非官方网站上能下载到的非法NHS应用程序。[3] 我们也在全球范围内主导推动互联性消费电子产品的“设计即安全”（secure by design）概念，在2018年制定了一套英国行为准则，鼓励其他人共同遵守，并为第一套全球适用的联网消费电子产品行业标准做出贡献。[4] [5]

21. 新的监管规则对网络安全已经产生的积极的影响，有82%的组织都表示他们是因为2018年《英国通用数据保护条例》（UK General Data Protection Regulation，UK GDPR）的出台而做出的改进。[6] 还有77%的企业现在将网络安全视为高优先级，相比于2016年增加了12%。[7] 2018年出台的《网络与信息系统监管条例》（Network & Information Systems Regulations，简称“NIS条例”）也要求指定的组织需要采取措施来保障其网络和信息系统的安全，进而减少了必要性服务和重要数字服务所面临的网络风险。[8] 英国四大地区合作的最佳案例是在卫生领域方面的改善，包括《网络与信息系统监管条例》的实施。

22. 我们为整个经济中的各个组织提供了全面的网络安全建议和指南，并在新冠疫情期间为关键行业提供定制化的支持。对于一般大众来说，我们的“网络安全意识”（Cyber Aware）计划提供建议，让民众了解可以采取哪些步骤在网上保护自己。当网络攻击突破防线时，我们运用世界一流的事件响应能力为最严重的案件提供直接支持，而且因为我们对地方执法专家进行了投资，所以现在每一个上报的事件都会获得响应。

23. 我们在全英国各地建立了专家执法网络处，还有与之并行的网络保护网（cyber PROTECT network）、经济犯罪受害者关怀处（Economic Crime Victims Care Unit）以及区域性的网络韧性中心（Cyber Resilience Centres）。这些倡议意味着一般公民和中小型组织可以就近联系到既有专业技能又有本地知识的专家，更容易获得支持与指导以提升其网络韧性。

[3] 国家网络安全中心，《2021年国家网络安全中心年度回顾》（NCSC Annual Review 2021）（2021年）
[4] 数字化、文化、媒体和体育部，《消费类物联网设备安全行为准则》（Code of Practice for Consumer IoT Security）（2018年）
[5] 数字化、文化、媒体和体育部，《基于行为准则的ETSI行业标准》（ETSI industry standard based on the Code of Practice）（2019年）
[6] 数字化、文化、媒体和体育部/容诚，《GDPR对网络安全结果的影响》（The impact of GDPR on cyber security outcomes）（2020年）；2018年引入英国法律的《通用数据保护条例》现已被《英国通用数据保护条例》取代
[7] 数字化、文化、媒体和体育部，《2021年网络安全漏洞调查》（Cyber Security Breaches Survey 2021）（2021年）
[8] 数字化、文化、媒体和体育部，《2018年网络与信息系统监管条例实施后审查》（Post-Implementation Review of the Network and Information Systems Regulations 2018）（2020年）

24. 但是，有越来越多证据显示我们的国家韧性出现了缺口，影响政府、个人和企业的网络犯罪、漏洞和借助网络进行的犯罪（例如欺诈）持续增加。[9] [10] 老旧的IT系统、供应链弱点和网络安全专业人才短缺都是令人担忧的问题。将近四成的企业（39%）和四分之一的慈善组织（26%）表示曾在过去一年经历网络安全漏洞或攻击，而且许多组织（尤其是中小企业）缺乏自我保护和响应事件的能力。[11] 产业告诉我们许多企业并不理解他们所面临的网络风险，对网络安全进行投资的商业激励也不明确，而且他们也没有足够动机去上报漏洞或攻击。

英国的国际领导力与影响力

25. 英国的网络专业技能在国际上受到合作伙伴的高度重视，英国也在增进国际能力与决心以对抗恶意网络活动的过程中扮演了关键的角色。通过负责任地运用我们的攻击性网络能力，英国的地位得到进一步加强，这与英国、国际法律与我们公开表明的立场一致，不同于有些对手无差别式的活动。

26. 就任英联邦轮值主席期间，英国构思并领导《英联邦网络宣言》（Commonwealth Cyber Declaration）的实施，这是我们对于网络空间的安全、繁荣与价值的共同承诺。国家打击犯罪署（National Crime Agency，NCA）的国际网络加强了我们与海外合作伙伴的网络犯罪执法行动，这是得益于我们与伙伴长期在行动响应方面合作所积累的紧密关系。英国也在五大洲拓展了其网络和技术安全人员的海外网络，在超过100个国家进行能力建设，加强英国的影响力并推广英国的价值观。

27. “网络安全大使”（Cyber Security Ambassador）项目培养了长期的合作关系并帮助英国企业获得许多大型的国际合同。英国的“数字接入计划”（Digital Access Programme）等国际发展干预措施成功与非洲、亚洲和拉丁美洲的国家合作，提供技术建议以加强当地政府、企业和使用者的网络安全能力，包括提升欠缺服务条件社区的网络卫生技能，让最弱势的族群能保护自己不受网上的风险和挑战影响。

28. 但是，系统性竞争者如中国和俄罗斯持续倡导以更强势的国家主权控制网络空间可以解决安全挑战，这样的方法使我们在国际上面临竞争。全球的互联网自由正在减少，互联网作为共享空间、支持开放社会之间知识和商品交流的地位也逐渐受到威胁。

[9] 定义为《计算机滥用法》（Computer Misuse Act）的犯罪

[10] 英国国家统计局（ONS），《英格兰与威尔士的犯罪情形：截至2021年6月一年的数据》（Crime in England and Wales: year ending June 2021）（2021年）

[11] 数字化、文化、媒体和体育部，《2021年网络安全漏洞调查》（Cyber Security Breaches Survey 2021）（2021年）

对抗针对英国的网络威胁并威慑我们的对手

29. 近年来，我们在网络空间内和通过网络空间所面临的威胁不管是强度、复杂度和严重性都有所提高。针对英国的网络攻击者范围也不断扩大，包括国家行动者、犯罪集团（有时候是在国家的指导或默许下进行攻击）以及活动份子，其目的可能是为了间谍活动、商业利益、蓄意破坏和散布错误信息。这类攻击会造成重大的财务损失、知识产权盗窃、心理压力、服务和资产受到破坏，也对关键国家基础设施、民主体制和媒体构成风险。投资人和消费者的信心可能受到影响，现有的不平等和伤害也会加剧。在新冠疫情期间，性别暴力的问题也因为线上攻击而越发严重。勒索软件攻击也变得越来越复杂，造成的破坏也更糟。尽管在疫情期间恶意行动者造成的网络威胁的水平整体与之前一致，但他们利用疫情，将其网络行动转向窃取疫苗和医学研究，并让已经陷入危机的国家雪上加霜。远程工作和线上交易导致我们对数字技术更为依赖，这也增加了风险敞口。此外，数字鸿沟也导致线上服务无法触及所有人，使得数字素养较低、或不知道采取哪些网络安全措施保护自己的人群更容易遭受网路暴力和伤害。[12]

30. 政府已经采取步骤来对抗这些越来越严重的威胁。我们在情报能力方面进行的重大投资增进了我们对威胁的理解，让我们得以进行更有效的秘密反制行动。我们制定了一套针对网络犯罪的执法响应，由国家打击犯罪署主导，并在区域性组织犯罪处以及英格兰、威尔士、北爱尔兰和苏格兰当地警力中设置专门的网络团队。这提升了我们应对网络罪犯和其他对手行动的调查优势。通过开发英国数字身份识别和属性信任框架，政府也正在强化越来越多的数字身份识别解决方案的安全性。[13] 这将能帮助应对涉及身份数据滥用的犯罪。NCA的“网络选择”（Cyber Choices）项目帮助人民在更知情的状况下做选择，引导人们将网络技能用于积极、合法的地方，而不是用于犯罪。

31. 我们在攻击性网络能力的部分进行了重大投资，先是通过“国家攻击性网络项目”（National Offensive Cyber Programme），最近则是建立了“国家网络部队”（National Cyber Force，NCF）。NCF结合来自政府通讯总部（GCHQ）、国防部、秘密情报局（也称为“军情六处”）和国防科技实验室的各方人才，首次将这些人才纳入统一指挥之下。NCF在网络空间内和通过网络空间运作，保障国家的安全，同时维护和促进英国在国内外的利益。

[12] 国家网络安全中心，“网络安全意识”（CyberAware）
[13] 数字化、文化、媒体和体育部，《英国数字数字身份识别和属性信任框架》（UK digital identity and attributes trust framework）（2021年）

32. 我们与盟友共同协调，想办法提高网络空间中由国家资助的活动成本，就像在近期的SolarWinds和微软Exchange数据泄露事件中，我们对攻击进行归因，并让该为攻击负责的人承担后果。自主英国网络制裁体系的开发也是一项新的颠覆性工具，让我们能用来响应WannaCry和NotPetya之类的攻击事件。然而，虽然有上述举措和工具，我们的网络威慑方法似乎还没有在根本上改变攻击者对风险的计算。近期重大网络攻击事件的例子如下。

近期网络攻击事件的案例研究

在2021年，英国持续与全球伙伴合作，一同侦测并破坏共同的威胁，而这些威胁许多都是出自俄罗斯与中国。除了俄罗斯政府构成的直接网络威胁外，也发现许多针对西方国家发起勒索软件攻击的组织犯罪帮派多位于俄罗斯。中国在网络空间中仍然是经验丰富的行动者，有越来越强的雄心希望将其影响力拓展到国境之外，也有证据显示中国对英国的商业机密感兴趣。中国在未来十年的发展可能会是英国网络安全未来最大、唯一的影响因素。伊朗和朝鲜虽然不如俄罗斯和中国经验丰富，两国还是持续以数字入侵行为达到其目的，例如通过窃盗和蓄意破坏。

网络罪犯使用勒索软件攻击公共服务

勒索软件在2021年成为英国面临最重大的网络威胁。基于勒索软件成功攻击必要性服务和关键国家基础设施可能造成的影响程度，NCSC评估认为勒索软件的伤害程度有可能等同于国家资助的间谍活动。[14]

2020年10月，哈克尼区政府（Hackney Council）遭受勒索软件网络攻击，造成好几个月的混乱，重新整顿花了几百万英镑。当时正是应对新冠疫情的关键时刻，但攻击导致区政府被封锁，无法取得重要数据，还有许多服务中断，包括市政税和补助金的支付。其他地方政府和数个教育行业组织也遭受类似攻击。

[14] 国家网络安全中心，《缓解恶意软件和勒索软件攻击的影响》（Mitigating malware and ransomware attacks）（2021年）

2021年5月，一起针对爱尔兰卫生服务执行局（Health Service Executive，HSE）的勒索软件攻击破坏了爱尔兰的医疗IT网络和医院长达10天以上，对患者和家属造成实质的后果。有些被窃取的患者数据也被在网上公开。HSE作为爱尔兰医疗和社会服务的提供者，在同一天关闭其全国和区域性的网络以遏制该起攻击。爱尔兰卫生部的网络也侦测到恶意网络活动，但因为在调查过程中部署了相关工具，所以能及时侦测并阻止勒索软件的执行尝试。这起攻击也影响了北爱尔兰，导致有些跨境患者服务无法访问HSE的数据。

重要的是，在两起案件中都没有支付赎金。**执法部门并不鼓励、支持或容忍支付赎金的行为。就算你支付了赎金：**

- **还是无法保证你能访问你的数据或使用你的电脑**
- **你的电脑仍是受到感染的状态**
- **你将付钱给犯罪集团**
- **你未来更有可能成为攻击目标**

NCSC发布了指南，说明组织如何抵御恶意软件和勒索软件的攻击，包括如何为事件作准备，或是组织已经受到感染时能采取哪些步骤。

国家利用战略脆弱性和供应链

软件公司SolarWinds受到攻击和微软Exchange服务器被滥用两起事件凸显了来自供应链攻击的威胁。在这些高度复杂的事件中，攻击者专门攻击经济供应链中安全性较低的元素（例如托管服务提供者或商业软件平台），NCSC目前所观察到最严重的网络入侵则是攻击政府和国家安全机构。

在2020年12月初，美国网络安全公司FireEye发现有攻击者在一项他们自己和世界各地许多组织都使用的产品中加入了恶意变更。这项变更让攻击者能发送管理员层级的指令给所有受感染的产品安装版本，这可以用来进一步攻击相连的系统。最初的供应链攻击是通过一个叫Orion的软件执行的，Orion是**SolarWinds**公司所开发的IT网络监测工具。攻击者早在2020年3月就在该软件的一个更新文件中植入了恶意代码。在2021年4月，NCSC与美国的同等安全机构首次揭露，这起近期最严重的网络入侵攻击的幕后黑手是俄罗斯对外情报局（SVR）。[15] SolarWinds证实全世界18000个组织（包括美国政府部门）都受到影响。SVR先前曾尝试入侵北约成员国和欧洲政府的IT网路，而这起事件便是其广泛入侵行为的一部分。

[15] 外交、联邦和发展事务部（FCDO），俄罗斯：《英国和美国揭露俄罗斯秘密情报服务所进行的恶意活动》（UK and US expose global campaign of malign activity by Russian intelligence services）（2021年）

2021年3月2日，微软公开表示高度复杂的行动者攻击了数个**微软Exchange**服务器，世界各地的组织使用这些服务器来管理其电子邮件、日历排程和共同协作。根据微软评估，初步的入侵早在2021年1月就开始，且背后有中国政府资助。为了回应攻击，微软为受感染的服务器发布了多个安全更新。2021年7月，英国加入了其他志同道合的伙伴，确认了中国政府资助的行动者对全世界超过25万个服务器进行网络攻击。[16] 这起攻击非常可能支持大规模间谍活动，包括获取个人身份识别信息和知识产权。微软Exchange服务器受创让犯罪者得到了立足点，得以进一步攻击IT网络中的其他受害者。在攻击发生时，政府快速向受影响的组织提供了建议和推荐的行动，微软表示到三月底之前，92%的客户已完成针对该弱点的安全补丁。

[16] 外交、联邦和发展事务部（FCDO），《英国和同盟追究中国政府的广泛黑客行为》（UK and allies hold Chinese state responsible for a pervasive pattern of hacking）（2021年）

改变的驱动因素

33. 接下来十年间，**数据和数字互联互通将会持续拓展到我们生活的几乎每一个方面**。数据和数据使用所依赖的基础设施支持着网络接入和使用的大幅增长，这正在创造新市场，也增加便利性、选择和效率。但这也让国家更依赖互联的数字系统，让恶意活动和重大的“实质”影响有机可乘。随着关键和非关键的技术越来越跨领域趋同，这些风险也散布到经济中的新领域，将数据和服务移动到云上、而且常常是移至英国境外，这又进一步增加我们风险敞口。

34. 我们看到受管制行业（如电信、能源等）中的成熟企业和新的、非管制企业之间有越来越多的互动，后者包括提供微型发电、电动车充电或“互联场所”能力的企业。关键基础设施未来将会更为去中心化和分散，我们依赖的关键功能和服务的安全性会如何受到监管影响，这也会有根本上的改变。此多元化的发展也会影响到更广泛的国家安全，不管是为了执法或为了网络安全，信息的获取都会变得更困难。这样的环境改变也会更广泛地影响到传统关键国家基础设施以外的产品和服务。

35. 越来越复杂的格局会让国家政府、企业和社会更难以理解所面临的风险或该如何自我保护。对第三方托管服务供应商与日俱增的依赖也创造了需要解决的新风险，这些第三方供应商通常有访问上千个客户IT系统的权力。各种装置和网络连接到互联网慢慢成为了标准，网络空间也逐步延伸到我们的家中、车辆、建成环境和工业基础设施中。传感器、可穿戴设备、医疗设备、生物信息等技术会进一步模糊线下与线上活动之间的界线。网络风险将会无所不在，随着个人和敏感信息数据量增加，系统受到攻击泄漏信息的风险也跟着上升。

36. 在此背景下，当高端网络能力商品化并为越来越多国家政府和犯罪集团所用，**网络空间的威胁将持续演变和多样化**。在网络空间中有能力和意图要攻击英国的行动者将会增加，各个国家政府也会采用各种手段来进行破坏性活动，包括使用代理行动者。在疫情之下，办公模式迅速转向混合模式、国际旅游也受限，导致对数字服务依赖程度增加，刺激组织犯罪集团转向网络犯罪。我们已经开始看到这个趋势的迹象，最近期的犯罪调查估计，网络犯罪在2019年到2021年间显著增加。[17] 这并非英国独有的挑战，只要依赖网络都会有这项弱点。

[17] 国家统计局，《英格兰与威尔士的犯罪情形：截至2021年6月一年的数据》（Crime in England and Wales: year ending June 2021）（2021年）

37. 随着国家政府和非政府行动者在网络空间内和通过网络空间建立战略优势，**网络空间的竞争也会越发激烈。**在未达武装冲突门槛和冲突前的情境中，网络作战行动对力量投射的重要性将会越来越高。未来的冲突中，网络能力的使用也会增加。英国如果要采取有效行动，国防能力中必须要具备高度的网络韧性。网络作战行动将需要与其他军力元素整合，才能打败威胁并赋能更广泛的国防活动。如《国家太空战略》所述，太空也将逐步成为重要活动领域，这将开启新的风险领域，同时创造机会让英国利用其网络能力建立新优势。[18]

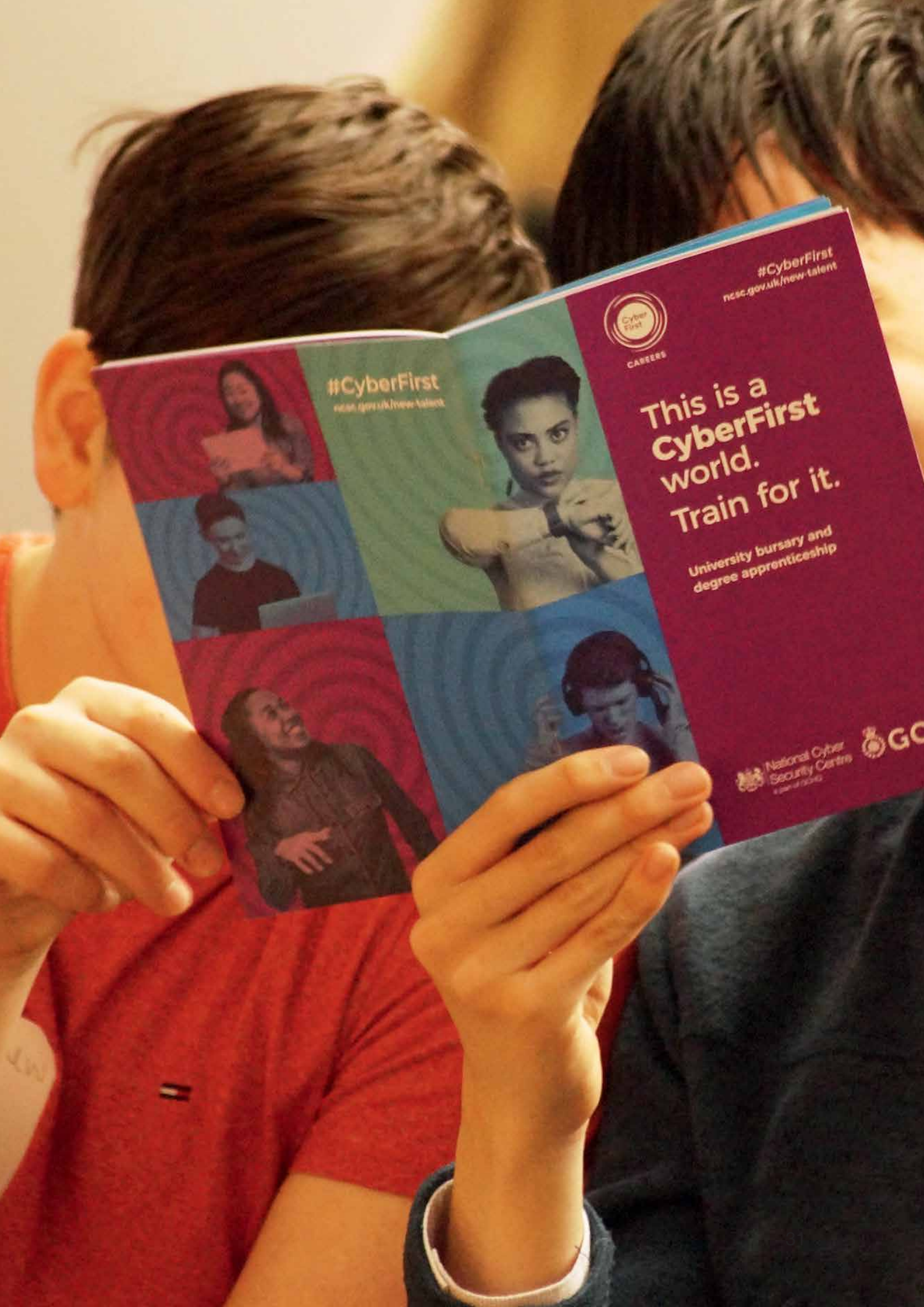
38. 与治理网络空间规则相关的辩论将逐渐成为**大国彼此进行系统性竞争**的场所，其中一方是想要维持一个基于开放社会的系统的国家，另一方则是中国与俄罗斯这样的系统性竞争者，主张更强大的国家控制是唯一能维护网络空间安全之道，两者之间必定将发生价值冲突。当国家政府、大型科技公司和其他行动者主张互相竞争的技术标准和互联网治理，自由开放的互联网将面临压力。

39. 大国之间互相竞争控制快速演变的技术格局也会导致此一情势加剧。随着数字技术与我们的日常生活、企业和基础设施整合程度提高，有些技术现在对社会运作具有不可或缺的关键性。在科技方面具有战略优势、拥有数据可以驱动创新的国家将会掌握更多的权力，他们将可以对其他国家施加其影响力，并塑造有利于自身经济和政治利益的全球标准。

40. 数字孪生、量子计算和大规模自治系统等**新兴技术**和其中生成的信息将会创造新的机遇和风险，为攻击者和防御者开启新的网络能力，就像加密货币被勒索软件帮派所利用一样。技术领导力将更为分散，英国将无法在所有重要科技领域都发展主权能力。国家和企业利用技术标准以维护自身利益，风险在于关键技术有可能被价值观与我们迥异的国家所主导。

41. 有超过十年的时间，英国一直秉持一套宏大的国家网络战略，并持续进行高水平投资，建立了英国作为网络全球领导者的地位。从上述分析可以明显看到，重大的挑战和机遇仍然存在。将在下文中概述英国国家回应。

[18] 英国政府，《国家太空战略》（National Space Strategy）（2021年）


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

英国国家回应

42. 在此战略环境中，英国必须做出选择。在越来越复杂的网络空间中，我们可以把目标设定为和我们面临的威胁与挑战保持相同步调，巩固过去五年的进展并尽可能应对最急迫的问题。这个方法有两个风险。第一，我们没有完全发挥英国的网络潜力来支持国家优先事项的发展，也会错失机遇。第二个更严重的风险是，我们可能到达一个技术的转捩点，才发现能够影响未来经济和社会基础的主导权掌握在竞争者和对手手里，而我们需要更努力才能确保自身安全。

43. 我们的判断是，随着网络空间对于我们与盟友和对手的利益都有越来越根本性的影响，**培养我们在网络空间中的竞争优势有战略必要性**。这将让我们不仅可以确保现在的安全，也能塑造未来的有利局面。

我们的愿景、目标和原则

44. 我们的愿景是，英国在2030年将仍然是**领先、负责和民主的网络强国，有能力在网络空间内和通过网络空间保护和促进本国的利益，支持国家目标**。

45. 为了实现这个愿景，我们将贯彻五项战略目标。各项战略目标分别要加强英国在五个网络力量维度中的国家实力，整体来说，五项战略目标旨在提升我们的能力，以维系一个能够反映英国价值和利益的网络空间。这五个目标（或者支柱）形成引导我们活动的战略框架，第二部分将阐述每个目标在2025年前要采取的行动。

- **支柱一：加强英国网络生态系统**，对人才和技能进行投资，并深化政府、学术界和产业界之间的合作关系
- **支柱二：建设一个富有韧性和繁荣的数字英国**，降低网络风险，让企业能够最大限度地获得数字技术带来的经济效益，让公民在网上更安全，对自己的数据受到保护更有信心
- **支柱三：引领对网络力量至关重要的技术**，发展我们的产业能力并建立框架以保护未来技术
- **支柱四：提升英国的全球领导力和影响力，建立更加安全、繁荣和开放的国际秩序**，与政府和行业伙伴合作，分享支撑英国网络力量的专长
- **支柱五：侦测、瓦解和威慑我们的对手，在网络空间内和通过网络空间加强英国的安全**，更加整合性地、创造性地和常规性地利用英国的各种手段

46. 这些目标应该能互相强化。举例来说，在国内达成更高水平的网络安全和韧性会是在国际上更活跃发展的必要基础。此外，我们的全球化供应链和来自海外的威胁意味着如果没有主动塑造国际行动者的行为，我们将无法保证自身的安全。还有我们影响网络空间、互联网和技术相关国际辩论的能力将会依赖我们的技术优势和创新生态系统的建设，这样的系统才能在最关键的技术领域带来真正的优势。

47. 对我们的愿景至关重要的是**要促进自由、开放、和平而且安全的网络空间**。我们对于网络力量的战略聚焦并不是要在冲突上火上浇油，也不是准备要让英国在一场零和游戏中取胜。如同《整合评估》中所提出的，一个开放的社会和经济能蓬勃发展的世界是我们未来的繁荣、国家主权和安全的最佳保障。英国将会与志同道合的国家合作，一同推广开放和民主的共享价值观，追求以**负责、民主的方法建立网络力量**。这意味着在努力实践五项战略目标时，我们将应用以下**原则**：

- 我们将优先建设公民和企业在网络空间中能安全、有保障地运作的能力，让他们可以最大限度地获得数字技术所带来的经济和社会效益，并行使其法律和民主权利

- 我们将尽力维系一个开放、可互操作的互联网，将其作为支持全球繁荣和福祉的最佳模范，抗拒威权国家意图分裂互联网的压力和其互联网国家主权的概念
- 我们会以合法、恰当和负责的方式使用网络能力，配合明确的监督和与民众及盟友的互动参与，若在网络空间中有鲁莽或轻率的行为，我们会向彼此问责
- 我们将对网络空间的犯罪使用采取一切可用的行动，揭露使用犯罪代理或在其领地藏匿犯罪组织的行动者，努力阻止高端网络能力向罪犯扩散
- 我们将会提倡以包容、多重利益相关方的方法来进行关于网络空间和数字技术未来的辩论，拥护网络空间中的人权，并对抗倾向数字威权主义和国家控制的发展

我们方法的关键调整

48. 在许多领域，我们的战略都是以现有的方法为基础，在必要时进行提升、扩展或适应调整。下文将简述这份战略与《2016-2021年国家网络安全战略》的主要差异，这反映了我们更广泛的雄心，希望巩固英国作为一流网络强国的地位。

49. 承诺让英国保持在网络科技的最前沿。政府将在未来三年间在网络和老旧IT系统方面投资26亿英镑。这是在《2020年支出审查》(Spending Review 2020，SR20) 中所宣布的国家网络部队重大投资之外的另一项投资。这包括在国家网络安全项目中增加1.14亿英镑的投资。此外，在研发、情报、国防、创新、基础设施和技能方面投资金额皆有增加，所有方面都将对英国的网络力量产生贡献。SR20和《2021年支出审查》所宣布的网络投资金额远远超过前一份战略所承诺的五年19亿英镑。[19]

50. 更全面的国家网络战略。网络安全仍然是这份战略的核心，但这份战略进一步结合了英国政府内和外所有的能力。本战略更强调关键技术和基础设施，这些是网络空间的基础，也支持着英国网络企业在国内的增长和在国际上的竞争，还有助于升级国际行动以塑造和影响网络空间的未来，并将攻击性网络融入为手段的一部分。这需要真正团结一致的国家战略方法。本战略将领导和协调责任分配给所有国务大臣，也与分权政府有更紧密的合作。这需要依赖我们成功地协调政府部门间的工作，而这正是英国的关键优势之一。

[19] 英国财政部，《2021年秋季预算和支出审查》（Autumn Budget and Spending Review 2021）（2021年）

51. 全社会的努力。我们的目标是希望国家战略方法是由全英国的组织共同塑造的成果，并能帮助引导这些组织的决策，同时提供与英国国内外伙伴合作的坚实基础。要实现这个目标，我们尚需努力。短期行动包括：(1) 建立新的国家网络顾问理事会（National Cyber Advisory Board），邀请私营和第三部门的高级领袖来挑战、支持和影响我们的方法；(2) 调整我们的网络行业创新项目方向，以往的倡议通常规模较大且以伦敦为中心，未来将会以区域交付的模式为主，与地方的产业、创新者、执法部门和学术界合作建立；还有 (3) 采取步骤增加网络劳动力的多元性，认知到能够驾驭和培养这个人口的技能和人才对于国家安全至关重要。这份战略在制定的过程中听取了北爱尔兰、苏格兰和威尔士分权政府、产业、执法部门、监管方、学术界、公民社会和国际合作伙伴的意见。我们计划在战略实施期间保持这些开放的对话。

52. 更积极地培养和保护我们在网络空间关键技术中竞争优势。《整合评估》和后续战略已经在人工智能、量子技术和数据等领域以此态度开始推进。这份战略进一步在安全的微型处理器设计、运营技术的安全性和密码学方面做出承诺。战略宣布成立运营技术安全国家实验室作为新的卓越中心，聚焦于和产业和学术界合作共同建设最高水平的网络韧性。也宣布要扩大国家网络安全中心（NCSC）的研究能力，包括曼彻斯特新的应用研究中心，以互联场所和交通运输等新兴技术为主要研究重心。我们成功地推广“设计即安全”方法，推动新技术在建设过程中就融入安全性，这也为这份战略奠定了基础。这将意味着在必要时投资和更多地使用监管和立法手段，以形成更多元、安全和有韧性的供应链，就如同我们在电信行业所做的一样。

53. 以政府为首，大幅强化我们推广网络安全的核心工作。我们将在对政府网络安全进行快速的全面改造、为政府部门设定明确标准和解决老旧IT基础设施等方面的工作投入前所未见的大额投资。政府的关键职能将在2025年前大幅强化，接着我们会确保整个公共部门的所有政府组织在2030年前对已知的弱点和攻击方法具备韧性。我们会做更多保护和与公民参与互动的工作，同时尽可能减轻他们的负担。我们将会加固数字环境，保护公民不受网络犯罪和欺诈的侵扰，要求制造商、零售业者、服务提供商、和公共部门负起更多提升网络安全标准的责任。通过将整个经济中的监管和激励机制进行对标，并提供更多支持，我们将会提高私营部门对网络韧性的投资和参与水平。我们也将更重视供应链风险，将测试一系列的干预措施来帮助组织管理其供应商所带来的网络安全风险，确保整个供应链都能采用最佳实践。

54. 更加整合和可持续的行动计划以瓦解及威慑我们的对手，并保护和促进英国在网络空间中的利益。这些行动计划将会运用政府各部门的外交、政策和行动手段。国家网络部队（NCF）的设立与扩张将对这些行动计划产生重要支持作用，NCF的据点将设置在兰开夏郡（Lancashire）的萨姆斯伯里（Samlesbury）。我们将更常规地运用NCF的能力来破坏来自其他国家和非政府行动者的威胁，并支持英国更广泛的国家安全利益。我们的行动计划也将受益于为国家、区域和地方各层级执法部门培养高端能力的一项重大新投资。这将帮助我们应对勒索软件和越来越创新的网络罪犯所带来的重大威胁。我们也将持续运用英国的自主网络制裁体系和归因流程，让对手付出代价，并点名恶意和鲁莽攻击背后的始作俑者。

55. 将网络力量放在英国对外政策议程的核心，并认知战略的每个部分都需要国际参与。我们会强化英国与核心联盟的关系，并与更多国家互动，共同对抗数字威权主义的扩散。在接下来几年，我们将会增加对于合作国家的国际项目投资，帮助建立他们的韧性、提高他们抵御网络威胁的能力。我们也会更妥善利用国内的各种优势，包括行动和战略沟通专长、思想领导力、贸易关系和产业合作，来支持我们的国际目标。

英国的角色和责任

56. 我们的战略核心是要对网络采取一种“全社会”的态度。我们需要在公共、私营和第三部门之间建立持久、平衡的合作伙伴关系，每个部门都扮演重要的角色影响国家的工作。

公民

57. 这份战略旨在尽可能消除公民所承受的网络安全负担，但我们所有人都还是有着关键的角色。尽管政府会竭尽所能地在网络攻击对人民造成伤害前就阻止攻击，但还是会有些行动者会设法避开这些保护措施。我们都能采取行动来保护实体和虚拟世界中重要资产的安全。[20] 这意味着尽个人的责任，采取所有合理的步骤来保护硬件（智能手机和其他设备）还有数据、软件和系统，这些让我们在私人和职业生活中能享受自由、弹性和便利。为了对此提供支持，政府会提供技术上准确、及时而且能转化为行动的建议。公民社会组织和社区团体也扮演着重要的角色，支持人们了解网络风险并学会自我保护。例如，许多慈善组织为弱势族群提供针对性的支持、建议和提高意识的信息与活动。

[20] “网络意识”是政府关于网上安全方面的建议

企业和组织

58. 企业和组织有责任确保他们有效地管理其网络风险、具备网络韧性，而且能够支持使用其服务的客户和人民。企业和组织的运营、创新和增长越来越依赖数字技术。这虽然提升了服务水平，但也创造了新的风险和挑战，例如企业和组织负责的个人数据和数字资产量不断增加。这意味着他们有责任保护这些数据和资产，同时维持服务。如果做不到，组织可能遭受重大的声誉风险和经济损失，他们的客户也会受到伤害。必要性服务的运营商和关键数字技术的提供商有具体责任，要应对他们面临的网络风险和履行《网络与信息系统监管条例》（《NIS条例》）中明定的义务。NCSC的建议和指导支持所有企业和组织，帮助他们保护信息、资产和系统。信息专员办公室（Information Commissioner's Office，ICO）也会为组织提供建议，协助其履行《英国通用数据保护法》对所规定的网络安全义务。

网络安全行业和大型技术公司

59. 英国蓬勃发展的网络安全行业扮演重要角色，对英国面临的新兴网络威胁和挑战做出回应。互联性产品的快速普及和企业与组织加速的数字转型提供了机会，让行业能增长和创兴，并提供新的服务和产品。这份战略描述政府将如何继续支持英国网络安全行业的发展，并在维系和强化合作关系的过程中受益于行业的能力与专业技能。我们也希望加强与学术界、广泛的技术社群和私营领域等多方合作，确保我们全面运用英国的技术专业技能和知识。

60. 提供数字服务的大型技术公司扮演着重要的角色，确保英国的企业和组织能在安全的环境中运营。托管服务提供商和整合大量活动的平台企业尤其如此。他们需要确保所提供的服务"默认即安全"，不能单纯依赖客户采取保护行动。大型技术公司也有特别重要的责任去优先建设其网络韧性。随着企业、政府和更广泛的社会越来越依赖云和线上服务，独特的新脆弱性和相互依赖性也应运而生。

政府

61. **英国政府**具备独特的地位，可以收集必要的情报以理解最复杂的威胁、制定和执行法律、设定国家标准，和对抗恶意行动者的威胁，包括执行攻击性网络作战行动。通过这份战略，我们将投资加强我们国家的网络能力。政府部门和公共部门机构也有责任保护自己的网络和系统。作为重要数据的持有者和服务提供者，政府采取严格措施保障其信息资产。最后，政府重要的角色还包含为公民、企业和组织提供建议和信息，让他们知道如何在网上自我保护。在必要时这包括设定标准，并期待关键企业和组织为了保护我们所有人会遵守相关标准。

62. 网络政策的绝大部分和这份战略所列出的多数措施与保留事务相关，例如国家安全、外交事务和国防、电信通讯、产品标准与安全，以及消费者保护。但这份战略和制定与实施仍然需要依赖**北爱尔兰、苏格兰和威尔士权利下放政府**的意见、行动和投资。特别是在地方分权的政策领域，这些主要位在战略的“生态系统”和“韧性”两大支柱中，例如教育、治安维护，以及特定关键行业的网络韧性，其中也包括分权政府本身的公共部门。英国四大地区之间的协调与配合是确保能在全国带来更强影响力的必要因素。这需要内阁办公室和其他政府部门及早且定期与其威尔士、苏格兰和北爱尔兰的同等机构共享优先事项和计划信息。这也会帮助避免重复劳动，并从公共资金中获得最大价值。分权政府将会继续制定各自的网络战略和计划，并与这份英国政府战略对标。

国家网络安全中心

“帮助将英国打造成能在网上安全生活和工作的地方”

国家网络安全中心（NCSC）于2017年正式启动，作为GCHQ的一部分，旨在成为英国网络安全环境的国家权威：共享知识、应对系统性脆弱性，以及在关键国家网络安全议题上提供领导力。[21] NCSC的成立简化了政府的运作结构、提升了英国响应国家级网络事件的能力，并启动了创新数字服务的推出，这些服务以自动化的方式维护组织和个人在网上的安全。

为了确保NCSC能应对接下来十年的挑战，我们明确指出支持其工作的持久性能力和属性、以可持续的方式提供基金支持，并根据过往运营经验，将NCSC的能力聚焦使用于在国家规模能有最大影响的地方。

支持NCSC工作的持久性能力和属性包括：

- 英国所需要的网络安全学科和专业领域中世界一流的技术专业技能；
- 能够理解影响英国利益现存和潜在的网络威胁（意图和能力）的敏锐洞察；
- 英国所有支持网络安全目标的国家安全能力和权威的使用权；
- 联合学术界、产业和国际合作伙伴与网络安全社群建立直接关系；
- 密码学方面的能力，这对保障英国在全球的利益至关重要。

在新的战略中，NCSC的主要职责如下：

- **采取直接行动降低针对英国的网络伤害**，手段包括：通过数字服务（例如：主动网络防御（Active Cyber Defence））提供大规模的保护、驱动技术变革、管理对有国家级重要性的网络事件响应，还有与国家网络部队（NCF）一起直接对抗对手的网络作战行动。

[21] 英国政府，《2016-2021年国家网络安全战略》（2016年）：段落1.9

- **支持英国社会的各个部分自我保护**，手段包括：提供定制化的专业技能和独特的知识，让全英国的公民、企业和组织能用来保护自己，并协助让英国成为一个大家在网上都能更安全的国家。
- **在网络安全最重要的议题上为英国政府的政策和监管提供技术意见**手段包括：利用NCSC的核心能力为英国中央政府的政策制定者提供权威的技术意见和威胁评估、支持政策与监管的制定与实施以确保英国公民、组织和利益的数字安全。
- 通过NCSC的国家加密关键能力中心（National Crypt-Key Centre）**提供英国主权能力**，国家加密关键能力中心保护英国军方和国家安全社群所依赖的关键信息和服务，包括抵挡最强大对手的攻击。
- **支持增加网络技能和投资**，这是通过为每个层级的网络教育提供技术支持，并与产业参与互动与支持，催化进到网络行业的投资。

NCSC也会对**进度评估**做出贡献，通过“NCSC评估”（英国的编辑独立网络评估职能）来了解这份国家网络战略各项目标的进展。

国家网络部队

国家网络部队（NCF）成立于2020年，负责在网络空间内和通过网络空间的运作，对抗、破坏、削弱和反对伤害英国和其盟友的行动者，保障英国的安全，并在国内外保护和促进英国的利益。NCF的组成大致上是国防和情报部门各半，将各自的专业技能、资源和权威机构统合到一个单一指挥架构下。部队的总部将设置在兰开夏郡的萨姆斯伯里。

NCF以国家安全为目的交付其工作，例如为国防、英国的经济福祉和重大犯罪预防工作提供支持。NCF的活动从战术性质到战略性质皆有，对象包括国家政府和非政府行动者。其工作主要分为三大类：

- 在恐怖分子、罪犯和国家政府利用互联网跨境伤害英国和其他民主社会时抵御威胁
- 对抗破坏网络空间中数据和服务的保密性、整体性和可用性的威胁（意即支持网络安全）
- 贡献于英国的国防行动，并帮助交付英国的对外政策议程（例如：干预人道主义危机以保护一般民众）

NCF的行动可用于影响个人和团体、干扰线上和通讯系统，以及削弱实体系统的运作。这类活动通常被称为攻击性网络（offensive cyber，OC）。

NCF的行动符合成熟的法律框架，包括《1994年情报服务法》（Intelligence Services Act 1994）和《2016年调查权力法》（Investigatory Powers Act 2016）。英国之前已经表明其能力的开发和部署都是符合国际法律，在适用情况下也包括武装冲突法。其活动需要经过部长批准、司法监督和国会审查，所以英国的网络作战治理体制是世界上最稳固的治理体制之一。

英国并不会定期谈论个别网络行动，但NCF可能进行的网络作战行动包括：

- 通过破坏恐怖组织的指挥和控制通讯和限制极端主义媒体散布，阻止恐怖组织计划
- 通过削弱对手武器系统减少对英国军队的伤害风险
- 通过对抗试图破坏选举的组织国家假消息行为，捍卫民主、自由、开放的选举
- 通过破坏犯罪集团的线上平台和服务使用，阻止犯罪集团从其活动中盈利
- 通过瓦解规避国际制裁的行为，协助其获得国际制裁
- 通过瓦解对手进行网络攻击所使用的基础设施，保护英国和其他国家不遭受该攻击影响
- 通过维护一般民众获取关键信息的能力，在人道主义危机中保护一般民众

作为在网络空间内和通过网络空间行动的国家卓越中心，NCF将会转化英国开发、整合和运用这些手段的能力，并配合优化其他能力以交付成效。

执法部门的国家网络犯罪网络

执法部门的国家网络犯罪网络成立于《2016-2021年国家网络安全战略》期间，该网络已经开发了针对网络犯罪的整合响应，准备好交付情报导向的响应以应对针对个人、组织或整个行业各种形式的网络攻击。这是在国家、区域和地方层级运营的全国性系统。该系统提供受害者关怀、帮助保护企业和个人并支持其快速康复，并追求让加害者面临刑事责任。

国家打击犯罪署的国家网络犯罪处（National Cyber Crime Unit，NCCU）提供国家级领导力并协调事件响应，在英格兰和威尔士的九个警察辖区还有专门的**区域网络犯罪处（Regional Cyber Crime Units，RCCUs）**网络，与苏格兰和北爱尔兰警察的同等部门以及大都会警察服务的网络犯罪处也都共同为NCCU提供支持。

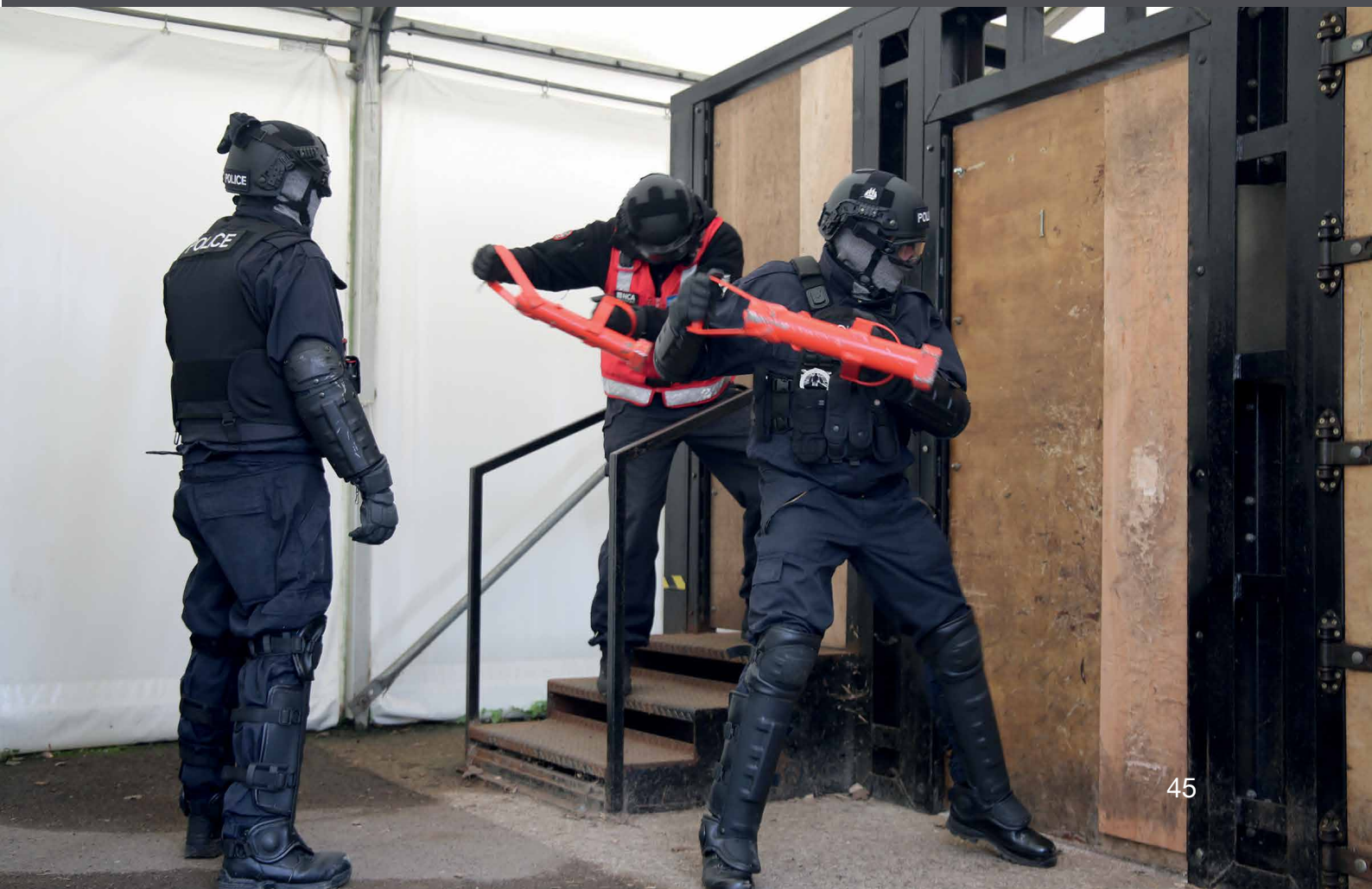
以上还进一步得到专门的**地方网络犯罪处（Local Cyber Crime Units，LCCUs）**的补充，LCCU嵌入在43个警力辖区中，并由区域层级的协调人统一协调。这些区域和地方的CCU能调查并追捕犯罪者、协助企业和受害者保护自己不受攻击，以及与合作伙伴共同防范弱势族群遭受引诱而犯下网络犯罪。

集中化的犯罪举报、分级和分析则由**伦敦金融城警方**下属的**反诈骗行动处（Action Fraud）**负责。最严重和/或复杂的案件会进一步转介交由NCA和区域网络进行追捕，其他案件则分派给地方警力。伦敦金融城警方也负责协调受害者支持，包括通过**经济犯罪受害者关怀处提供服务。**

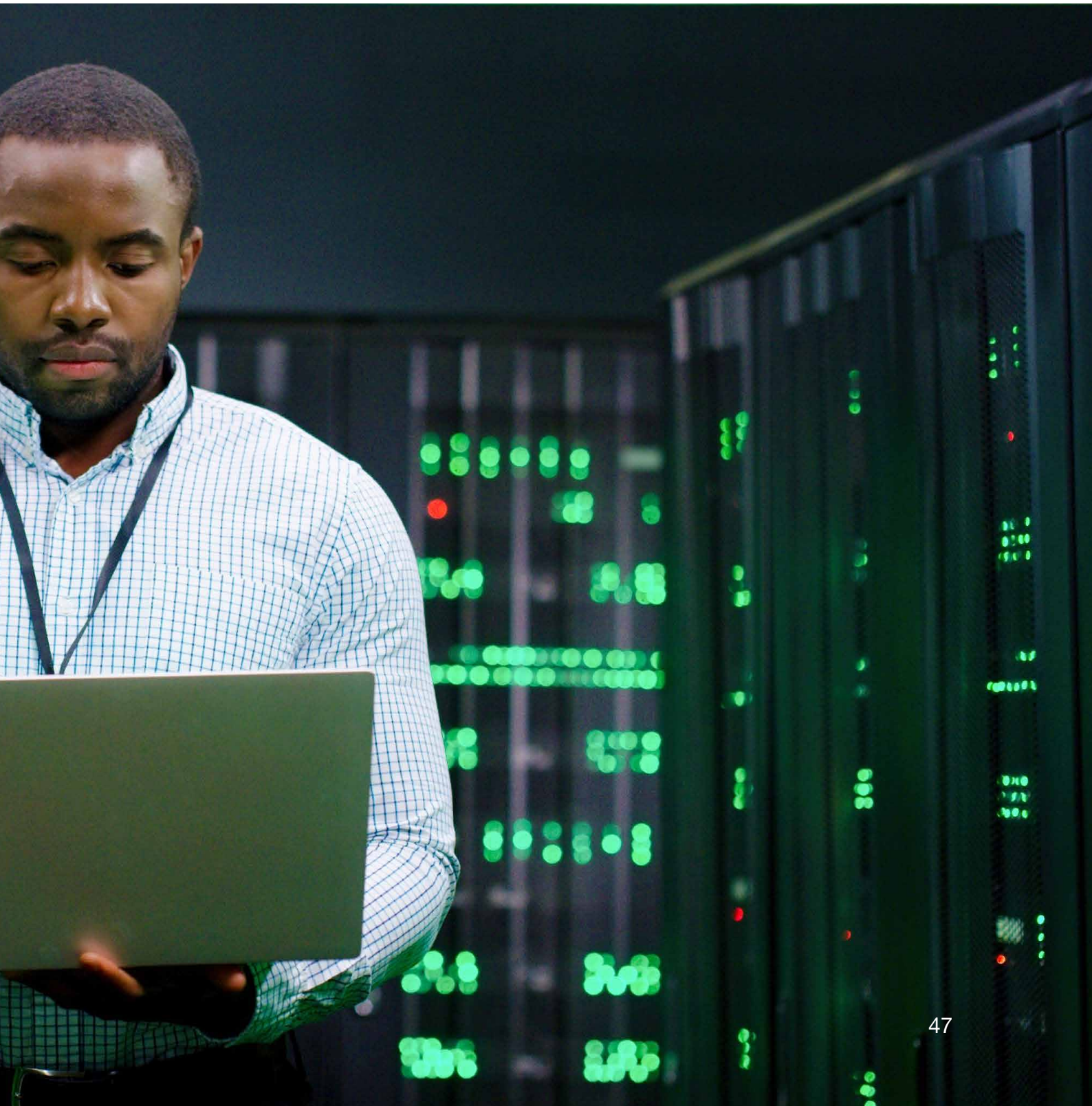
不同的系统现在与提升的鉴识、情报和数据共享等能力进行结合，建立单一个平台，让国家和区域的各个部门都能获取新开发的高端专业能力和工具。这包含与安全和情报社群的合作伙伴有效协作的能力，尤其是在响应混合式犯罪和国家威胁时。贯彻“一次做好全国性建设以造福整个网络犯罪网络”的原则，这些能力也可以通过区域性协调人为地方网络犯罪处所用。这整套系统已经交付了显著提升的网络犯罪威胁响应。

网络犯罪网络的执法部门将会持续驱动我们对于网络空间恶意活动的刑事司法响应，无论威胁的行动者是在国际、国家、区域还是地方层级。上述手段还有以下其他破坏方法补充，包括但不限于：

- 发展专业高端调查和破坏性网络能力
- 运用NCA广大的国际网络来支持合作国家基于情报和证据的干预措施
- 通过破坏犯罪集团的犯罪市场和相关服务使用，阻止犯罪集团从其活动中盈利
- 通过削弱和破坏对手进行网络攻击所使用的基础设施，保护英国和其他国家不遭受该攻击影响
- 贡献于针对高端犯罪者的制裁和公开归因
- 冻结作为网络犯罪和加密货币和其他资产



第二部分：
实施计划



支柱一：英国网络生态系统

加强英国网络生态系统

63. 为使这一战略取得成功，我们需要确保英国拥有合适的人才、知识和合作伙伴。我们必须拥有技术水平较高的多元化劳动力、充满活力的研究社区、具有国际竞争力的网络行业和蓬勃发展的区域创新生态系统，使我们能够在关键技术领域处于领先地位。而这一切都建立在政府、行业和学术界之间更强有力的伙伴关系之上。

64. 网络生态系统的发展需要依靠自我维持，而不是政府干预。在这一战略的实施期间，我们将从资助一系列以定制和集中管理为主的技能和创新项目，转向更为可持续的、系统性的和区域性的方法。我们会在政府更广泛的技能和教育体系改革的基础上，支持和激励更多的人获得从事网络职业所需的技能。我们也会优先采取一系列具体行动，以增加网络劳动力多样性。这不仅是为了确保这些工作和职业向所有人开放，也是我们国家安全的关键任务，保证我们利用整个人口的才能和技能。我们还会保证网络行业的增长惠及整个英国，不仅限于伦敦和东南部。据估计，这两个地方占网络行业就业的45%，占外部投资的85%。[22]

65. 总体而言，我们将发挥更具战略性的作用，促进行业领袖、学者、创新者、执法机构、国家安全社区和其他希望通过合作增强英国应对网络威胁的韧性的各方聚集在一起。我们将协调政府的所有手段来支持网络生态系统，从学校如何教授网络到经济法规如何提高标准，确保英国培养保护自己免受未来威胁所必要的关键能力。

[22] 英国数字、文化、媒体和体育部（DCMS）《2021年网络安全部门分析》（Cyber Security Sectoral Analysis 2021）

目标1：
加强支持全社会网络方法所需的结构、伙伴关系和网络

66. 网络力量需要全社会的参与。我们的竞争优势将来自我们在英国培养和利用人才的能力，让整个公共部门、行业和学术界的合适的人员用正确的方式合作，将整个网络社区团结在一起。我们将需要与行业建立真正的整合交付伙伴关系，保证整个英国的各个地区采取广泛的地理位置方法，与北爱尔兰、苏格兰和威尔士的分权政府密切合作，抓住网络力量带来的实现均衡发展的机会。到2025年，我们将实现以下成果：

67. 通过建立一个全新的高级别国家网络咨询委员会，在已然强大的网络增长和韧性伙伴关系网络以及网络安全研究和教育卓越学术中心的基础上更进一步，与行业、学术界和公民开展 **更具包容性和战略性的国家网络对话** 。

68. 在整个英国建立更加整合和有效的区域网络，使政府、企业和学术界之间的伙伴关系更加牢固，以支持行业增长和商业韧性。我们将同区域网络集群以及最近成立的英国网络集群协作组织（UKC3）、日益增加的区域网络创新中心和网络韧性中心合作，加强当地企业、卓越学术中心和执法部门之间的联系。

69. 这些步骤将建立在国家网络安全中心（NCSC）及其利益相关方之间，在政府部门、独立机构及其所代表的经济领域（包括CNI和监管机构）之间的现有关系之上，也建立在政府与行业、数字和技术领域之间更广泛的对话的基础之上。

ScotlandIS网络负责人希亚拉·米切尔 (Ciara Mitchell)

希亚拉也是苏格兰网络集群的管理人以及UKC3的成员。

“苏格兰网络集群在支持苏格兰网络安全社区方面发挥了关键作用。人们日益了解苏格兰在集群管理方面的专业知识，以及建立在蓬勃发展的网络行业基础上的发展机会。随着集群的价值日益受到认可，我很高兴在全新的英国网络集群合作组织中担任生态系统发展主管这一关键的职位。通过UKC3，我们将更加聚焦于合作、创新和技能发展，为英国网络安全部门的发展提供一个平台。”

网络组织 （各地理位置代表性组织）

英国网络集群

1. 布里斯托尔和巴斯网络
2. 北方网络
3. 威尔士网络
4. CyNam（切尔滕纳姆网络）
5. 英格兰东部网络安全集群
6. 英格兰中部网络
7. 苏格兰网络
8. 西南网络安全集群
9. 约克郡网络安全集群
10. NI网络（北爱尔兰）
11. 西北网络安全集群
12. 英格兰西部网络集群

网络安全教育卓越学术中心

网络安全研究卓越变革学术中心*

英国政府通信总部（GCHQ）/
英国国家网络安全中心（NCSC）站点

分权政府组织

*红点和黑线表示网络安全中心和网络安全研究

1 东北部商业韧性中心

2 西北部网络韧性中心

3 英格兰中东部网络韧性中心

4 英格兰中东部网络韧性中心

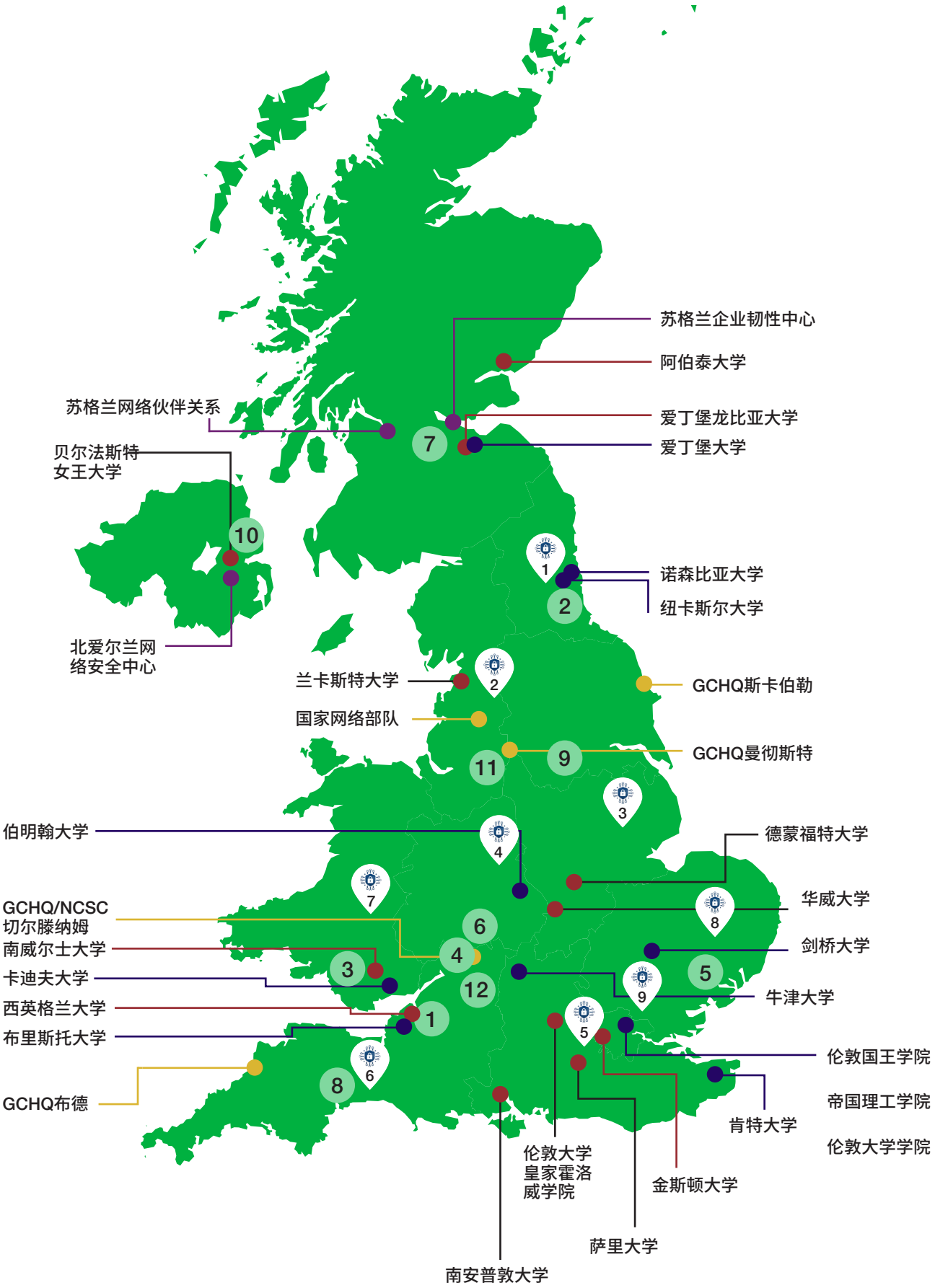
5 东南部网络韧性中心

6 西南部网络韧性中心

7 威尔士网络韧性中心

8 东部网络韧性中心

9 伦敦网络韧性中心


苏格兰企业韧性中心
阿伯泰大学
苏格兰网络伙伴关系
爱丁堡龙比亚大学
爱丁堡大学
贝尔法斯特
女王大学
诺森比亚大学
纽卡斯尔大学
北爱尔兰网
络安全中心
兰卡斯特大学
GCHQ斯卡伯勒
国家网络部队
GCHQ曼彻斯特
伯明翰大学
德蒙福特大学
GCHQ/NCSC
切尔滕纳姆
华威大学
南威尔士大学
剑桥大学
卡迪夫大学
牛津大学
西英格兰大学
布里斯托大学
伦敦国王学院
帝国理工学院
GCHQ布德
肯特大学
伦敦大学学院
伦敦大学
皇家霍洛
威学院
金斯顿大学
萨里大学
南安普敦大学

目标2：
增强和扩大英国在各个层面的网络技能，包括通过世界一流的多元化网络安全专业来激励和装备未来的人才

70. 英国雄心的核心将是为网络劳动力提供持续和多元化的高技能人才，能够保护数字经济的核心要素，并创新和开发新方法。如此一来，我们的目标将得到支持，即通过认可和保留整个公共部门的专业知识，提高我们在执法、国防和安全方面的能力，包括国家网络部队（NCF）的能力，并以此树立榜样。与本战略的其他部分一样，我们将与苏格兰、威尔士和北爱尔兰的分权政府合作，保证在全国范围内对英国政府在教育和技能等地方分权事项上提出的举措采取一致的做法。到2025年，我们将实现以下成果：

71. 显著增加拥有进入网络劳动力所需技能的人数，在英国四大地区的工作基础之上，进一步保证教育和技能政策满足人们和雇主的需求。我们将通过一系列措施做到这一点，包括根据网络劳动力的需求扩大对16岁以上人口的培训项目，资助一系列网络安全技能训练营，在全国推出技术学院项目，以及继续为本科生提供网络优先（CyberFirst）助学金计划。在政府工作的基础上，在2030年前使大多数16岁以上人口的教育和培训与雇主主导的强化标准相一致。这些都会联合英国网络安全委员会（UK Cyber Security Council）一起，为更广泛的网络社区开发，以此巩固学徒制、T Levels（技术资格考试）和更高水平的新技术资格认证。这会保证雇主在设计和开发资格和培训项目方面发挥核心作用。

72. 更高质量、更成熟、更受认可和更结构化的网络安全专业。英国网络安全委员会将在《皇家特许状》的支持下，在世界领先的网络安全知识体系（CyBOK）的基础上，建立进入和贯穿网络职业生涯的专业标准和途径。我们将探索包括立法在内的所有政府手段，将这些标准嵌入整个专业，确保卓越和专长能够在网络劳动力中获得明确和一致的认可。

73. 更加多元化的网络劳动力，让未得到充分代表的群体和来自英国各地弱势群体的人们获得更有效的支持，开启网络职业生涯并蓬勃发展。我们的一系列措施将包括支持更多妇女进入网络劳动力市场，以及采取具体干预措施，支持未得到充分代表的群体晋升到高级职位。通过我们的旗舰项目“网络优先”（CyberFirst）开展的课外活动已经获得成功，包括“CyberFirst女生竞赛”。我们将在此基础上再接再厉。我们还将通过英国国家打击犯罪总局（National Crime Agency）的“网络选择”（Cyber Choices）项目，增加处于风险中的青少年接受教育和就业的机会，引导他们远离非法网络活动，转向更积极的机会，发挥他们的才能和热情。

74. 通过我们的教育系统源源不断地输送高技能和多样化人才。我们将鼓舞和支持更多的年轻人通过教育走上技术之路，包括参加计算机科学GCSE和在苏格兰参加同等资格考试、参加例如英格兰的T Levels（技术资格考试）等继续教育考试、学徒制和高等教育机会等，增加其参与考试的人数和多样性。我们还将通过国家计算教育中心（NCCE）提升更多英格兰教师的技能，保证他们获得资源和发展机会，这将有助于他们激发起学生对此的兴趣。

75. 政府能够更好地识别、招聘、培训和保留其所需的网络专业人员。作为网络专业人员的主要雇主，政府和公共部门需要以身作则，支持和加强上述措施。我们将在整个公共部门采取更加一致和有效的方法，同时定制具体措施来提高公务员和高级领导人的技能，并建设我们在国防和安全方面的能力，包括NCF、NCSC和执法机构。这将包括通过扩大“Cyber Fast Stream”（网络快速升迁）项目的规模以及提供更多网络安全学徒制项目来投资于具有潜力的人才，支持NCA的专家技能项目，包括毕业生和实习生的实习安排、专门定制的神经多元性项目和夏季多元性项目。它将借鉴国防网络学校的成功经验，将其扩展为国防网络学院，提供更广泛的防御性和进攻性网络培训课程，同时与学术界、行业以及国际伙伴开展合作。

英国网络安全委员会（The UK Cyber Security Council）

英国网络安全委员会于2021年3月成立，是网络安全职业的世界首创。它的使命是成为该职业的声音，为日益增长的网络劳动力以及该行业现有的资格、认证和学位带来清晰度和结构。这是至关重要的一步，因为我们认识到，网络职业包含了整个经济中各种技术和非技术专业知识，其广度类似于医学和法律等更成熟的职业。

委员会有四个目标：

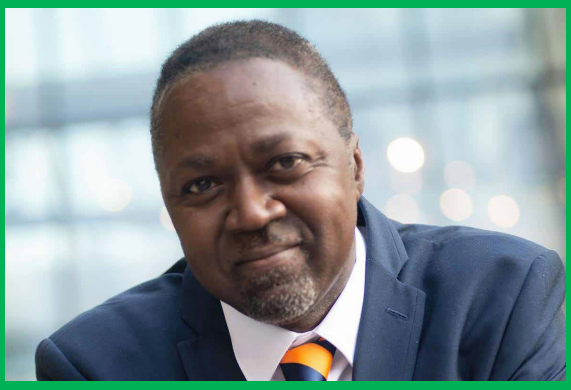
- 思维领导力和专业标准：发挥领导作用，制定并同意通过定义网络安全的标准
- 职业发展和学习：支持雇主和个人做出关于职业发展的决策，提供网络安全技能、职业发展和认可方面的建议
- 职业道德：提供指导原则，在这些原则范围内，从业专业人员和组织本身可以展示网络安全方面的道德实践
- 多元化和包容性：推动网络安全成为所有年龄和背景的人的职业机会，努力消除该行业的准入门槛和发展障碍

在本战略实施期间，委员会将寻求发展和建立其作为专业权威机构的信誉和可持续性。委员会将汇集一系列现有的专业和认证机构，确定和授权专家组织，让他们可以为新进人员、现有从业人员和雇主等就职业发展和能力要求提供清晰度。

2021年11月，女王批准授予英国网络安全委员会《皇家特许状》。这是首次出现专门针对网络安全的定制特许状，涵盖了该领域现有的专业领域。

我们认识到，在整个网络生态系统中嵌入专业标准和途径方面还有很多工作要做，包括政府、国防和执法机构。委员会将在这方面发挥重要作用，支持年轻人和变换职业者在网络这一专业上找到自己的职业发展道路。

英国网络安全委员会主任西蒙·赫本（Simon Hepburn）



我的工作包括推动英国网络安全委员会成为“网络安全职业之声”。委员会是英国网络安全专业的自我监管机构，我们的目标是联合行业共同制定、推广和管理国家认可的网络标准，使英国成为最安全的在线生活和工作场所。委员会在组建项目成功后于2021年3月正式成立，我们现在开始接受成为成员的申请。《国家网络战略》是一个至关重要的元素，保证个人和组织能够促进该行业，而委员会则是关键的协调者。

目标3：
促进可持续、创新和具有国际竞争力的网络和信息安全行业的发展，提供满足政府和更广泛经济需求的优质产品和服务

76. 为了增强英国的国家网络力量，推动数字增长和出口，英国需要一个由高质量、值得信赖的公司组成的充满活力的网络行业。英国企业为英国和全球的行业和政府提供世界领先的技术、培训和建议。但是，为了开发尖端技术，一些企业需要支持和帮助它们获得投资的关系，以达到能够提供可行产品的阶段。

77. 企业还需要有信心，相信自己的创新符合政府批准的参数，而这些参数其他组织也在遵循。在帮助买家找到面对复杂局面的方法，提供各种质量的产品和服务方面，我们可以做的还有很多。而反之，这也会刺激生态系统中的需求，并支持其进一步增长。
到2025年，我们将实现以下成果：

78. 一个年增长率高于全球平均水平的网络部门，包括通过贸易和网络出口的。我们将通过支持世界领先的英国旗舰网络活动，以及邀请我们最具创新精神的网络企业参加贸易代表团和国际网络博览会，帮助网络企业进入国内外新市场。我们将更有效地利用公共部门采购，并建立一个全面的NCSC认证供应商名录，以鼓励对高质量网络安全产品和服务的需求。

79. 一个更具创新性的网络行业早期投资显著增加，更多的网络企业得以启动、发展和扩大规模。我们全新的“网络跑道”（Cyber Runway）项目为企业提供了一个统一的支持中心，从我们以前的项目中吸取经验教训，如“科技国家网络计划”（Tech Nation Cyber Programme）、“网络101”（Cyber101）和“Hut Zero”等。我们将把包括网络加速器“NCSC初创企业”（ NCSC for Startups）的切尔滕纳姆创新中心（Cheltenham Innovation Centre），转变成一个真正的国际创新中心：英国国家网络创新中心（National Cyber Innovation Centre）。我们将利用现有组织的专业知识来促进和实现共同创造，如国家安全技术和创新交易所（National Security Technology and Innovation Exchange）。我们将鼓励对处在发展早期的网络初创企业进行高风险投资，包括通过与英国商业银行合作（British Business Bank）的国家安全战略投资基金（National Security Strategic Investment Fund）。

80. 随着东南部以外地区的增长，**英国的网络经济已经进一步实现均衡发展**，这为英国从新冠肺炎（COVID-19）疫情中恢复作出了贡献，同时也支持更广泛的区域经济活动。我们将在英格兰西北部的萨姆斯伯里（Samlesbury）建立NCF的常设总部，推动伦敦以外的科技、数字和国防领域的发展，并帮助该地区建立新的合作伙伴关系。我们会加大对伦敦和东南部以外地区的创新者和企业家的支持力度，帮助他们开发产品和服务、发展业务、招聘有技能的员工。这包括切尔滕纳姆区议会领导的黄金谷园区（Golden Valley），这一园区致力于支持网络相关技术企业的增长。我们将通过与区域网络集群的合作，增加更多英国地区的网络企业的出口能力，并组织活动向国际买家展示我们更多的网络行业人才。

81. 更多的企业能够提供符合独立验证的质量标准的网络安全技术、产品和服务，增强用户信心。我们将按照NCSC于2021年9月发布的《NCSC技术保障的未来》（The Future of NCSC Technology Assurance）白皮书提供这一服务，利用NCSC的品牌和专长建立一个值得信赖的市场，帮助英国消费者放心购买服务，提高他们的安全性，并提升国家网络安全标准。[23]

[23] NCSC，白皮书：《NCSC技术保障的未来》（2021年）

Cyberfish公司首席执行官兼创始人伯塔·帕彭海姆（Berta Pappenheim）

CyberFish参与了政府的网络加速器项目。我们的使命是帮助企业和政府团队做好准备，更好地处理业务中断，如网络事件。为此，我们与他们一起进行事件模拟演习，观察他们在压力下的团队动态，并指导他们如何改进。许多顾问要不擅长事件响应的技术方面，要不擅长领导和决策的行为方面。我们拥有两方面的专业知识，并借此同时做到了这两点。我们的演习已经帮助全球近500位来自关键任务团队的行业领袖转变观点，改善团队合作，从而改进危机响应和决策。

有兴趣成为网络劳动力的一员或开启自己的事业吗?

82. 我们之前的战略主要强调在英国发展网络技能基础和网络安全服务领域。正如在战略背景中所述,我们在**发展该行业和增加出口**方面已经取得了重大进展:

帮助网络企业寻找国际市场。2020年,英国出口了 42亿英镑的网络服务。

网络交易所,我们的在线网络门户,汇集了英国所有地区的网络业务。

网络增长伙伴关系一直以来将政府和行业聚集在一起,以打破增长的障碍。

83. 我们一直以来 **支持创新者发展和扩大企业规模**,,确保英国网络生态系统在过去五年蓬勃发展:

NCSC初创企业 为创新者指出了最重要的战略挑战,旗下的初创企业已经参加了160多个新的企业试点项目。

LORCA已经帮助72位网络创新者筹集了超过2亿英镑的投资,获得了超过3700万英镑的收入。

网络跑道在Hutzero和Cyber101的成功基础上,支持创新者启动、发展和扩大他们的业务。

84. 我们一直在努力缩小每年缺口达1万名的**进入 网络劳动力市场**的专业人员缺口：[24]

网络优先（CyberFirst）助学金计划为本科生提供支持，每年向网络劳动力市场输送数百名有工作经验的个人。

目前有四个网络学徒制标准 已经由行业制定出来，还有三个通过英国教育部“就业课程”（Courses for Jobs）计划提供的可以实现初步学习成果的网络课程。

通过最近的国家技能基金（National Skills Fund），已经有九个网络训练营_ 获得支持，带领人们进入激动人心的网络职业发展道路。在下一个开支周期内的每一年都有计划推出更多的网络训练营。

85. 我们一直努力**使网络劳动力专业化**，让组织更直接地了解他们需要什么技能，让个人更容易找到他们需要知道的内容：

英国网络安全委员会是世界上第一个网络安全专业权威机构。它在现有专业机构迄今为止所做的所有工作的基础上，已经开始制定明确和一致的专业标准。委员会计划从现有的各种认证资格中明确确定有效的资格。

网络安全知识体系（CyBOK）为网络安全部门的教育和专业培训提供信息和支持。

[24] 英国数字、文化、媒体和体育部（DCMS），《了解网络安全人才库》（2021年）

86. 我们一直致力于**保证每个人都能加入网络劳动力**，解决这一行业的不平等问题。业内的女性劳动力只占16%，而只有3%的高级职位由女性和少数族裔担任。[25]

“网络优先”（CyberFirst） 课程和探索（Discovery）项目吸引了近30万名11-17岁的青少年。

英国网络集群合作组织 正在行业、学校和大学之间建立伙伴关系，确保各地区都能获得机会和专长。

NCA的 “网络选择”（Cyber Choice） 项目正在帮助年轻人做出明智的选择，并以合法的方式使用他们的网络技能，提高认识并提供更好的选择，如学徒和实习机会。

[25] 英国政府，《英国劳动力市场的网络安全技能》（2021年）

支柱二：
网络韧性

建设一个富有韧性和繁荣的数字英国

87. 网络安全和韧性是我们作为网络强国的更广泛战略目标的基础。没有它们，我们就不能指望充分利用数字技术的变革潜力，重建更好、更公平和更强大的网络，并保护英国在网络空间内外的战略优势。我们必须继续建立强大的网络防御，在国家、地方和个人层面采取行动保护英国的数字网络、信息和资产，并确保它们在事件发生时具有韧性。

88. 虽然我们本章的重点是关注网络韧性，但要获得完全有效的韧性，网络韧性需要成为一个全社会共同努力的一部分，才能提高英国的韧性。即将出台的《英国国家韧性战略》（National Resilience Strategy）是《整合评估》的一项重要承诺，会阐述英国建立国家韧性的总体方法。

89. 过去十年，随着国家网络安全中心（NCSC）建立，咨询、指南和其他工具的增加，以及包括《网络与信息系统监管条例》（简称《NIS监管条例》）、《一般数据保护条例》（General Data Protection Regulation）和《2018年数据保护法案》在内的立法的实施，我们在提高网络韧性方面取得了重大进展。但是严重的差距仍然存在。网络入侵影响政府、企业、组织和个人。许多组织仍然报告大量网络安全漏洞或攻击。

90. 我们在之前战略的基础上进一步进化我们的方法，改变英国网络韧性的标度，并着重强调：

- 加大我们的工作力度，使互联网自动地变得更加安全，预防攻击，建立基本的保护机制，使所有英国企业、组织和公民受益，并增加对那些最无法在网上保护自己的人的支持
- 为政府树立雄心，使其成为网络安全最佳实践的典范
- 通过更好地利用监管和其他激励措施，将网络安全作为良好商业的核心部分，并利用我们对威胁的洞察力来建立能够自我保护的社区
- 用客观可衡量的标准、证据和数据支撑所有上述这些内容，并从收集数据转向根据这些数据采取行动

91. 在本战略中，网络韧性的概念有三个关键方面。首先，需要了解**风险**的性质。其次，我们需要采取行动来给系统提供**保障**，以预防和抵御网络攻击。第三，在认识到一些攻击仍然会发生的同时，我们为这些攻击做好准备，要有足够的**韧性**来最小化这些攻击带来的影响，并拥有能够恢复的能力。

92. 我们的方法在使我们能够应对系统性风险的国家能力的支持下，为每个受众量身定制。我们寻求保护和影响的受众是英国公民、企业和组织、政府和公共部门，以及那些运营我们关键国家基础设施，即为我们提供我们赖以生存的饮用水、电力、金融、交通和电信等关键服务的各方。

93. 我们将首先关注为所有英国互联网用户保障数字环境的措施，预防攻击，建立产品和服务的基本安全，并通过基本行动帮助个人、小企业和组织提高网络安全。随着我们转向有更大责任和能力的各方，我们将建立与其风险相称的额外安全和韧性层，最终为我们的人民和经济所依赖的关键公共和基本服务提供最高水平的保护。

94. 这必须是政府与经济和社会所有部门共同努力的结果。企业和组织的董事会有责任管理自己的网络风险。我们的目标是设定明确的预期，以正确的激励、支持和监管框架为基础来实现改进。同时，我们并将网络安全风险的负担从最终用户转移到最适合管理网络安全风险的人身上。

95. 我们要求政府部门、更广泛的公共部门和关键国家基础设施（CNI）的受监管运营商，更加积极主动地管理风险。我们期望大型企业和组织，包括数字服务和平台提供商，会更加负责地保护他们的系统、服务和客户，将其作为经营业务的核心部分。作为回报，政府将采取更多措施来保护数字环境，应对系统性风险，并通过建议、工具、市场认证和发展可以促进改善的技能来提供支持。

96. 我们在英国促进网络韧性方面做出的努力也必须成为我们国际参与的一部分。供应链、信息技术平台、跨国企业和互联网本身的日益全球化，意味着我们无法孤立地改善英国的网络安全。为了应对这一挑战，我们需要继续更好地理解英国和全球网络韧性之间的联系，解决高风险领域的问题，并与国际伙伴合作，建立韧性，促进数字化转型、安全和贸易，互惠互利，以实现支柱四：全球领导力一章提出的内容。


减轻每个人的负担
与提供商合作，更好地保护英国互联网 用户，并将基本保护纳入公民在线服务中
扩大主动网络防御，预防和破坏网络犯罪和欺诈
公民意识和网络卫生
更有韧性的企业和组织
对网络基础（Cyber Essentials）等标准的采用并提高透明度
市场激励和更多的地方支持
在数字服务和个人数据等目标领域加强监管
更有韧性的公共服务
到2030年，所有政府组织对已知的攻击方法都具有韧性
加强问责制、标准和独立保证明机制
投资解决遗留IT问题
更具韧性的关键国家基础设施
对常见攻击方法建立起韧性，同时根据风险态度提供更高级的保护
了解并解决数字化和新技术带来的风险

目标1：
提高对网络风险的认识，从而在网络安全和韧性方面采取更有效的行动

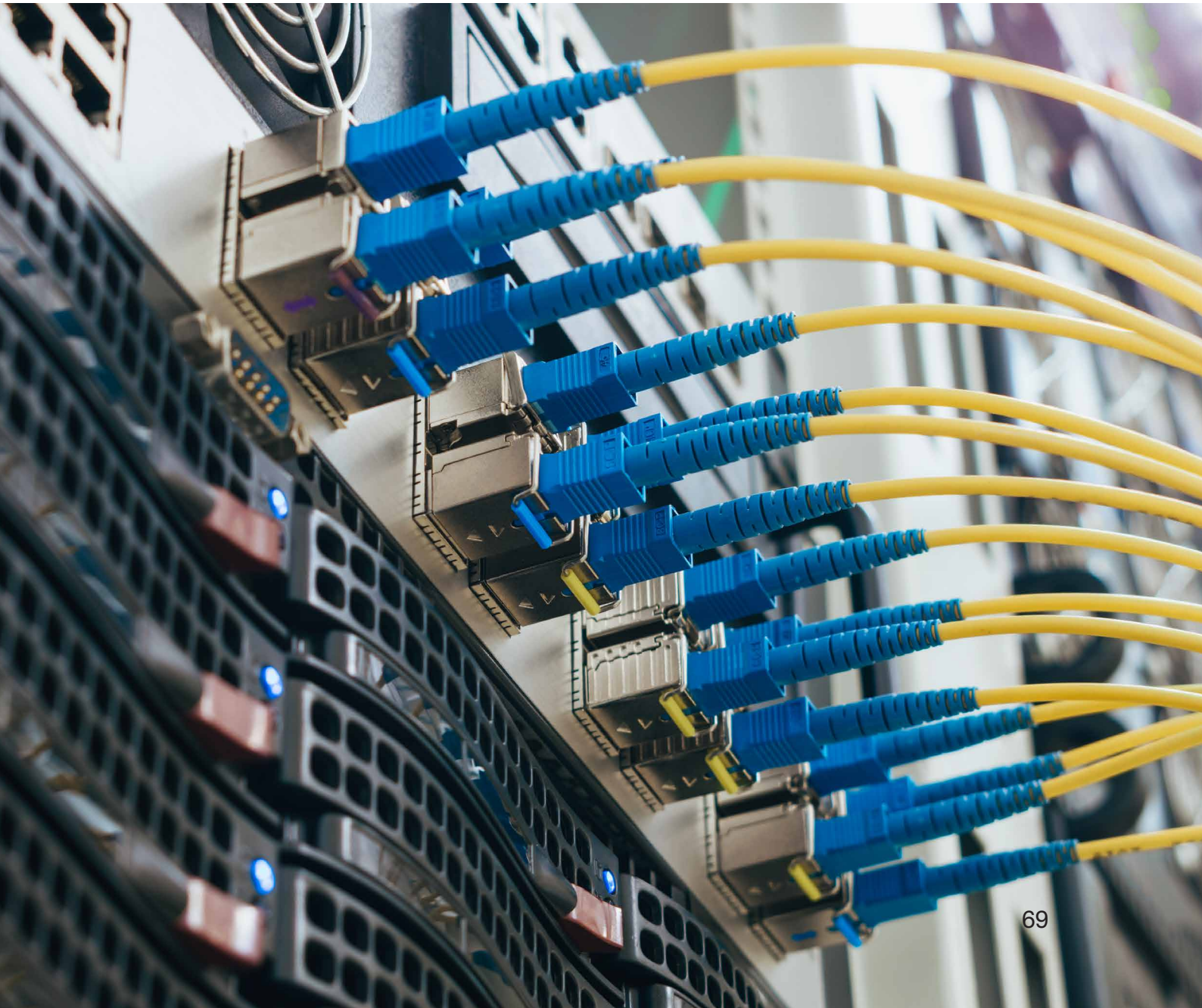
97. 我们将在政府、企业和组织之间建立更紧密的伙伴关系，以提高对风险的集体认识，指导确立优先事项，并建立行动的基础。我们将通过与向消费者提供服务的企业和组织合作来支持公民，同时进一步加强政府识别跨领域风险的能力。到2025年，我们将实现以下成果：

98. **政府对国家网络风险拥有最新的战略理解**，并利用这种理解来识别系统风险、传达优先事项以及推动战略和实施。我们将维持《国家网络安全战略》中对于“理解威胁”的重大投资，并进一步发挥它的价值。我们也将在现有努力的基础上理解互联度增加的世界中的风险。这包括识别数字供应链过于集中的地方，以及与国际伙伴合作管理集体风险。我们还将改进《计算机滥用法案》（CMA）的违法犯罪记录，了解数据泄露和下游犯罪之间的联系，并增加我们对CMA违法犯罪如何促进其他类型犯罪活动的了解。

99. **政府在理解网络风险方面以身作则。**我们将采用NCSC的“网络评估框架”（CAF）作为所有政府部门的保证框架，并比对关键系统和公共供应商的关系。我们将建立一个新的政府网络协调中心（GCCC）和跨政府部门漏洞报告服务（VRS），使政府在管理事件、漏洞和威胁时能够“一体防御”。VRS将致力于与安全研究员社区建立有价值且值得信任的关系，从而减少整个政府产业的漏洞。我们还将继续支持和协调地方分权政府中的类似举措，例如提议为苏格兰的网络韧性建立中央协调职能。

100. **对于整个英国关键国家基础设施的网络风险有更深刻的理解。**我们将在关键国家基础设施各部门提高对“网络评估框架”（CAF）或类似框架的采用率，并提高与其他正在使用的网络安全评估和报告框架的可比性。我们将完成关键性评估，并比对关键国家基础设施及其供应链的依赖性。我们将与关键国家基础设施所有者和运营商建立更强的伙伴关系，改善威胁和风险信息的获取，并就应对风险的立场达成一致。我们将努力了解数字化和新技术带来的新风险或出现新的关键国家基础设施的领域，包括更广泛的优先事项，比如向净零排放的过渡。

101. 英国企业和组织对网络风险及其管理责任有了更好的理解。我们将帮助组织更好地了解其客户面临的风险，包括他们持有的数据是如何被利用实施欺诈、身份盗窃或勒索等犯罪。我们将分享更多关于网络攻击的发生率和影响，以及各行业在改善网络安全方面取得的相对进展的研究和数据。



目标2：
通过改善英国组织内部的网络风险管理，更有效地预防和抵御网络攻击，并为公民提供更大的保护

102. 我们预防和抵御网络攻击的方法：(i) 各组织有责任采取行动管理自己的网络风险，但在董事会层面需要更强有力的问责制和善治框架，使管理网络风险成为优先事项；(ii) 政府可以发挥作用，与行业合作采取措施，在其能够发挥独特作用的地方大规模地直接减少风险；以及(iii) 我们必须保证能够提供支持和指导，帮助个人、个体经营者、小型企业和组织管理其网络风险。到2025年，我们将实现以下成果：

103. 政府大规模地减少对英国造成的危害，减轻英国公民的负担。我们将代表英国所有互联网用户针对上游采取更多行动，扩大我们积极的网络防御措施，为更广泛的领域提供支持，包括慈善机构、学术界和中小型企业及公民。我们也会通过加强与业界的接触和信息共享，加强对在线服务的保护。

104. 这项工作是对其他政府重点推出的旨在保护英国公民在线活动的补充，比如《在线安全法案》(Online Safety Bill) 草案和打击欺诈等经济犯罪的政策。

105. 这意味着我们将与包括在线服务提供商、电信、技术、银行和零售在内的相关行业进行更密切的合作，在以下这些方面更好地保护英国互联网用户：使非法注册网站更加困难；加强对在线恶意内容的清除和阻止；改善被盗账号密码的追回和返还；以及增强英国电信基础设施的安全性。我们还将制定各种方案，在自愿安排不足以解决问题的情况下，为公民保护提供立法的支持。

106. 我们大规模减少危害的努力还将包括应对来自数字供应链的系统性风险。必要时，我们将进行干预，促进供应链多元化，就像我们在电信业所做的那样。我们会加强我们的集体经济安全，改善信息共享，在关键部门对外商直接投资 (FDI) 方面采取稳健、可预测和相称的筛选方法，为政府的关键和共同供应商制定明确的要求。

107. 到2030年，政府的关键职能对网络攻击的抵御能力显著增强，整个公共部门的所有政府组织都将能够抵御已知的漏洞和攻击方法。我们的目标是将英国的公共部门树立为最佳实践的典范。为了支持这一成果，我们将发布首个专门的《政府网络安全战略》(Government Cyber Security Strategy)。《战略》侧重于更有效的风险管理流程、治理和问责制；集中开发和部署的能力 (包括主动网络防御)；对系统、网络和服务进行更全面的监控；快速和规模化的事件响应；以及对技能、知识和促进可持续变革的文化的投资。

108. 英国关键国家基础设施的网络风险得到更有效的管理。这些服务从定义上说就是国家最依赖的服务。我们将继续与运营商密切合作，尽快实现对常见攻击方法的韧性，并在适当的情况下实施更高级的保护。对于根据《NIS监管条例》指定的基本服务运营商来说，这意味着至少要达到相关职能部门为每个行业设定的基准标准。

109. 为了支持这一结果，我们将检视政府对CNI运营商问责的能力，确保他们对关键系统的网络安全进行了投资，并有效管理其风险，包括来自其供应链的风险。我们会加强监管框架，在更广泛的国家安全风险以及快速变化的威胁和技术的背景下，提高其覆盖面、权力和快速适应能力。首先要做的是就《NIS监管条例》的改革进行意见征集，为英国电信提供商实施新的安全框架，并制定相应的监管框架，以确保英国为了实现净零排放所需要的智能灵活的未来能源系统安全可靠，能够具备应对网络威胁的韧性。

110. 与此同时，我们将提高监管机构的能力；通过投资提升技能，提高CNI运营商吸引、培养和留住网络专业人员的能力（参见《英国网络生态系统》章节）；通过加强与关键供应商的合作，探索从指导到立法和采购等方面提案所提供的全方位手段，来支持运营商管理供应链风险。

111. 我们的数据使用所依赖的基础设施是安全且有韧性的。这些基础设施是至关重要的国家资产，支撑着我们的经济、提供公共服务并推动增长。我们将在确保数据在处理、传输或大规模存储（例如在外部数据中心）时得到充分保护方面发挥更大的作用。我们会建立一个更强大的风险管理框架，确保整个行业拥有更高的安全和韧性标准，并实施《2021年国家安全和投资法案》（National Security and Investment Act）的规定，加强投资筛选。我们会加强与国际伙伴的合作，确保全球数据访问和流动的增加不会增加英国面临的安全风险，同时能够解决因为收集大量数据带来的安全挑战。

112. 我们还将考虑英国数据基础设施服务在支撑经济中所日益增加的重要性及其在关键国家基础设施中的作用。这些措施符合《国家数据战略》（National Data Strategy）和《整合评估》中提出的承诺。

113. 越来越多的英国企业和组织正在积极主动地管理他们的网络风险，并采取行动提高他们的网络韧性。我们将开发会鼓励有效网络安全的市场激励机制，通过这些激励机制提供支持并推动行为改变。必要时，我们会通过有针对性的立法来进行补充，确保网络风险由负有最大责任的各方来有效管理，并且英国的网络安全立法在不断发展的风险和技术下仍然有效。

114. 为了支持这些目标，我们将越来越多地与市场影响者（采购方、金融机构、投资者、审计机构和保险公司）合作，以激励整个经济中良好的网络安全实践。我们会对企业应对风险（包括网络风险）的韧性的报告机制提出改良建议。这会让投资者和股东更好地了解公司如何管理和减轻其业务的重大风险。我们将继续推动认证和标准的采用，如网络基础（Cyber Essentials）认证计划，并推动董事会参与网络风险管理。

115. 针对性的立法将主要关注受网络攻击潜在影响最大的行业，包括某些基础和数字服务的提供商、更广泛经济中的数据保护以及大型企业。这将是对《数字监管计划》（Plan for Digital Regulation）的补充，最开始会侧重于如上文以及《技术》一章所述的管理网络和信息系统安全（NIS）的法规，也会侧重于改革英国个人数据保护制度的后续步骤。

116. 《网络安全监管和激励评估》（Cyber Security Regulation and Incentives Review）将进一步详细阐述我们将采取的行动，以提高英国企业和组织的商业韧性和网络安全。

117. 提高网络韧性的技术建议、自助工具和有保证的产品和服务很容易找到，也在不断改进，它们特别强调帮助公民、个体经营者和小型组织。我们将继续通过NCSC开发技术上准确、及时和可以采取具体行动的指南和自助工具。我们将保证通过最有效的渠道传递出一致和清晰的信息，无论是通过网络意识运动、NCSC网站、政府、执法网络还是行业伙伴关系。我们也会在地方一级提供更多的支持。通过“数字权益”（Digital Entitlement），我们将继续为有需要的成年人提供必备数字技能（Essential Digital Skills）的资格，确保学习者拥有安全、负责任地上网所需的基本数字技能。我们会帮助企业和组织找到应对复杂的网络安全市场的方法，将我们的安全产品和服务框架进行延伸，并围绕网络基础（Cyber Essentials）开发商业产品，使小企业更容易获得基础建议。

Tarian区域网络犯罪调查处网络保护和预防事务官员伊莉斯·鲍尔（Elis Power）

Tarian区域网络犯罪调查处（Tarian Regional Cyber Crime Unit）是一个由从威尔士警察部队借调的警官和工作人员组成的跨学科小组。他们的使命是为在南威尔士提供一个更安全的网络环境做出贡献。

网络保护/预防事务官员伊莉斯·鲍尔（Elis Power）为互动小组工作：

“这是老生常谈了，但这个部门每天的工作都不一样。日常而言，我可能需要负责向内部警察部门或外部组织做包含建议的介绍演示，保证他们充分了解如何保护自己和工作场所免受网络威胁。也可能需要向学校里的年轻人介绍许多话题，从互联网安全到《1990年计算机滥用法案》（Computer Misuse Act 1990）等。我经常参与合作机构和部队的会议，讨论新的威胁和相关的指导方针。我还会联系给我们发送漏洞警报的组织、参与国家行动、应邀出席相关活动和会议，并抽时间不断提升我的能力和知识库。”

目标3：
加强国家和组织层面的韧性，以准备、应对网络攻击并从中恢复

118. 尽管我们努力了解风险并采取预防措施，但一些事件仍然会发生。我们需要加强所有组织的事件管理和响应能力，以最大限度地减少造成的伤害，并为受害者提供更好的支持。到2025年，我们将实现以下成果：

119. 英国对国家重大网络事件的战略管理和响应协调更加有效。我们将借鉴政府应对重大网络事件的经验，确保吸取经验教训来改进我们的政策和流程。我们会与国际伙伴和行业分享危机管理经验，并反过来从其他地方找出最佳做法，加强我们的准备工作和流程。我们将确保NCSC和执法机构的事件管理团队具备必要的专长和工具，以应对各种不断变化的事件类型，并协调国家对优先威胁的响应。

120. 上报网络事件是更容易的一件事，网络犯罪的受害者可以得到更好的支持。上报信息还将用于帮助预防未来事件，支持执法部门调查、瓦解和起诉网络犯罪分子。为了支持这一点，我们将提供一个新的国家欺诈和网络犯罪报告和分析服务，在2025年之前取代反诈骗行动处（Action Fraud）。我们将鼓励以其他方式报告更多网络事件，包括通过伦敦金融城警察局启动的最新的商业报告机制。在受监管部门，我们将允许监管机构对更广泛的事件提出报告要求，包括“未遂事件”。国家经济犯罪受害者关怀处（National Economic Crime Victim Care Unit）的推出将改善受害者在经历了紧张且带来伤害的事情后可获得的支持和指导。

121. 政府和CNI为应对事件和从事件中恢复过来做好了更充分的准备，包括更好的事件规划和定期演习。我们将帮助英国政府和CNI运营商从市场中找到他们需要的网络演习和事件管理服务，方法是扩大NCSC的网络事件响应（Cyber Incident Response）认证计划的范围，并引入一个新的演习计划。

122. 在政府内部，各部门和整个政府数字产业的监测和检测能力将得到提高。我们确保会识别经验教训并用于改进我们的政策和流程；会与国际伙伴和行业分享危机管理经验；确保我们的事件管理团队具备必要的专长、能力和技能，以应对各种不断变化的事件类型。

123. 在CNI内部，我们将对CNI运营商的演习和测试或攻击模拟提出明确的要求，并在事件响应和演习中鼓励创新和合作，考虑应用金融行业网络合作中心（Financial Sector Cyber Collaboration Centre）等模式。作为我们技术雄心（下一章将阐述）的一部分，我们将建立一个运营技术安全国家实验室，作为关键工业技术测试、演习和培训的卓越中心，与行业、学术界和国际伙伴合作建设该领域的能力。

124. 英国企业和组织对发生事件时该做什么、该打电话给谁、谁可以帮忙以及如何恢复拥有更清晰的认识。我们将在有保证的行业服务的支持下，改善培训和演习，包括新的网络事件响应（Cyber Incident Response）计划和网络事件演习（Cyber Incident Exercising）服务。我们将确保网络犯罪的个人受害者获得一致的全国性执法支持，并鼓励小企业和组织利用地方支持，如他们的区域网络韧性中心（Cyber Resilience Centre）。

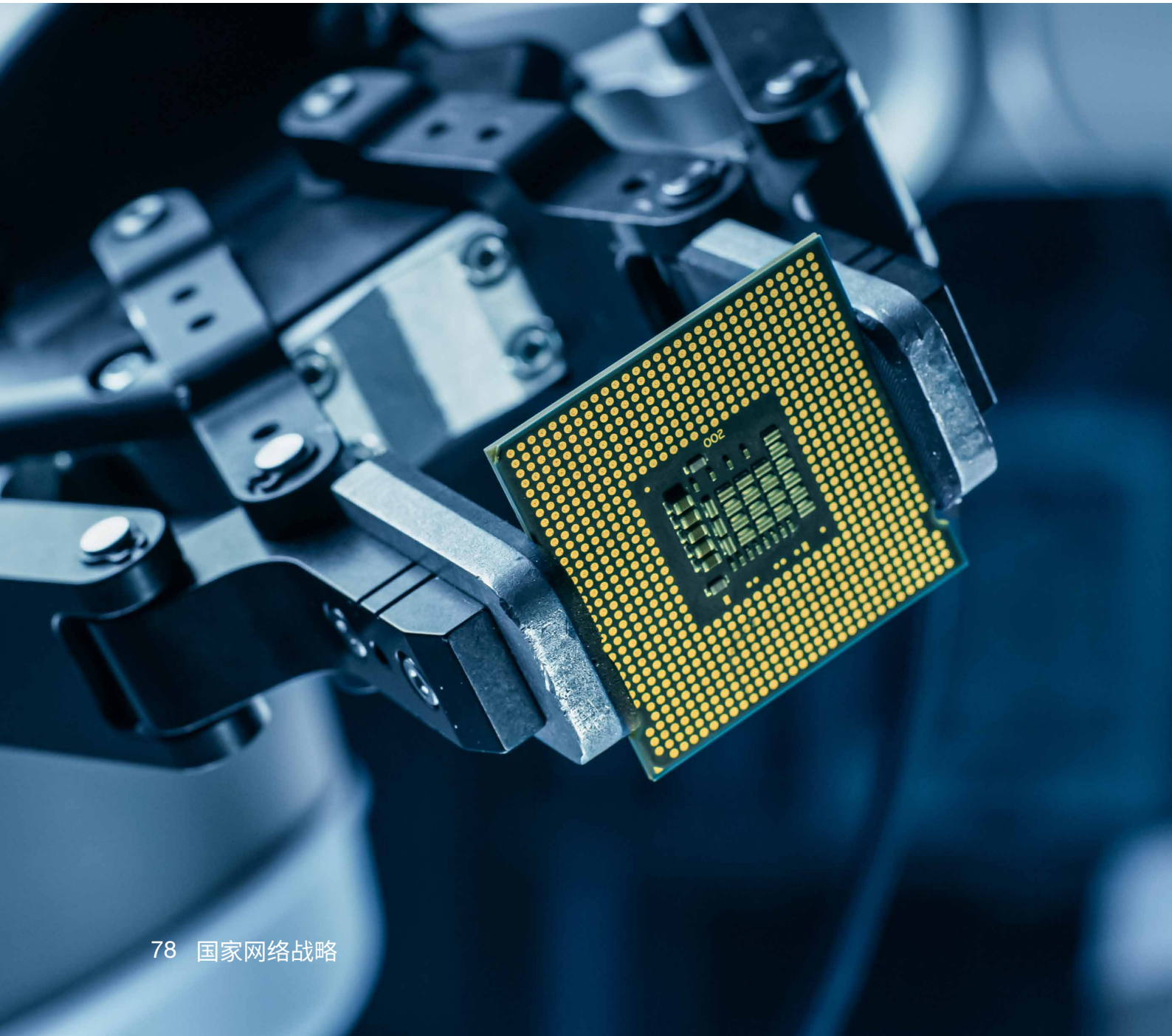
CyberOwl首席执行官丹尼尔·吴（Daniel Ng）

CyberOwl受益于政府的网络发展计划。我们为海事和CNI部门的运营资产提供网络安全监测和分析。实现可持续发展的驱动力对实地资产的连通性和数字化程度提出了更高的要求，这使它们曝露在网络风险中。CyberOwl帮助运营商识别和比对他们的资产，获得网络风险的预警，并向他们自己和监管机构证明他们已经对资产实施了保护。我们与整个欧洲中东非洲（EMEA）和亚太地区全球最大的海运资产运营商合作，提高全球海运物流供应链的韧性。2021年，我们的预订量增长了14倍，在英国和新加坡的运营翻了一番。

Rapid7社区和公共事务副总裁珍·埃利斯（Jen Ellis）

我的工作包括与各种规模和行业的组织中的安全专业人员和领导者交流，了解他们面临的挑战，并尝试确定解决方案来帮助他们提高网络安全。我经常听说组织不堪重负，不知道该关注哪里，如何开始，或者如何取得进展。技术人员也很难得到领导层的认可。政府制定清晰、一致、透明的网络战略有助于解决这一问题。它给技术人员提供了在与领导层讨论时的依据。还能识别需要聚焦的核心领域和走向成熟的潜在途径。网络安全仍然非常复杂，永无止境，但随着网络战略的广泛实施，人们对其重要性有了更深的理解，能够感到我们都有份参与。

支柱三：
技术优势



引领对网络力量至关重要的技术

125. 一些技术对于塑造网络空间的未来至关重要。能够在这些技术中确立领先地位的国家将处在更有利的地位，更能影响这些设计的设计和部署方式，更有能力保护它们的安全和经济优势，也更能利用机会快速地在网络能力上取得突破。随着技术成为地缘政治力量越来越重要的工具，这一领域的竞争将会加剧。

126. 对英国来说，通过科学和技术及其所依赖的数据获取来实现战略优势，将是一个先决条件，决定我们能否实现作为网络强国这一更广泛的目标。政府在以前的战略中已经采取措施促进网络安全技术的研究和创新，如通过设立初创企业加速器项目和网络安全研究卓越学术中心（Academic Centres of Excellence in Cyber Security Research），并鼓励开发“设计即安全”的消费设备。但是，我们现在需要用更有雄心、更主动的方法来保持在关键技术上的利益，避免过度依赖竞争对手和敌手。

127. 《整合评估》提出了使英国成为科学和技术超级大国的计划，并利用科学和技术来建立和保持我们的战略优势。这份战略为国家科学技术委员会（National Science and Technology Council）和科学技术战略办公室（Office of Science and Technology Strategy）在实现这一目标方面的工作提供了支持，并补充英国在人工智能、量子技术和数据等领域的战略。

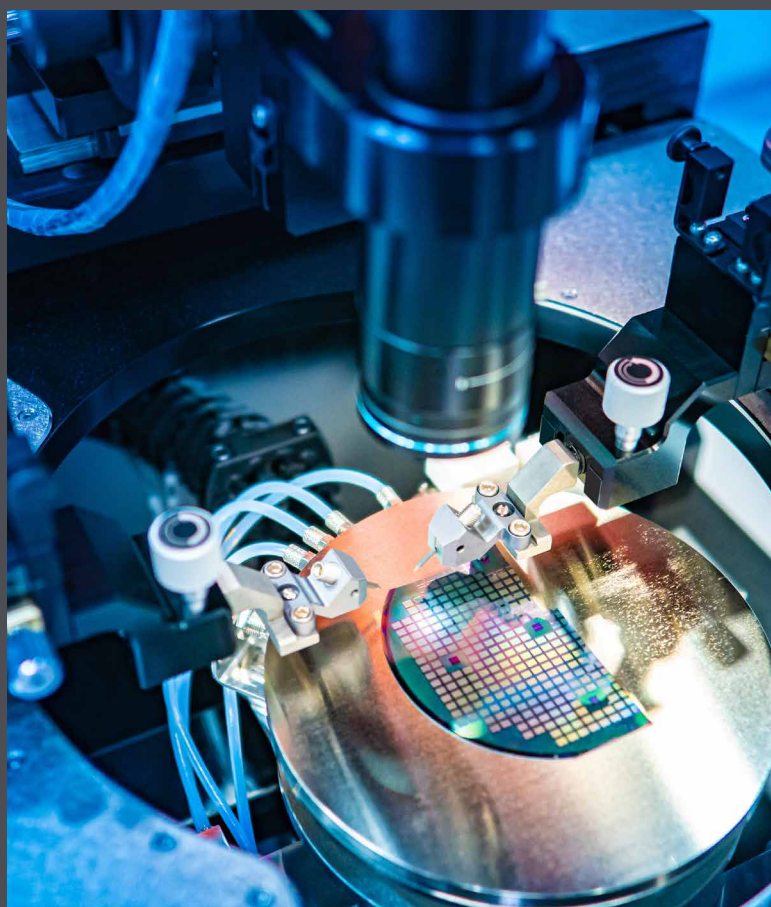
128. 我们将加强我们的能力，由国家网络安全中心（NCSC）和政府其他部门的技术专家主导，识别对我们的网络力量最关键的技术领域。我们将使用《整合评估》所确定的拥有、协作、可用框架，就优先事项做出国家级战略决策。在一些选定的领域，我们将对发展英国国内能力所需的研发活动和战略伙伴关系进行投资。在我们依赖全球市场的领域，我们将与行业、监管方和国际伙伴合作，鼓励值得信赖和多样化的供应链的建立，并制定标准保证技术的安全和开放。我们还将加强英国以《国家数据战略》（National Data Strategy）中设定的框架为基础，进一步利用和保护日益增长的由新兴技术产生并推动着创新的数据和信息的能力，使我们的经济和社会效益最大化。

对网络力量至关重要的技术

各种现有和新兴的技术会对英国的网络力量产生至关重要的作用，我们需要能够预测、评估和应对这些发展。我们计划在实施战略时将优先考虑一系列技术和应用，如下文列举的技术和应用。这并不是一个详尽或固定的列表，我们会咨询产业界、学术界和技术专家，并在这个过程中持续调整我们的优先事项：

- 5G和6G技术，以及其他新兴的数据传输形式
- 人工智能，包括保护人工智能系统的安全，以及在网络监控等各种广泛的应用中使用人工智能增强网络安全的潜力
- 区块链技术及其应用，如加密货币和去中心化金融
- 半导体、微处理器芯片、微处理器架构及其供应链、设计和制造流程
- 加密认证，包括身份和访问管理以及高保障加密产品
- 消费者、企业、工业和物理环境（如互联场所）中使用的物联网和技术
- 量子技术，包括量子计算、量子传感和后量子密码术

这项工作将支持并配合政府各部门的许多战略和成果的实施，例如《国家数据战略》、《国家人工智能战略》（National AI Strategy）和《整合评估》，以及该支柱内以技术为焦点的成果。



目标1：
提高我们预测、评估和应对对我们网络力量至关重要的科技发展的能力

129. 为了建立和保持网络相关技术的竞争优势，我们需要一种相互协调、严谨和一致的方式来识别和分析科学技术的关键领域，并确定国家努力的优先次序。这将要求我们在政府和学术界进一步发展我们的研究和技术专长。我们将把这一点与政府新的科技水平检视和情报收集结构相结合，同时动用行业专家的洞察，充分利用我们的海外网络，用于了解国际伙伴和竞争对手的优先事项和系统。到2025年，我们将实现以下成果：

130. 政府能够更好地分析新的和发展中的科学技术，并理解其对英国网络政策和战略的影响。我们将扩大研究能力，包括NCSC在曼彻斯特刚刚启动的研究中心。我们将聚焦于互联场所和交通等领域的新兴技术，并与政府科学办公室（Government Office for Science）和其他地方的专家合作。我们将利用政府以外的专长，包括支持四个网络安全研究机构和19个网络安全研究卓越学术中心，资助重点课题研究人员的开拓者奖（Pathfinder Awards），以及更有效地利用我们的海外足迹和国际伙伴关系。

131. 这种认识的提高将更迅速、更有效地为政府进行更广泛的水平检视、优先排序和决策提供信息，使我们能够采取更主动的方式来利用机会和降低风险。我们将建立一个全新的内部水平检视职能，以预测科技进步及其网络影响。我们将在掌握更多信息的基础上进行决策，优先考虑关键的网络技术，引导有利于英国安全的研发和政策制定。在适当的情况下，这将通过科学和技术战略办公室（Office for Science and Technology Strategy）和国家科学和技术委员会为更广泛的科学和技术优先事项决策提供信息。

安全信息技术中心（CSIT）首席研究员梅尔·奥尼尔（Máire O'Neill）

CSIT是英国最大的专注于网络安全的大学技术研究中心之一。在首席研究员梅尔·奥尼尔教授的领导下，该中心于2009年入选英国首批创新和知识中心。过去十年里，CSIT在研究、创新和与业界合作方面的成功使其在国内和国际上的声誉显著增长。CSIT一直是北爱尔兰网络安全集群成功的一个关键因素，它支持着该地区衍生企业的建立、本地企业规模的扩大和外商直接投资的吸引力。从2009年起步以来，北爱尔兰的网络行业现在雇佣了2300名员工，就职于104家公司，每年创造1.1亿英镑的收入。

目标2：在对网络空间至关重要的技术安全方面，建立和维持自主性以及盟友联合优势

132. 如果英国有潜力在网络技术的关键领域建立领先地位或者获得竞争优势，或者在依赖非盟国供应来源而造成不可接受的安全风险的领域，英国将寻求发展本国产业基础。我们需要在某些领域保持真正的自主能力，在另一些领域则与国际伙伴合作，或在市场的某一方面寻求领先地位。这将需要与产业界和学术界合作，采取协调一致的方式来促进创新和研发。到2025年，我们将实现以下成果：

133. 对于对我们的网络力量至关重要的技术领域，英国在把研究转化为创新和新公司方面更为成功。我们将通过与行业伙伴合作，采用更为基于挑战的方式，支持英国学术界将其研究商业化并投入运营。这样有助于识别出最有潜力的想法，并促进投资者的投资。我们将在《创新战略》（Innovation Strategy）中提出的方法的基础上，进一步提供支持，使得关键技术所在的生态系统更为成熟，保证英国的优势更加强大，难以复制。

134. 英国在安全微处理器设计方面更加强大，处于世界领先地位。[26]我们将在“数字设计即安全”项目的基础上进一步发展。这个项目为计算机芯片开发了一种新的、更安全的技术，以保护软件免受漏洞的影响。我们将把这种经验应用到人工智能处理器上，让英国供应商获得国际优势。我们将与“国家量子技术计划”（National Quantum Technologies Programme）合作，为量子计算机设计一个安全模型，并确保英国公司在这项技术上处于世界领先地位。

135. 在运营技术和关键工业控制系统的安全性研究方面，以及在测试和运用这些技术的能力方面，英国被认为是世界领先的。我们将与产业界和学术界合作，建立一个关于运营技术安全的国家实验室。实验室将开展世界领先的研究项目，并为政府、军队、行业和国际伙伴提供在英国运用和测试这些技术的设施。正如《5G电信供应链多元化战略》（5G Telecoms Supply Chain Diversification Strategy）中所确认的那样，我们将建立英国电信实验室，把政府和监管机构与行业结合起来，为建立新的电信安全框架提供支持，同时帮助提升英国供应链中电信设备供应商的多样性。[27]

136. 政府能够更好地保护英国在关键网络技术领域的创新和知识产权，抵御敌对活动，保持我们的竞争优势。[28]我们将投资于所需的资源和专长，在这些技术发展的过程中为其安全性提供技术领导，包括按照《2021年国家安全和投资法》（National Security and Investment Act 2021）提出的目标就外商直接投资风险提供建议。我们将继续与企业和学术界合作，在研发的关键领域创造一个值得信赖的环境，并制定强有力的措施来防止窃取数据和知识产权。

[26] 微处理器是我们今天使用的许多设备的大脑。它们无处不在，包括电信、国防、医疗卫生等关键领域以及我们的主要行业都有它们的应用。系统设计中的技术进步目前受到保障和安全问题的阻碍，这种问题由于系统复杂性的增加而被放大。

[27] 数字化、文化、媒体和体育部《5G电信供应链多元化战略》（5G Supply Chain Diversification Strategy）（2020年）

[28] 特别关注《2021年国家安全和投资法》识别的领域：先进机器人、人工智能、通信、计算硬件、加密认证和量子技术

数字设计即安全

当前70%的网络安全漏洞都利用了微处理器设计中的某个缺陷，而这个缺陷自上世纪70年代就已为人所知。从电视到电信，每一个数字设备中都有这种微处理器。政府一直在与技术行业合作解决这一问题，到2025年，一种新的微处理器设计将用于智能手机和越来越多的其他设备。

改变微处理器的设计需要全球合作与投资。在英国的带领下，加上英国政府7000万英镑的投资，未来设备的安全性正在设计之中，会极大降低网络攻击成功的风险。

这项改变游戏规则的技术是在英国研发的。包括微软、谷歌和其他公司在内的技术领军企业正在投资，将这些新的安全优势引入他们的产品。英国各大学的研究人员正在努力寻找使用这种安全技术的更好的新方法，政府也正在支持英国中小企业为内置有这种新安全技术的产品寻找新市场。

The Hut集团研发总监菲尔·威尔逊（Phil Wilson）

The Hut 集团是一家专注于快速消费品的电子商务企业。我们有200多个网站在一个公共平台上运行，每分钟要处理多达3000个订单，因此我们平台和客户的安全性是重中之重。我们投入了巨大的努力，以确保可以遏制任何网络攻击，这就是为什么我们对在系统中使用数字设计即安全（DSbD）技术的可能性感到如此兴奋。在这些由政府和行业投入1.8亿英镑合作开发的新微处理器上运行我们的系统，将使我们的系统更有韧性，但管理这种过渡是复杂的，只有可以满足我们对性能的要求，我们才能采用新技术。很荣幸成为数字设计即安全（DSbD）计划的第一个示范项目。我们希望在不久的将来，我们所有的系统都能受益于这种新的安全性。

目标 2a：保持一个强有力并具有韧性的国家层面的加密关键能力（Crypt-Key），满足英国政府客户、我们的伙伴和盟友的需求，并适当减轻我们最重大的风险，包括来自我们最强大对手的威胁

137. 加密关键能力是一个术语，用于描述英国使用加密技术来保护英国政府、军队和国家安全领域所依赖的关键信息和服务，包括保护其免受我们最强大的对手的攻击。它支撑着我们选择如何部署国家安全和国防能力的能力。要成为具有加密关键能力的全球领军者，我们需要政府和私营部门都具有正确技能和技术。

138. 我们将继续投资于提升我们政府的能力，与国内的加密关键能力相关的行业合作，确保英国在未来仍然是少数几个能够自主发展加密关键能力的国家之一。我们还将继续在加密关键能力相关的领域发挥全球领导力，包括支持北约成为关键材料的供应商。这种领先地位将带来二级效益，帮助英国维持高技能水平的行业，同时保持我们在具有高韧性的工程方面的优势，并有可能为其他高保障环境，如关键国家基础设施，提供新的强大能力。到2025年，我们将实现以下成果：

139. 更具韧性和安全性的英国加密关键能力，拥有更加可持续的、世界领先的产业基础，提供英国所需的全套解决方案，并向选定的合作伙伴和盟友出口。我们将更有效地结合政府和行业的能力和专长，并采取更严格的、国家性的方法来管理这一企业。这将确保我们可以提升所需的独特的专业技能。

140. 英国政府拥有更强的加密关键能力和服务，能够满足英国及其盟友不断变化的需求，并确保我们始终处于开发加密关键能力的前沿。我们将提供强大的技术领导力，以了解用户需求并改进我们的核心服务，包括提供关键材料和产品及系统保障。我们还将转变加密关键能力相关的服务，利用新技术使其变得更加灵活和隐形。

141. 英国已经提升了其在加密关键能力领域的全球领导地位，并增加了对我们的合作伙伴和盟友的出口。我们将保持我们在五眼联盟、北约和其他国际伙伴关系中的领导地位，并塑造国际公认标准的发展，以使英国加密关键能力解决方案具有互操作性。我们还将与业界合作，最大限度地增加出口机会。

目标 3：保证下一代互联技术，降低依赖全球市场的网络安全风险，并确保英国用户获得值得信赖的多样化供应

142. 在未来十年，我们将继续看到计算能力、互联网连接和自动化嵌入到我们环境中越来越多的部分，包括物理对象和基础设施，从长远来看，还包括人类自身。这将扩大网络空间的范围，并极大地增加产生的数据量。安全有保障地管理数据的能力对于我们经济的安全运行将变得越来越重要。

143. 我们需要确保尽可能在设计、开发和部署下一代互联技术时考虑到安全性和韧性，并将其作为支持“设计即安全”方法的共同努力的一部分。技术供应链的全球性意味着我们需要利用所有可用的手段来更主动地管理技术依赖的风险。在可能的情况下，我们将努力确保安全性得以内置；如果我们做不到这一点，我们将实施强有力的措施来降低风险，包括国内监管和在标准方面进行国际合作。到2025年，我们将实现以下成果：

144. 在英国销售的可连接消费者产品符合基本的网络安全标准。我们将引入并实施《产品安全和电信基础设施法案》（Product Security and Telecommunications Infrastructure Bill），以便在英国销售的所有新的可连接消费者产品中实施最低安全标准。我们将以具有网络安全的方式向智能灵活的能源系统过渡，包括智能电动汽车充电站和智能节能设备。我们将与标准机构、行业和国际伙伴合作，在全球对技术标准的共识方面发挥影响力。我们将帮助英国组织以更安全的方式采购、部署和管理互联设备，包括通过发布新的企业互联设备安全指南这样的方式。

145. 包括云、软件、托管服务和应用商店在内的主要数字服务提供商需要遵循更好的网络安全标准，这有助于保护组织和消费者免受网络威胁。我们将加强和扩大对数字服务提供商的现有监管，并提高ICO的能力，以确保数字提供商更主动地管理与其服务相关的风险。我们将继续与行业合作，包括主要的技术公司，以利用市场的专长，并确保各方都在保护英国的数字供应链中发挥作用。我们还将引领制定聚焦于数字供应商的国际政策解决方案。

146. 英国在安全和可持续地采用互联场所技术方面处于领先地位，这对公民和企业都带来了益处。互联场所，有时被称为智慧城市，拥有为社会提供切实益处的潜力，包括管理交通，减少污染，节省资金和资源。然而，虽然互联性使场所更有效地运作，但也造成了网络漏洞和网络攻击的可能性。我们将在NCSC《互联场所安全原则》的基础上，降低企业、基础设施、公共部门和公民面临的风险。[29] 我们将加强港口、大学和医院等地方政府机构和组织的能力，以安全地购买和使用互联场所技术。我们将建立一个国际共识，对互联场所的安全采取一致和有效的方法。

147. 网络安全从设计上已经被纳入英国部署的其他新兴技术中。我们将识别有可能造成网络安全风险的新兴技术应用，并确保英国处于安全发展这些技术的前沿。政府在考虑英国在数字孪生和更广泛的"网络物理基础设施"技术方面拥有的能力，保证网络安全处于决策的核心。[30] 我们将推出一项保障计划，以确保英国在广泛的联网和自动车辆部署方面处于强有力的地位。[31]

[29] 英国国家网络安全中心（NCSC），《互联场所安全原则》（Connected Places Cyber Security Principles）（2021年）
[30] 发布于《创新战略》（2021年）
[31] 《确保安全和有保障的互联和自动化车辆流程（CAVPASS）》

Angoka的首席技术官兼创始人沙迪•拉扎克（Shadi A. Razak）

政府发布了互联场所安全指南。自动驾驶汽车日益增长的使用，凸显了安全在我们社会中的重要性。Angoka是NCSC网络加速器项目的光荣校友。我们为广泛的应用提供解决方案，从关键的国家基础设施到陆地和空中移动性等，确保端到端的韧性和安全保障。

公司的宗旨是确保智慧城市和移动性的安全和韧性，智慧城市和移动性正变得越来越复杂，日益依赖由互联设备构成的网络和机器对机器的通信。我们的解决方案允许创建可信区域，运行去中心化的、无量子威胁的安全做法，实现动态更新，为攻击者提供始终移动的靶。也就是说，设备所有者可以完全控制它们的安全。

Angoka 团队在展示其解决方案

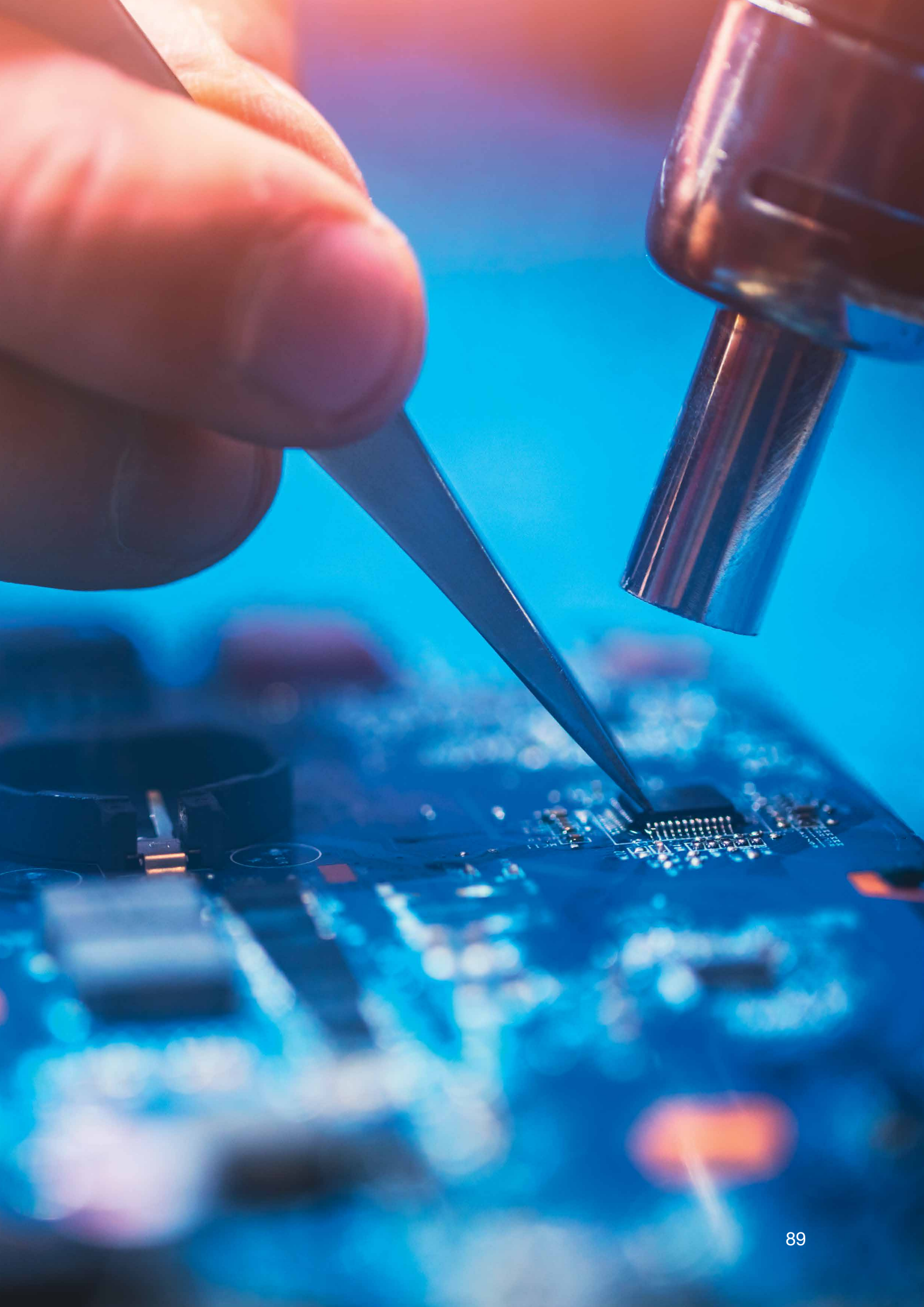
目标4：
与多利益相关方群体合作，在对维护我们的民主价值观、确保我们的网络安全以及推进英国战略利益至关重要的优先领域，通过科学和技术制定全球数字技术标准

148. 全球数字技术标准是互联网、电信网络和新兴技术运行的核心部分。它们的制定和部署方式会影响我们的网络安全目标、经济繁荣以及我们的规范和价值观。从历史上看，这些标准是由那些最具市场力量的机构制定的，并且存在实质性的准入壁垒。这妨碍了一些重要的利益相关方，包括中小企业、学术界和其他专家的参与。到2025年，我们将实现以下成果：

149. 全球数字技术标准生态系统中的多利益相关方参与度更高。我们将加强多利益相关方在关键标准制定组织中的参与，并通过我们派往国际电信联盟（International Telecommunication Union）的代表团树立榜样。我们将通过联合国互联网治理论坛（UN Internet Governance Forum）和其他论坛，促进决策者就关键趋势和考虑因素进行开放的讨论。我们将加强与国际合作伙伴的协调和信息共享，包括通过在英国担任七国集团（G7）轮值主席国期间成立的数字标准联络点小组（Digital Standards Points of Contact Group）。

150. 英国的优先领域的全球数字技术标准将更有效地得到民主价值观、网络安全考虑以及英国在新兴技术领域的研究和创新的塑造。我们将在互联网协议、未来网络和人工智能等领域与行业、学术界、技术专家和民间社会合作，以提高对技术标准制定中重要公共政策考虑因素的认识。正如如《国家人工智能战略》（National AI Strategy）中所述，我们将试点人工智能标准中心，以支持英国在人工智能标准化方面的全球参与。

151. 所有这些工作都将得到英国国内战略协调机制的支持，例如政府、英国标准协会（BSI）和国家物理实验室之间的《国家人工智能战略》中提出的倡议。这种参与还将通过促进支持创新、促进增长和均衡发展的标准来支持英国的繁荣。



支柱四：
全球领导力

提升英国的全球领导力和影响力，建立安全繁荣的国际秩序

152. 一个自由、开放、和平和安全的网络空间对于我们的集体安全和繁荣仍然至关重要。国际参与对于实现所有英国网络战略目标仍然意义重大。然而，为了应对一个系统性竞争的时代，英国现在将发挥更积极的国际领导作用，促进我们在网络空间的利益和价值观。英国在网络空间的活动以及我们的网络专长也将被置于实现政府更广泛的外交政策议程的核心：我们将主动利用它们来帮助实现一个开放、安全和繁荣的国际秩序。

153. 我们将加强我们的核心联盟，同时作为一个解决问题、分担责任的国家，与更广泛的合作伙伴合作，包括行业、全球技术标准机构、民间社会和学术界。我们将进一步投资，与非洲和印度太平洋地区的合作伙伴建立更深的关系，并抓住机会建立新的、更敏捷的联盟。我们还将继续加强我们的外交手段，把我们在海外的影响力与国内实力联系起来，利用我们的行动和战略沟通专长、技能项目和经济伙伴关系，成为一股积极的全球力量。我们的做法符合全球安全和繁荣的利益，而不仅仅是我们自己的利益。

目标 1：加强国际伙伴的网络安全和韧性，增加集体行动以瓦解和威慑对手

154. 集体的行动和彼此共有的韧性对于应对上游威胁至关重要，同时也能减少网络威胁行为者对英国及其伙伴实施攻击的动机。到2025年，我们将实现以下目标：

155. 英国的国际伙伴拥有更强的能力、政治决心、治理和系统来调查和破坏网络威胁，并且建立韧性。这将减少英国公民面临的海外威胁。我们将优先在东欧、非洲和印度太平洋地区提供网络能力建设援助，并继续与中东和美洲的主要盟友合作。我们将建立一个更加一体化的政府整体技术方案，加大对执法和国防专长的投资，更多地听取英国行业和学术界的意见。我们的重点将是保护关键的国际供应链和基础设施，促进数字技术的安全使用，并与行业伙伴一起大规模开展这项工作。

156. 我们还将做更多的工作来建设民间社会组织的能力，让围绕技术和社会的由价值观驱动的辩论得以实现，同时建立地方问责机制。我们将继续与有效的多边组织和伙伴合作，包括联合国、五眼联盟、北约、七国集团、欧盟、英联邦、经合组织、全球网络专业知识论坛（GFCE）、东盟论坛、非洲联盟和世界银行等。

157. 为了加强对英国海外利益和公民的保护，我们还将为英国海外使团开发和实施一项国际网络卫生运动，该运动将在当地定制和实施。其目的是提高恶意活动的成本，如黑客攻击、数据和知识产权窃取以及勒索软件等。该活动将通过我们的外交官、当地国家工作人员、当地英国商界和英国发展项目的执行者来开展。

158. 一个更广泛的国际联盟，愿意并且能够对英国的对手施加更有意义的影响。我们将通过更多的外交交流、行动协作、信息共享和联合演习来增强国际决心与能力。通过政策、行动和执法渠道，我们将加大措施的影响力，如有采取针对性的网络制裁，识别新的工具来提高网络威胁行为者的行为成本。我们将在主要盟国和伙伴国家的网络力量之间建立更深的相互理解，并将网络作战更好地融入所有领域的盟国作战，包括陆地、海洋、天空、太空和网络空间。

159. 我们将继续支持发展北约联盟的网络安全能力，以加强集体行动，包括支持将英国和其他一些盟国自愿提供的主权网络影响力纳入北约行动和任务。

目标 2:
塑造全球治理，促进自由、开放、和平和安全的网络空间

160. 不认同英国价值观的国家利用自由开放的互联网所带来的挑战，在安全的幌子下推进他们对网络空间的专制愿景。英国将采取更加主动的方式，与我们的盟友和伙伴合作，确保国际规则和框架的制定符合我们的民主价值观。我们的目标是支持国家和全球经济增长，加强集体安全，鼓励负责任地使用攻击性网络工具，并让恶意和不负责任的活动承担真正的后果。到2025年，我们将实现以下成果：

161. 网络空间和互联网的全球治理正在保护着英国的利益和价值观，英国和我们的合作伙伴具有更大的影响力 影响着国际治理和标准框架的制定和实施。我们将采取更加积极主动的方法来塑造网络空间的治理框架，以促进全球经济增长和安全。我们将设计并实施切实可行的步骤，为关于网络空间规则、规范和原则的应用的国际辩论消除障碍，并推动其就如何有效限制破坏性和破坏稳定的活动方面达成共识。我们将通过包括欧洲安全与合作组织（OSCE）、东盟和全球网络专业知识论坛（GFCE）在内的主要区域和专业组织来实现这一目标，并建设性地参与联合国进程，以制定一项新的国际网络犯罪条约，该条约将与《布达佩斯公约》平行，确保其加强国际合作并维护人权保护。

162. 我们还将继续推动《布达佩斯公约》打击网络犯罪，与国际伙伴合作，保持该公约的信服力，继续作为首要的国际合作协议。我们将继续推动和加强互联网治理的多利益相关方流程，包括互联网名称与数字地址分配机构（ICANN）和互联网治理论坛（IGF）。这些努力将得到我们制定全球数字技术标准的工作（在技术章节中阐述）和我们扩大英国网络安全出口的工作（如下所述）的补充，这也将有助于将英国标准嵌入其他国家的网络生态系统。

163. 大多数“中间地带”国家都支持和促进英国对网络空间和互联网未来的愿景，更成功地对抗专制国家对多利益相关方系统的影响。我们将展示，在不采取专制方式的情况下，解决网络空间的挑战是可能的，同时也能促进创新、发展和增长。我们将支持正在努力解决数字化问题的国家建立他们参与国际辩论和实施商定框架所需的全方位法律和战略传播专长。我们将继续揭露不负责任地使用网络能力的行为，在国际上建立信任。我们将继续展示我们在任何可能的情况下对使用攻击性网络能力所采取的开放和透明的态度，巩固英国作为正义力量的声誉。

目标 3：
利用和输出英国的网络能力和专长，以增强我们的战略优势，促进我们更广泛的外交政策和繁荣利益。

164. 为了应对系统性竞争和快速的技术变革，英国的网络活动和能力将与国家力量的其他来源一起纳入考虑，以加强我们的战略优势，促进我们的外交政策和繁荣目标。我们的目标是建立一种国际秩序，在这种秩序中，开放的社会和经济体能够繁荣发展，人权得到保护，同时推动国内的繁荣。到2025年，我们将实现以下成果：

165. 我们在网络空间的活动以及与网络空间有关的活动加强了全球稳定，保护了基于规则的国际体系、开放的社会和正在遭受破坏的民主制度 。我们将实施一场基于国际价值观的运动，在网络空间的设计、开发和使用中倡导人权、多样性和性别平等。这将包括但不限于解决互联网关闭、人工智能算法中的偏见问题以及提高在线安全性。我们将通过进一步投资于遍布六大洲的网络官员网络，更有效地进行竞争，以保护民主价值观、制度和程序，加强基于规则的国际体系（包括联合国、世界卫生组织和全球贸易体系）。我们将加强战略传播的使用，以促进英国的研究合作和学术交流项目，并帮助确保把英国的想法转化为实际应用。

166. 英国是全球三大网络解决方案和网络专长出口国之一，我们的网络行业被视为外国政府和主要商业客户网络安全解决方案的“首选”提供商。我们将在英国网络安全大使计划（UK Cyber Security Ambassador Programme）和我们的国际网络的支持下，通过更积极的国际政府间接触，展示英国网络安全的最佳水平。我们将在出口创新的每个阶段支持英国的公司成为有能力的出口商，吸引外来投资，并为中小企业提供更多支持，包括通过一个新的出口学院。[32] [33] 除了通过网络增长伙伴关系和英国网络生态系统章节中概述的其他工作以外，我们还将建立一个新的网络能力活动办公室，为主要出口活动提供更加结构化和协调的支持。

[32] 阐述见 《英国创新战略》（2021年）

[33] 英国国防和安全出口（UKDSE）出口学院（The UK Defence & Security Exports (UKDSE) Export Faculty）是一个在线学习和发展中心，面向国防和安全领域的中小企业，为网络安全公司提供特定模块。在学院注册可获得一个基于学习模块的课程计划，此外，还可获得英国国防和安全出口安排的活动的有价值的信息。

英国内罗毕数字接入项目查尔斯·祖玛 (Charles Juma)

我叫查尔斯·维松加·祖玛作为肯尼亚全球和跨政府的英国数字接入计划的成员，我领导、塑造和践行网络安全、数字发展、包容性和创业精神。我还支持冲突、稳定和安全基金（CSSF）网络项目组合下的补充项目。在线安全、保障、数据保护和负责任地使用网络空间的重要性值得一再强调。我们从新冠肺炎疫情中学到，网络安全和卫生与公共健康和卫生同等重要。作为英国政府整体网络力量的一部分，我热衷于确保每个人都免受网络威胁和伤害。

驻第比利斯英国大使馆的网络官员萨拉·麦钱特（Sara Merchant）

我是萨拉，我被派驻到英国驻第比利斯大使馆，担任我们的网络官员，与格鲁吉亚政府和英国NCSC密切合作。我的日常工作涉及从政治参与到支持新网络战略的实施，再到通过英国的专家提高格鲁吉亚的技术能力。我很荣幸能够处于最前沿，展现英国的专长，支持格鲁吉亚增强抵御网络威胁的韧性。我们可以在格鲁吉亚，这个不幸作为一个在敌对国家活动中有大量经验的国家这里学到很多东西。我们的工作让我们变得更强大、更有韧性、掌握更多信息。

支柱五：
应对威胁

侦测、瓦解、威慑我们的对手，以增强英国网络空间的安全

167. 我们面临的威胁的本质很复杂。我们担心网络空间的威胁（比如对我们在线活动的威胁）、通过网络空间对英国和伙伴的威胁（比如对联网的英国关键国家基础设施的威胁），以及对支撑国际网络基础设施功能的威胁。所有这些威胁都可能影响人们所依赖的服务的可用性，或通过这些系统传输的数据和信息的保密性或完整性。如本文前面所述，我们应对威胁的方式的基础是促进网络韧性。本章重点关注我们将如何提高在网络空间攻击英国的成本和风险，以及确保我们充分实现作为网络强国的潜力。

168. 自发布《2016-2021年国家网络安全战略》以来，我们已经转变了减轻威胁的方法。作为国家网络安全中心（NCSC）的一部分，我们建立了世界级的网络威胁侦测和分析能力。NCSC与国内外公共和私营部门的伙伴合作，侦测并应对威胁和事件。NCSC作为我们情报社区的一部分，还能够就针对英国利益的攻击的归因向决策者提供信息，这是我们遏制网络威胁的方法的一个关键部分。我们通过国家进攻性网络计划（National Offensive Cyber Programme）和现在新的国家网络部队（NCF）对我们的进攻性网络能力进行了大量投资。我们还制定了一个由国家打击犯罪署（NCA）牵头的一体化国家执法响应，并寻求瓦解网络空间的敌对和犯罪活动以及提高其成本。我们已经创建了世界一流的威胁侦测和评估能力，能够将由此产生的洞见转化为公共和私营部门可有效减轻风险的措施。我们还开发了一个自主的网络制裁机制，作为让敌对行动者付出代价的另一种手段。我们将外交沟通、NCSC、安全和情报机构、NCA、执法部门、NCF联合在一起，通过采取行动直接反击对手、帮助防止攻击、减少伤害，减少了威胁对现实世界造成的影响。

169. 但是，这些威胁的水平、复杂性和严重性也在提高；我们的努力还没有从根本上改变那些继续成功针对英国及其利益的攻击者的风险计算。针对英国的网络攻击的动机有间谍活动、犯罪、商业、金融和政治利益、破坏及虚假信息。攻击者开发可躲避减轻风险措施的能力；越来越复杂的网络工具和相关赋能工具已经在一个处于增长的行业中商品化，降低了所有类型的恶意行动者的准入门槛。随着行动者窃取和加密有价值数据的能力不断增强以及勒索软件赎金支付的增长，回报也在增加，同时扰乱企业和关键公共服务。结果是攻击者越来越多地从经济上获利、利用隐私和言论自由，并试图通过传播虚假信息操纵事件。

170. 因此，英国的应对方式现在将转向更加整合和持续的行动立足点，这将涉及常规、整合地、创造性地利用各种可用的手段和能力，让我们的对手付出代价，追查和瓦解犯罪分子，遏制未来的攻击。这一方式的关键支持要素将是：

- 持续发展NCF，这是英国对对手实施进攻性网络行动能力建设的下一步
- 有针对性地开展跨政府部门活动，应对英国面临的威胁——利用我们的外交、军事、情报、执法、经济、法律和战略沟通工具
- 进行新的投资，使执法部门能够以一定的规模和速度进行调查，并保持相对于我们对手的技术优势，从而防止和侦测严重犯罪分子及其依赖的赋能服务
- 《韧性》章节中阐述的跨政府部门和行业数据共享的重大进步

171. 网络空间为英国提供了机会，创造了积极追求我们国家利益的新途径。例如，进攻性网络行动为我们提供了一系列灵活、可扩展、缓和紧张局势的措施，这些措施将帮助英国保持战略优势，实现国家优先事项，且通常可避免将个人置于人身伤害风险当中。

172. 我们将通过NCF持续发展和投资于我们的进攻性网络能力。NCF将改变英国在网络空间和现实世界中与对手竞争的能力，以保护我们的国家、人民和生活方式。这些能力将与外交、经济、刑事司法和军事力量一道，负责任地作为一种向善的力量使用。它们将用于支持和推进一系列广泛的与国家安全、经济福祉相关的政府优先事项，并为防止和侦测严重犯罪行为提供支持。

目标1：
侦测、调查、分享关于国家、犯罪和其他恶意网络行动者和活动的信息，以保护英国、英国利益和公民。

173. 到2025年，我们将实现以下成果：

174. 政府全面了解国家、犯罪和其他恶意网络行动者的网络能力和他们对英国的战略意图。我们将保持并扩大在2016年战略下对情报机构和执法部门的大量投资，以了解网络威胁。特别是，我们将增强执法能力，以了解和应对网络犯罪威胁，包括其与国家和其他国际、国内威胁的联系及其技术手段，帮助我们制定更有效的对策。我们将通过情报机构和执法部门之间的联合数据共享和利用战略，改进我们在政府各部门之间协调威胁侦测的方式。我们将更加注重了解我们对手的意图和决策标准，以及我们的活动对他们的影响，包括个人是如何成为网络罪犯的，以及我们可以采取什么行动来防止这种情况的发生。

175. 《韧性》章节中概述的我们旨在实现更快、更容易地报告网络事件和犯罪的工作也将有助于实现这一成果。

176. 最严重的国家、犯罪、和其他威胁都会得到例行和全面的调查，利用所有信息来源，汇集政府、执法部门和私营领域的专长。我们将建立英国执法部门网络方面的情报、行动和技术能力。我们将投资于NCA的网络情报能力，用于针对有组织犯罪集团；区域情报建设倡议，这将加强整个英国的情报获取和流动能力；以及执法部门调查和瓦解网络和数字犯罪所需的技能和能力。

177. 调查将得到所有来源的情报的支持，并利用私营领域的技能和知识，包括通过帮助企业更容易地与执法部门共享数据。我们将继续实施HMICFRS关于针对网络犯罪的警务响应的建议，以确保国家、地区和地方各级网络犯罪网络保持安全。[34]

[34] 英国警察、消防和救援服务监察署（Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services）

178. 关于威胁的信息和数据常规地大规模、快速共享，信息接收方更有能力采取行动。NCSC试行了一些列举措，在各领域建立更有效的网络捍卫者社区，他们不仅能够接收和分享威胁信息，而且越来越有能力利用这些信息造福集体。我们将扩大这项工作，最初的重点是在政府网络协调中心（Government Cyber Coordination Centre）（在《韧性》章节有所描述）的支持下，帮助政府更好地捍卫自己。金融行业网络协作中心（Financial Sector Cyber Collaboration Centre）已在私营领域处于领先地位。[35]

179. NCSC也在研究追踪新威胁的方法，并继续与阿兰·图灵研究所合作，探索机器学习是否可以用于侦测某些类型的网络攻击。这项研究将继续提高我们对如何使用人工智能来侦测恶意活动的理解。

[35] NCSC，金融行业网络协作中心（FSCCC）（2021）

阻止网络犯罪也意味着应对其他类型的犯罪活动

网络犯罪（定义为《计算机滥用法案》犯罪）是指未经授权访问计算机、网络、数据和其他数字设备，造成损害的相关行为，或制造或提供实施这些犯罪的工具。这可能会让网络犯罪份子实施进一步的恶意网络活动，如勒索软件攻击、未经授权的帐户访问、知识产权盗窃、拒绝服务（DoS）攻击或窃取大型个人数据集，这些都是重大且不断增加的犯罪。

对公民而言，网络犯罪往往表现为这些犯罪促成或助长的进一步犯罪。未经授权的计算机访问会导致各种各样的欺诈、盗窃、性勒索，在某些情况下还会助长跟踪、家庭暴力、骚扰等。所有这些犯罪每天都对英国公民造成重大伤害，摧毁企业、毁掉生活。因此，网络犯罪不同于更广泛的在线安全问题，如欺凌和骚扰、仇恨言论、传播虚假消息、宣扬帮派文化和暴力，或未成年人接触色情制品。政府正在通过在线危害白皮书和在线安全法案草案应对这些问题。

目标2：
遏制和瓦解针对英国、英国利益和公民的国家、犯罪和其他恶意网络行动者和活动。

180. 到2025年，我们将实现以下成果：

181. 国家、犯罪和其他恶意网络行动者以英国为目标的代价更高、风险更大。我们将实施持续的和有针对性的遏制行动，利用英国的全部能力（包括外交、经济、秘密和公开手段）来影响恶意和犯罪网络行动者的行为。特别是，我们将更好地向对手发出信号，表明我们有能力也有意愿通过制裁、执法、NCF行动等方式，施加有意义的成本。我们将通过NCA的“网络选择”计划，引导个人不要参与网络犯罪，并与产业界和学术界合作，为潜在违法者提供更好的选择，如学徒制或实习工作。

182. 我们还将通过《反国家威胁法案》、更新现有立法并引入新的罪行，反映出国家威胁的演变，为执法和情报机构提供所需的工具和权力。并且，我们将修订《2002年犯罪收益法案》，以优化执法部门识别、没收、追回网络犯罪收益的能力。特别是，我们将通过建立民事没收权力来减轻那些无法被起诉的人带来的风险。

183. 由于我们对国家、犯罪和其他恶意网络行动者活动和能力的瓦解和贬斥，他们将更难将英国作为目标。我们将评估政府应对勒索软件的政策和行动方案，将此作为我们的优先活动之一，与行业和国际伙伴合作。我们将最大限度地加强NCF、NCSC、NCA及整个执法部门与外交和情报界之间的伙伴关系，以应对破坏网络空间或网络空间数据和服务的保密性、完整性、可用性的威胁特别是，我们将投资于针对网络犯罪基础设施的能力，部署我们的执法和进攻性网络能力，以瓦解恶意网络活动。我们的对手正在建立网络能力，并越来越多地将其用于恶意目的。我们将在我们认为合适的地方充分利用NCF，来瓦解这些行动，捍卫和保护英国。

184. 我们还将打击高端网络能力通过商业和犯罪市场向国家和有组织犯罪集团的扩散，打击那些助长、便利、美化网络犯罪的论坛。

185. 随着英国用于起诉网络犯罪份子的刑事司法能力的提高，**对于网络犯罪份子的刑事司法和其他破坏性后果随之增加。**我们将评估《计算机滥用法案》(CMA)和相关权力，以确保执法机构有能力调查来自犯罪分子的新威胁，并引入更多专业检察官来处理越来越多的网络案件。我们还将通过国家警察局长理事会(NPCC)网络技能计划书和警务学院网络数字职业路径(College of Policing Cyber Digital Career Pathways)，提高专业执法技能，将其纳入主流，以确保可以不断提供具备所需网络专业知识的执法官员。

北爱尔兰警察服务署(PSNI)预防事务官员苏珊·穆迪(Susan Moody)

从左到右：苏珊·穆迪(Susan Moody)(PSNI)、莎拉·特拉弗斯(Sarah Travers)(电视主持人)、乔·多兰(Joe Dolan)(北爱尔兰网络安全中心负责人)

电脑和移动设备是年轻人日常生活的一部分。它们带来了巨大的机会，但如果被滥用也会带来危害。PSNI的预防职能部门为年轻人提供了急需的早期干预，并帮助他们了解使用和滥用计算机的相关法律。其突出了潜在犯罪活动的危险迹象，也突出了“网络优先”(CyberFirst)和“网络为职业”(cyber as a career)等计划带来的巨大机遇，这些计划可以为那些有好奇心或天赋的人提供违法以外的选择，防止被他人滥用于犯罪目的。苏珊孜孜不倦地制定了一个适用于所有中学的学校网络信息计划，并与40多所小学、数所中学、青年组织和制服团体直接接触。这些年轻人很可能成为我们未来的网络大使和捍卫者。

目标3：
在网络空间中及通过网络空间采取行动，支持我们的国家安全及预防和侦测严重犯罪

186. 到2025年，我们将实现以下成果：

187. 英国的网络能力在遏制和瓦解非网络威胁方面具有更大的影响力。我们将扩大和发展NCF，实现我们对这一关键能力的长期愿景，确保它与英国政府通讯总部（GCHQ）、国防部（MOD）、秘密情报局（SIS）、国防科技实验室（Dstl）完全整合，并与执法部门和整个政府密切合作。我们将通过NCF实施合法、适度的进攻性网络行动，在网络空间负责任地行动，并以身作则。进攻性网络行动将继续支持英国的国家安全，包括我们的国防和外交政策，以及预防严重犯罪。

188. 我们还将扩大和发展针对基础设施和加密货币的执法技术能力，它们可用于应对其他威胁。

189. 根据《2025年综合作战概念》，**英国的网络能力被整合到国防行动的所有领域**。[36] 这将保持我们相对于对手的作战竞争优势，并使我们与盟友和伙伴的协作更加紧密。我们将继续推进国防多领域整合变革计划（Defence Multi-Domain Integration Change Programme），这将整合各领域的能力，并与我们国家权力的其他工具实现更大程度的整合，增强我们相对对手的军事优势。网络将成为国防事业的一个主流部分，这将得益于高技能的网络专家、国防员工的整体网络意识和先进、有韧性的网络能力。

[36] 国防部，《综合作战概念》（2020）

执法部门重大网络犯罪调查

Imperil行动：Imperil行动是东南地区打击有组织犯罪小组（SEROCU）与美国联邦调查局针对一个网站的联合调查，该网站出售网络攻击受害者被窃的个人和银行信息。这让他人可以购买个人数据来实施欺诈和进一步的计算机滥用违法行为。通过大量调查，查明了用于技术基础设施的银行账户和付款信息，确定了网站所有者位于巴基斯坦。这使得美国联邦调查局能够秘密查封该网站，并在随后将其关闭。东南地区打击有组织犯罪小组逮捕了主要的英国嫌疑人，发现该嫌疑人代表网站所有者开立了一个美国银行账户，用于清洗犯罪资金。这位英国嫌疑人犯下了重大欺诈罪，其利用一些被窃的受害者数据、以其他姓名开立银行账户、利用被窃银行账户支付豪华假期、向就业与养老金部索要虚假款项，导致国家损失超过90000英镑。该嫌疑人被控九项罪名，被判处四年有期徒刑，因其提前认罪得到减刑。案件法官授予调查组法官嘉奖（Judge's Commendation）。在发布信息时，没收和根据《犯罪收益法案》的终身处罚申请正在进行。

Nipigon行动：这是大都会警察对一名保加利亚国民的调查，该人涉嫌创建定制的钓鱼网页，估计给英国造成了超过4000万英镑的损失。他身份的确定发生在对另一名知名网络犯罪分子进行调查后，该网络犯罪分子此前在2018年被判处10年监禁，曾使用该保加利亚国民创建的钓鱼页面来实施自己的犯罪行为。调查是在确定了与嫌疑人有关联的一个重要电子邮箱地址后开启的，经过多次持久复杂的调查，带来了与保加利亚当局的接触及嫌疑人的逮捕和引渡，并在全面披露后，嫌疑人对所有刑事指控认罪，被判处九年半监禁。

Leasing行动2020年，NCA牵头了一项调查，调查在COVID-19疫情高峰期针对英国国家医疗服务体系（NHS）的恐怖炸弹威胁，其要求支付比特币（BTC）。NCA与德国当局合作，确定并逮捕了嫌疑人，该嫌疑人在德国法院被成功定罪。

2020年4月12日，一名居住在德国的意大利国民通过TOR网络发送了一封电子邮件，称他打算炸掉一家NHS医院，除非他收到价值1000万英镑的比特币。

这很快被NCA确定为高优先级事件，专门的网络犯罪官员受命查出肇事者并防止任何潜在的攻击。

该名肇事者还发送电子邮件威胁要袭击英国议会成员和在伦敦用炸弹袭击“黑人的命也是命”（Black Lives Matter）抗议者。尽管他的电子邮件是用英语写的，NCA的调查人员利用专门的网络技术以及行为和语言分析，推断出这名肇事者很可能是一名母语为德语的人。

在与德国当局的合作中，NCA官员确定了这些邮件是从一台位于柏林的电脑上发出的。通过国际合作，尽管该嫌疑人为掩盖其身份和位置付出了巨大努力，他还是被德国执法部门确认并置于监视之下。2020年6月15日，嫌疑人被捕，指控勒索未遂，并被还押候审。他于2021年2月26日被定罪，判处三年监禁。

通过网络空间采取行动打击恐怖主义

反达伊沙（Daesh）运动：国防部和政府通讯总部针对达伊沙的工作展示了我们如何采取积极措施来反击那些利用互联网和现代通讯力量的人的威胁。

达伊沙在技术上投入了大量时间和精力，创造媒体内容，用来煽动和吸引新成员，并在世界各地激发恐怖袭击。近年来，我们已经在整个欧洲看到这种方法的影响，包括伦敦和曼彻斯特的袭击事件。达伊沙还使用现代通信系统来指挥和控制他们的战场行动。这使他们能够灵活行动，具有规模和速度，对他们试图控制的人口构成更大的威胁，并最大限度地扩大他们在所谓的“哈里发国”（caliphate）的势力范围。

在自行宣布的达伊沙首都的摩苏尔战役中，我们在支持联合军队的军事行动中使用了网络工具和技术，将其作为更广泛、全方位战役的一部分。这些行动带来了广泛的成果。中断通讯、摧毁宣传、造成团体内部的不信任、剥夺作为其行动一部分的设备和网络，都是可以降低达伊沙的有效性的方式。我们还可以利用网络技术向目标宣传英国政府的信息，或向那些可能无意中给他们提供援助的人强调他们的活动。这些行动对联军压制达伊沙宣传的努力做出了重大贡献，阻碍了他们协调攻击的能力，并在战场上保护了联合军队。

国家网络部队的成员安德鲁（Andrew）

我一直对最新的尖端技术感到着迷。在为情报部门工作之前，我加入了警察队伍，从一名巡逻警员一路晋升到专门从事数字取证的工作——从嫌疑人的电子设备中寻找证据。我非常喜欢这个工作，但也想看看还有什么其他的机会。

我离开学校后没有上大学，到目前为止，我的职业生涯都是由一种天生的好奇心驱使的。我所有加入国家网络部队的同事都是如此。他们来自各种背景。有处于这一切核心的技术深厚的专家，也有前超市分店经理、小学教师、消防员。我们所有人都有的一个共同点就是开放的心态、对学习的渴望，以及保卫国家安全的共同目标，看到新兴技术给国家安全带来的威胁和机遇。

作为一名警察，我曾为能在个人层面帮助人们感到非常自豪。今天，作为国家网络部队这个独特团队的一员，我是全球层面正义力量中的一员。

实现我们的雄心

190. 如果没有严格的方法来实现目标、监测和评估进展情况，以及在必要时调整方向的机制，这一战略将毫无意义。本章阐述了我们实现目标的方法。

政府各部门的职责

191. 国家网络战略将是集体实现《整合评估》雄心的子战略之一。国家安全委员会将对这些战略进行部级监督，监测执行情况，并考虑英国战略的总体平衡和方向。实现该战略目标的进展情况也将通过政府规划和绩效框架以及成果交付计划来进行评估。

192. 所有部长都发挥作用，确保英国巩固其作为负责任、民主网络强国的地位，能够保护和促进其在网络空间的利益。这份清单包括担任领导角色的部长们的一系列具体职责，或是实施或协调国家网络战略五大支柱中的一项或多项，或是监督我们最重要的网络能力和决策。

- **兰卡斯特公爵郡大臣，**在**财政部主计长**的支持下，提供跨部门的全面领导，确保政府有效应对网络威胁，并实现我们作为网络强国的雄心。这包括国家网络战略的制定和实施、投资支持方案、政府在加强网络韧性方面工作的协调。他们还对英国关键国家基础设施的网络安全和韧性负有全面的跨部门政策和协调责任。在有必要召开关于网络事件的部长级COBR会议时，兰卡斯特公爵郡大臣是默认的会议主席。

- **内政部国务大臣** 在实现整体国家网络战略和根据其国土安全职责应对网络事件方面具有关键作用。他们与外交、联邦和发展事务大臣和国防大臣一起领导政府在侦测、瓦解、威慑我们对手方面的工作，并提供这项工作的总体协调。他们还有打击网络犯罪方面的具体责任。
- **外交、联邦和发展事务大臣** 对政府通讯总部及国家网络安全中心负有法定责任。他们领导政府的工作，推进英国在网络方面的全球领导力，并负有网络归因流程、网络制裁制度、高级别网络事件国际参与方面的具体责任。他们还与内政大臣和国防大臣一起领导政府在侦测、瓦解、威慑我们对手方面的工作。
- **国防大臣** 与外交、联邦和发展事务大臣和内政大臣一起领导政府在侦测、瓦解、威慑我们对手方面的工作。
- **外交、联邦和发展事务大臣和国防大臣**对国家网络部队负责，这是国防和情报部门的联合项目。
- **数字、文化、媒体和体育大臣**领导更广泛经济中组织的网络安全，因为其涉及数字政策，以及领导国家网络战略的相关增长、创新和技能方面的工作。他们领导的政府工作是为了加强英国的网络生态系统，以及在对网络力量至关重要的技术方面处于领先地位。
- **负责关键国家基础设施的所有主要政府部门的部长们** 对其部门的网络安全和韧性负有责任。
- **所有部长** 应监督其部门的网络安全并实施适当的减轻风险的措施。如果某个部门监管公共或私营部门的某个组成部分（如均衡发展、住房和社区部（DLUHC）与地方政府，或环境、食品和农村事务部（DEFRA）与水务公司），他们对与该部门相关的网络政策和保证活动负有责任。

193. 负责情报、安全和韧性的国家安全副顾问是该战略的高级负责人，将在各部门相关高级官员的支持下，领导政府各部门在官方层面的实施工作。

部长责任

*提供跨部门的全面领导，确保政府有效应对网络威胁，并实现我们作为网络强国的雄心。

投资于我们的网络力量

194. 政府将在未来三年投资26亿英镑用于网络和遗留信息技术上。这是在对国家网络部队大量投资以外的投资。它包括在国家网络安全计划中增加1.14亿英镑，将基于2016年战略的能力建设年度支出转移到部门管理下，并建立在长期的基础上。通过冲突、稳定和安全基金（CSSF）实施国际项目，以援助伙伴国家，建设其网络韧性和应对网络威胁。与此同时，还宣布了增加在研发、情报、国防、创新、基础设施和技能领域的投资，所有这些都将在一定程度上提升英国的网络力量。[37]

对成功的衡量

195. 该战略将遵循一个不断发展的绩效框架，向高级负责官员和国家安全委员会报告。该框架将用于指导与议会和监督国家安全部门工作的其他机构的讨论。与《2016-2021年国家网络安全战略》采用的方法一致，由于包含敏感信息，此文件不会公开，但政府将发布年度进展报告。

196. 该绩效框架将：

- 提供一条清晰的路径，说明活动将如何实现战略中概述的各种目标
- 确保实现战略的问责制
- 提供国家在实现该战略中提出的目标进展方面的透明度
- 说明活动需要如何适应，以使其符合该战略
- 了解哪些活动对实现战略雄心是有效的，以便未来可以应用这些经验教训
- 提供跨五大支柱活动的整体考量，减少重复并识别国家网络力量的优势和劣势
- 确保该战略为社会各界提供网络支持

[37] 英国财政部，《2021年秋季预算和支出评估报告》（2021）

后续步骤

197. 该战略旨在作为行动指南，不仅适用于政府中负责网络和其他相关政策的人员（见附录A），也适用于整个社会中对我们的国家网络工作感兴趣和负有责任的每一个人和组织。这也是我们希望可以持续下去的对话的开始，以确保我们的目标和优先事项在未来五到十年内仍然保持相关性。我们将把该战略的发布作为一个平台，与全英的公共、私营和第三部门进一步合作，并邀请大家将反馈直接发送至 ukcyberstrategy@cabinetoffice.gov.uk。我们将每年汇报该战略实施工作的进展。

附录A: 网络是政府更广泛议程的一部分

《国家网络战略》旨在支持和扩大政府在安全、国防、外交政策和经济议程方面的一系列其他优先事项。反过来，该战略将依赖于通过我们的教育和技能体系发展起来的更广泛的能力，以及我们对数字和技术产业政策、研究和商业增长的国家方针。关键相关战略和计划包括：

- **《整合评估》**，包括国家努力增强韧性，应对国家威胁、严重的有组织犯罪和恐怖主义，通过科学和技术保持我们的战略优势及塑造国际秩序。
- **《国家数据战略》**，阐述了我们的愿景，即通过负责任地使用数据来提高生产力，创造新的企业和工作岗位，改善公共服务，支持更公平的社会，并推动科学发现，让英国成为下一波创新的先行者。这包括转变政府对数据的使用，通过解决部门间数据共享的障碍和提高数据质量来提高效率和改善公共服务。这对于支持我们的网络议程至关重要，例如确保我们能够整理和使用有关网络事件的高质量数据。
- **增长计划，**通过对基础设施、技能和创新的额外支持和投资，以及阐述了我们对创新主导型经济的雄心的**《创新战略》**，帮助我们 **“重建得更好”**
- **《数字监管计划》**，阐述了我们在监管数字技术方面的创新友好型方法，以促进繁荣并建立对这些数字技术使用的信任
- **《国家人工智能战略》**，旨在通过投资对人工智能生态系统的长期需求，支持向人工智能经济的过渡，确保英国做好人工智能技术的国家和国际治理，为英国迎接即将到来的人工智能转型十年做好准备。这还包括采取措施，支持人工智能系统中的网络安全创新、同时保护公众并建立对人工智能使用的信任
- 即将发布的**《国家韧性战略》**，将部分聚焦于英国如何应对技术威胁并在网络空间保持韧性
- 即将发布的**《数字战略》**，将阐明政府具有雄心的清晰愿景，利用对数字化转型的新需求，加快增长，并持续为未来构建更具包容性、竞争力、创新性的数字经济；这将建立在数字、文化、媒体和体育部（DCMS）的《十大技术优先事项》的基础上，进一步阐述政府在数字行业的雄心
- **《净零战略》，**确保我们繁荣、创新主导的经济是低碳经济
- **《打击犯罪计划》**，阐述了我们将如何重建人们对刑事司法体系的信心，并实现我们的共同愿景，即建立一个更安全的英国，减少犯罪和受害者[38]

[38] 内政部，《打击犯罪计划》（2021）

还有两份文件直接支持《国家网络战略》，它们阐述了如何实现该战略的各个部分。

- 即将发布的**《政府网络安全战略》**，将制定更详细的计划来提高政府和公共部门的安全性，以支持这一国家战略
- 即将发布的**《2021年激励和监管评估》**，将阐述我们在激励整个经济中网络安全改善方面的工作成效，以及我们建议如何实施韧性支柱的商业和组织要素

附录B:《网络与信息系统监管条例》——国家战略

介绍

《网络与信息系统国家战略》

1. 《国家网络战略》被指定为《2018年英国网络与信息系统(NIS)监管条例》第2条规定的英国国家战略。

2. 本附录提供了更多信息,包括:

- 英国负责NIS实施的主要机构的职责;和
- 所涉主要机构的名单。

《英国NIS监管条例》

3. 2016年,欧盟委员会就一项指令达成共识,旨在提高欧洲联盟(欧盟,EU)内部网络和信息系统的安全性。这得到了英国政府的支持。

4. 2018年4月20日,英国政府向议会提交了新的《2018年网络与信息系统(NIS)监管条例》。这些监管条例于2018年5月10日生效。

5. 《NIS监管条例》在英国建立了新的监管制度,要求指定的基础服务运营商(OES)和相关数字服务提供商(RDSP)采取技术和组织措施来保护其网络和信息系统的安全。

6. 它适用于对我们的经济和社会至关重要并严重依赖网络和系统的领域;能源、交通、饮用水、医疗保健、数字基础设施。

7. 关键数字服务提供商(搜索引擎、云计算服务、在线市场)也包括在内。

8. 《NIS监管条例》建立了:

- 支持实施的**国家框架**,包括国家战略;
- 作为具体行业监管机构的**主管部门**;
- 作为**单一联络点**(SPOC)和**计算机安全事件响应小组**(CSIRT)的国家网络安全中心(NCSC)。

9. 每隔2-5年通过《实施后评估》评估进展情况。

关键职责

国家框架

10. 内阁办公室负责国家网络战略，其中包括NIS国家战略。内阁办公室还整体负责提高关键国家基础设施的安全性和韧性。

11. 数字、文化、媒体和体育部（DCMS）负责《NIS监管条例》的整体实施，包括协调相关机构和NCSC。DCMS为主管部门发布指南，以支持NIS在英国的整体实施。

单一联络点（SPOC）

12. 与国际【欧盟】伙伴就NIS进行交流的国家联络点，协调行动或信息请求，并提交年度事件统计数据。国家网络安全中心是英国的SPOC。

计算机安全事件响应小组（CSIRT）

13. 国家网络安全中心是英国的CSIRT。它负责在国家一级监测网络安全事件；提供实时威胁分析、防御国家网络攻击、提供技术建议，以及对重大网络事件进行响应，以帮助将危害降至最低。

14. NCSC维护基于结果的网络评估框架（CAF），并作为国家技术权威机构就网络安全问题提供广泛指导。

主管部门

15. 他们负责在其行业监督和执行《NIS监管条例》，指定和评估OES和RDSP遵守《NIS监管条例》要求的情况。《NIS监管条例》第1节列出了具体内容，并在第3节提供了名单。

基础服务运营商（OES）和相关数字服务提供商（RDSP）

16. 符合该行业领域指定门槛的OES或RDSP，或由相关机构根据《NIS监管条例》第8（3）条指定的OES或RDSP，必须遵守《NIS监管条例》的要求。

17. 这包括：

- 采取适当和相称的技术和组织措施来管理网络和信息系统安全面临的风险；
- 采取适当和相称的措施，以防止和最大限度地减少影响网络和信息系统安全的事件的影响；
- 向有关主管部门通报任何对其服务有重大影响的事件；
- 符合《NIS监管条例》的检验要求；以及
- 遵守信息、执行和处罚通知。
- RDSP还需要向ICO注册。

其他相关部门：

18. 在执行《NIS监管条例》方面，英国政府与分权的行政部门和其他相关机构（包括主管的政府部门）密切合作。

19. 国家基础设施保护中心（CPNI）就相关的物理和人员安全提供咨询。

实施NIS的主要机构清单

国家部门	
《英国NIS监管条例》	数字、文化、媒体和体育部
《英国国家网络战略》	内阁办公室
英国单一联络点（SPOC）	国家网络安全中心
英国计算机安全事件响应小组（CSIRT）	国家网络安全中心

主管部门					
行业	**子行业**	**英格兰**	**威尔士**	**苏格兰**	**北爱尔兰**
能源	电力	联合：商业、能源和产业战略部与天然气和电力市场管理局（Ofgem）			财政部
	石油	商业、能源和产业战略部			财政部
	天然气	联合：商业、能源和产业战略部与天然气和电力市场管理局（Ofgem）[39]			财政部
交通	航空	联合：交通部和民用航空管理局（CAA）			
	铁路	交通部			财政部
	水运	交通部			
	公路	交通部		苏格兰部长	财政部
医疗保健	医疗保健场景	卫生和社会照护部	威尔士部长	苏格兰部长	财政部
饮用水	饮用水	环境、食品和农村事务部	威尔士部长	苏格兰饮用水质量监管局	财政部
数字基础设施	数字基础设施	通信管理局（Ofcom）			

[39] 在某些例外情况下，商业、能源和产业战略部是唯一的主管部门。更多详情请参见《2018年网络与信息系统监管条例》附表1和附表2。

附录C: 词汇表

COBR – 内阁办公室简报室。COBR的使用支持着英国中央政府对紧急事件的响应;其物理位置通常位于威斯敏斯特,从这里启动、监测、协调中央响应,并为政府响应提供焦点,为地方响应者提供权威建议。

GCHQ – 政府通讯总部;政府信号情报活动和网络国家技术权威机构(NTA)的中心。

GFCE – 全球网络专业知识论坛。

ICANN – 互联网名称与数字地址分配机构。协调网站名称与IP地址。

NCA – 国家打击犯罪署。

《2018年网络与信息系统(NIS)监管条例》– 为提供基本服务和数字服务提供法律措施以提高网络和信息安全水平(网络和物理韧性)的英国法规。

《数字监管计划》– 制定了政府管理数字技术的总体方案,从而推动增长和创新。

《整合评估》–《竞争时代的"全球化英国"——安全、国防、发展和外交政策整合评估》,描述了政府对未来十年英国在世界上的角色的愿景,以及政府到2025年将采取的行动。

主动网络防御(ACD) – 帮助组织发现和修复漏洞,管理事件或自动中断网络攻击。有些服务主要是为公共部门设计的,而其他服务则根据其适用性和可行性,更广泛地提供给私营领域或公民。

主管部门 –《2018年网络与信息系统(NIS)监管条例》中描述的监管机构。多个主管部门负责NIS覆盖的不同行业领域。

事件响应 – 用于解决事件的短期、直接影响,并且可能支持事件短期恢复的活动。

事件管理 – 活动管理与协调,以调查和补救实际发生或可能发生的危害或损害系统或网络的不良网络事件。

互联场所 – 整合信息与通信技术和物联网设备的社区,用于收集和分析数据,以为其建成环境提供新服务,提高公民生活质量。

互联网 – 一个全球计算机网络,提供各种信息与通信设备,包括以标准化通信协议相互连接的各个网络。

五眼联盟 – 五眼联盟是美国、英国、加拿大、澳大利亚、新西兰之间情报联盟的名称，该联盟帮助共享信息，以尽可能保护其公民免受威胁。

人工智能 – 一种技术，其中计算机系统被编码进行“独立思考”，自主适应和操作。人工智能越来越多地用于更复杂的任务，如医学诊断、药物研发、预测性维护。

关键国家基础设施 – 基础设施的关键要素（即资产、设施、系统、网络或流程，以及操作和辅助其运作的关键工作人员），其损失或损害可能导致：

a. 对基本服务（包括完整性一旦受损可能导致重大人员伤亡的服务）的可用性、完整性或交付产生重大不利影响，这包括重大的经济或社会影响；和/或

b. 对国家安全、国防或国家运作产生重大影响。

分权政府或分权行政部门 – 苏格兰、威尔士和北爱尔兰权力下放后的独立立法和行政部门，负责其区域内的许多国内政策问题，并有权制定这些区域的法律。

加密关键能力（CK）– 该术语用于描述英国使用加密技术来保护英国政府、军队和国家安全社区（包括让我们免受最强大对手的攻击）所依赖的关键信息和服务。

加密货币 – 一种数字货币与支付系统，如比特币。

勒索软件 – 一种要求用户支付赎金才能访问其文件、计算机或设备的恶意软件。

北约（NATO）– 北大西洋公约组织。

区块链技术 – 一种特殊的数据存储方式。区块链是分布式分类帐的一个例子，这是一种只添加、防篡改的存储技术。

反诈骗行动处 – 欺诈和网络犯罪报告中心，在英格兰、威尔士和北爱尔兰，如果公民和组织遭到诈骗、欺诈或遭遇网络犯罪，应向此机构报告欺诈行为。在苏格兰，向苏格兰警察局报告。

国家网络安全中心（NCSC）– 英国的网络威胁技术权威机构，对网络事件提供统一的国家响应，以最大限度地减少伤害、帮助恢复，并为未来吸取经验教训。

域 – 域名可用于查找组织或其它实体在互联网上的位置，并与互联网协议（IP）地址相对应。

基础服务运营商 – 严重依赖信息网络的重要行业中的组织，如以《2018年网络与信息系统（NIS）监管条例》中的标准确定的公共事业、医疗保健、交通、数字基础设施领域。

完整性 – 在信息安全中，完整性指的是信息未被意外或蓄意变更，且保持准确和完整。

密码学 – 分析与破译代码和密码的科学或研究；密码分析。

工业控制系统（ICS）– 用于控制制造、产品搬运、生产和分配等工业流程或控制基础设施资产的信息系统。

微型发电 – 家庭、小企业和社区的小规模发电。

托管服务提供商 – 向客户提供一组已明确的服务并承担运行、维护和保护这些服务安全的责任的第三方。

政府网络协调中心（GCCC）– 提议的GSG、CDDO和NCSC的联合机构，将各自的职能和专长领域结合在一起，从而更好地协调整个政府的网络安全工作，转变网络安全数据和威胁情报在整个政府的使用方式，并真正提高政府“一体防御”的能力。

数字孪生 – 建成、社会或自然环境中的资产、流程、系统或机构的虚拟复制或体现，提供对复杂物理资产和公民行为的洞见，帮助组织改进决策和优化流程。现实世界的变化反映在孪生中，孪生的变化亦可在现实世界中自动复制。

数据外泄 – 未经授权将网络上的信息迁移或披露给无权访问或查看这些信息的一方。

水平检视 – 对信息进行系统性检查以确认潜在威胁、风险、新问题和机会，从而更好地为政策制定流程做好准备，并且在政策制定过程中更好地结合缓解与利用。

漏洞 – 可能被攻击者利用的软件程序故障。

漏洞报告服务 – 一种让组织可以在安全缺陷被攻击者利用之前得到警告的机制。

物联网 – 嵌入能够通过互联网通信和交换数据的各种电子产品、软件和传感器的所有设备、车辆、建筑和其他物品。

经合组织（OECD） – 经济合作与发展组织，一个政府间经济组织。

网络事件 – 实际或可能对计算机、联网设备、网络或其系统中处理、存储或传输的数据构成威胁的事件，可能需要做出响应以消除其后果。

网络威胁 – 主要通过网络方式危害信息系统与互联设备（包括硬件、软件和相关基础设施）安全、危害该信息与互联网设备上的数据及提供的服务的任何事物。

网络安全 – 保护联网系统（包括硬件、软件和相关基础设施）、系统中的数据和它们所提供的服务，防止未经授权访问、危害或滥用这些系统、数据和服务。包括由于未遵守安全规程或受到操纵而由系统运营商故意或无意造成的伤害。

网络安全知识体系（CyBOK） – 一个独特的资源，首次提供了涵盖网络安全广度和深度的基础知识体系，表明网络安全涵盖了范围很广的很多学科。

网络攻击 – 蓄意刺探计算机系统、数字化企业和网络以造成伤害。

网络犯罪 – 依靠网络实施的犯罪（只能使用信息与通信技术设备实施的犯罪，其中信息与通信技术设备既是实施犯罪的工具，也是犯罪行为的目标）；或利用网络实施的犯罪（比如金融诈骗等可以不通过信息与通信技术设备实施，但可利用信息与通信设备大大改变其规模与范围的犯罪）。

网络生态系统 – 相互连接的所有基础设施、人员、程序、数据、信息和通信技术的总和，以及影响其互动的环境与条件。

网络评估框架（CAF） – 提供一种系统而全面的方法来评估负责组织对基本职能的网络风险的管理程度。

网络韧性 – 系统、组织和公民抵御网络事件，并从网络事件伤害中恢复的整体能力。

网络风险 – 特定网络威胁利用信息系统的漏洞并造成伤害的可能性。

自治系统 – 其路由处于某具体实体或域控制下的一系列IP网络。

设计即安全 – 从头至尾采用安全设计的软件、硬件和系统。

身份验证 – 验证用户、程序或设备身份或其他属性的过程。

运营技术（OT） – 结合硬件和软件来监测、控制、自动化物理过程，尤其用于能源、制造、水、运输等工业领域。

进攻性网络 – 添加、删除、操纵系统或网络上的数据，以产生物理、虚拟或认知效果。进攻性网络操作通常利用技术漏洞，以其所有者和操作者不希望或不容忍的方式使用系统或网络，并可能依赖欺骗或虚假陈述。

遗留IT – 遗留IT指的是不在供应商支持范围内的、享受扩展支持和/或定制支持的系统及其组建软件和硬件。

量子技术 – 量子技术依赖于量子物理学原理。我们对叠加和纠缠等所谓“量子效应”的理解和控制不断推进，将带来支撑我们经济和社会的新一轮进步，包括：传感、数据传输和加密、计时和计算。