HM Government

国家网络安全战略
2016-2021 年

目录

序

英国是世界领先的数字化国家之一。我们今天的繁荣很大程度上有赖于我们有能力保护技术、数据和网络免受我们所面临的诸多威胁。

然而网络攻击愈发频繁和复杂，一旦成功，破坏性更加巨大。我们正在坚决果断采取行动保护经济和英国公民隐私。

我们的国家网络安全战略提出的计划是，使英国在快速变化的数字世界中满怀自信、具备能力并保持韧性。

在此五年战略期间，我们将投资 19 亿英镑用于保障系统和基础设施，遏制对手，增强全社会——从大型企业到公民个人——的能力。

从最基本的网络健康到最复杂的遏制，我们需要全面回应。

我们将重点放在通过加强防御和优化网络技术来提高对英国任何人发动攻击所需的成本。这不仅对于信息技术部门，对于整个劳动力群体来说都是一个重要议题。网络安全的触角需要延伸到每个行业。

新的国家网络安全中心将会为公司和个人提供世界一流、用户友好的专业知识技能中心，在重大事件发生时快速应对。

政府有明确的领导职能，但是我们也将培养更加广泛的商业生态系统，识别在哪些地方行业创新速度要快过我们。这其中就包括推动最优秀的年轻人才进入网络安全领域。

网络威胁影响整个社会，因此我们想要非常清楚地表明，在国家应对方面人人有责。这也是为什么这个战略在透明度上前所未有。我们不能再关起门来讨论这个话题了。

最终，这一威胁不能被完全消除。数字技术能够发挥作用是因为它开放，这种开放性也带来了风险。我们能做的是将威胁降低到能保证我们仍然处于数字革命前沿的水平。本战略提出了相应的解决方法。

菲利普·哈蒙德（Philip Hammond）
议员阁下，
财政大臣

前言

我们的首要责任是维护国家安全，交付一个称职的政府。本战略就是对这些职责的反映。应对我们国家在网络空间中面临的诸多威胁是一种勇敢且雄心勃勃的做法。管理和减轻那些威胁是我们所有人的共同任务，但政府承认，自己有特殊的职责来牵头全国做出所需的努力。

政府决心确保本战略中提出的承诺得以履行，保证准确监测并定期报告进展情况。我们也将不断审视我们的做法，对我们所面临威胁程度以及安全技术发展方面的变化做出回应。

政府对本国公民、对在英国运营的公司和组织，以及国际盟友和合作伙伴也有特殊责任。我们应当能够向他们保证会尽一切努力维护系统安全，保护我们的数据和网络免受攻击和干扰。因此我们必须给自己设定并坚决遵守网络安全的最高标准，以此作为国家安全和经济福祉的基石，同时为他人树立榜样。我们会每年报告进展情况。

作为负责网络安全与政府安全的内阁办公室部长，我决心全面实施这一战略。我将与整个政府的同事以及地方分权政府、更广泛的公共部门、行业和学术界的合作伙伴们密切合作，确保我们实现这一宏伟目标。

本·古默（Ben Gummer）议员阁下，内阁办公室部长，财政部主计长

1.执行概要

1.1. 英国的安全和繁荣前景有赖其数字基础。我们这一代人的挑战是建设一个欣欣向荣的数字社会，这个社会既能应对网络威胁，又具备最大化各种机会和管理风险所需的知识和能力。

1.2. 如今互联网对我们来说不可或缺。然而互联网天生就不安全，始终会有人试图利用其漏洞发动网络攻击。这种威胁不能完全消除，但其风险可以大大降低，降低到能够使我们的社会继续繁荣并享受数字技术带来巨大机会的程度。

1.3. 在英国政府 8.6 亿英镑国家网络安全计划（National Cyber Security Programme）的支持下，2011 年实施的国家数字安全战略（National Cyber Security Strategy）大大改善了英国的网络安全。通过依赖市场推动安全网络行为，该战略取得了重大成果。不过该战略没有达到领先于迅速发展的威胁所需的变革规模和速度。我们现在需要更上一层楼。

1.4. 我们 2021 年的愿景是**让英国成为安全、能应对网络威胁的国家，在数字世界繁荣而自信。**

1.5. 为实现这一目标，我们将努力实现下列具体目标：

- **防御**。我们具有保卫英国不受日益发展的网络威胁、对事件做出有效反应，以及确保英国网络、数据和系统得到保护、具备韧性的各种手段。国民、企业和公共部门具有自我防御的知识和能力。
- **遏制**。英国将成为网络空间各种形式入侵难以得逞的硬目标。我们探测、了解、调查、破坏针对我们的敌对行动，追查、起诉侵犯者。我们具备在网络空间采取进攻行动的各种手段——如果我们选择这样做。
- **开发**。我们有一个创新且不断发展的网络安全行业，得到全球领先的科技研究与开发支持。我们有能够自我持续的人才输送渠道，这些人才提供各种技能满足公私领域的全国需求。我们先进的分析和专长使英国能应对、克服未来的威胁和挑战。

1.6. 为了支持这些目标，我们将通过投资于影响全球网络空间发展的各类伙伴关系来寻求**国际行动**和施加影响力，促进我们更广泛的经济与安全利益。我们将加深与我们关系最密切合作伙伴的现有联系，并认识到这将增强我们的集体安全。我们还将发展与新合作伙伴的关系，构筑他们的网络安全水平，保卫英国的海外利益。我们将通过双边和多边行动做到这一点，其中包括通过欧盟、北约和联合国进行。对于那些威胁在网络空间危害我们利益或我们盟友利益的敌人，我们将毫不含糊地警告这样做的后果。

1.7. 为了在接下来的五年实现这些成果，英国政府希望更加积极地予以干预，使用增加的投资，同时继续支持市场力量以提高全英国的网络安全标准。在与苏格兰、威尔士和北爱尔兰地方分权政府的合作下，英国政府将与公私部门一道，确保个人、企业和组织采纳在互联网保持安全所需的行为规范。我们将（在必要的情况下和在我们的权力范围之内）推出干预措施，推动符合国家利益的进步，尤

其是与我们关键国家基础设施网络安全相关的利益。

1.8. 英国政府将利用政府能力和行业能力开发、应用主动网络防御[1]措施，显著提高全英国网络的网络安全水平。这些措施包括，尽量减少最常见的网络钓鱼攻击、过滤已知有害 IP 地址，积极阻止恶意网络活动。基本网络安全改善将增强英国应对最常见网络威胁的韧性。

1.9. 我们已设立了全国网络安全中心（National Cyber Security Centre, NCSC），使之成为负责英国网络安全环境、共享知识、解决系统性漏洞、在关键国家网络安全议题上发挥领导作用的机构。

1.10. 我们将确保我们的武装部队具有韧性，具备保卫、防御其网络和平台所需的强大网络防御力量，从而能够在面对网络威胁的情况下继续行动和保持全球机动自由。我们的军事网络安全运营中心（Cyber Security Operations Centre）将与全国网络安全中心密切合作，我们将确保国家在遭受重大网络攻击的情况下武装部队能够提供支持。

1.11. 我们将具备应对网络攻击的各种手段，就像我们应对任何其他攻击一样，使用最合适的无论哪种能力，其中包括进攻性网络能力。

1.12. 我们将利用英国政府的权力和影响力投资从中小学到大学、到劳动力市场的各类项目，以解决英国网络安全技术人才的不足。

1.13. 我们将设立两个新的网络创新中心，以推动尖端网络产品的开发，推进充满活力的新网络安全公司的发展。我们还将安排 1.65 亿英镑规模的国防与网络创新基金（Defence and Cyber Innovation Fund）的部分资金支持国防和安全创新采购。

1.14. 我们将在今后五年总计投资 19 亿英镑，以显著改变英国的网络安全状况。

[1]了解网络威胁，然后制定、实施相关措施，以主动打击或防范这些威胁。技术术语解释参见词汇表。

2.介绍

2.1. 过去二十年来，信息与通信技术不断发展，如今几乎融入到我们生活的方方面面。英国已是一个数字化社会。我们的经济因此更加富裕，我们的日常生活因此更加丰富。

2.2. 这种数字化造成的转变形成了新的依赖。我们的经济、我们的政府行政、基本服务供给如今依赖网络空间的完整和支持网络空间的基础设施、系统和数据。对这种完整性失去信任将危及这一科技革命的益处。

2.3. 最初开发用于促进这种互联数字环境的软硬件很多优先考虑效率、成本和用户的方便，但并非是从一开始就具备安全设计。恶意分子——敌对国家、犯罪分子或恐怖组织及个人能够利用便利性与安全性之间的这一缺口。缩小此缺口成为了国家的一个优先事项。

2.4. 互联网的发展突破计算机和智能手机，进入其他信息物理或“智能”系统领域，这使远程利用的威胁扩大到一整套新技术。支撑我们日常生活的各种系统和技术——比如电网、空中交通管制系统、卫星、医疗技术、工业工厂和交通信号灯都接入互联网，因而可能容易受到干扰。

2.5. 2015 年国家安全战略（National Security Strategy, NSS）重申网络威胁是对英国利益的一级威胁。国家安全战略提出，英国政府决心解决网络威胁，“作为全世界网络安全领军者，推出强硬、创新的措施”。国家网络安全战略履行了这一承诺。

2.6. 英国政府以 2011 年发布的国家网络安全战略首个五年的成就、目标和判断为基础筹划这一新战略。在此期间，英国政府投入了 8.6 亿英镑，取得了骄人的成绩。过去五年制定的政策、制度和倡议推动英国成为网络安全的全球领军者。

2.7. 上述成果奠定了坚实的基础。然而，我们的威胁者执着又灵活，我们的漏洞又很普遍，我们的能力和防御还有差距，这意味着为了跟上威胁的发展，我们甚至需要更加努力。如果我们要有效确保我们的网络利益，必须全面采取办法。基于下列评估结果，我们决心作进一步投资和干预。

- 网络威胁的规模和活跃性，以及我们的漏洞与依赖性，意味着保持现行办法本身不足以维持我们的安全；
- 促进网络健康的市场化方式未产生变革所要求的速度和规模，因此，政府必须加以领导，更直接地予以干预，利用其影响和资源承担解决网络威胁的任务；
- 单凭政府不能提供国家各方面的网络安全。需采取内嵌的、可持续的方式，让国民、行业、社会和政府的其他合作伙伴充分发挥作用，确保我们的网络、服务和数据安全；
- 英国需要一个生机勃勃的网络安全行业，以及能够赶上并领先于不断变化的威胁的支持性技术基础。

本战略范围

2.8. 本战略意在影响英国政府的政策，同时提出具有内在一致性的、引人注目的愿景，与公私部门、公民社会、学术界和更广泛的人群共享。

2.9. 本战略覆盖英国全境。英国政府将确保英国各地实施本战略，认识到

实施过程中涉及地方事务时我们将与苏格兰、威尔士和北爱尔兰地方分权政府密切合作（尊重英国存在的这三个独立司法辖区和四套教育体制）。凡是本战略提出的与地方分权事务相关的建议，其实施将按照地方解决办法得到这些政府酌情同意。

2.10. 从中央政府各部门到各行业领袖和个人，本战略提出针对经济各行各业和社会的提议或建议行动。本战略旨在为了我们的共同利益加强各个层面的网络安全，成为英国在国际上促进良好互联网治理的基础。

2.11. 本战略“网络安全”是指保护信息系统（软硬件和相关基础设施）、信息系统中的数据，以及信息系统所提供的服务不受非法读取、损害或滥用。这包括信息系统操作人员有意造成的损害，或者因未能遵守安全流程造成的偶然损害。

2.12. 本文件与我们对所面临挑战作出的评估一致，基于 2011 年战略所取得的成就，特此提出：

- 我们对战略背景的最新评估，包括当前威胁和不断进化的威胁：谁对我们的利益构成最严重的威胁，以及他们所使用的工具；
- 评估各种漏洞，以及过去五年各种漏洞的发展情况；
- 2021 年英国政府网络安全愿景，实现该总目标的关键具体目标，其中包括指导原则、任务和职责，以及以什么方式、在哪些方面进行政府干预将产生效果；
- 我们打算实施政策的方式：确定政府在哪些方面加以领导，预计在哪些方面我们将与他人合作；
- 我们打算如何评估实现目标的进度。

3.战略背景

3.1. 当最新国家网络安全战略于2011年公布时，技术变革的规模和影响已经显而易见。当时所描述的各种趋势和机会之后加速发展。大量新技术和新应用涌现，全球范围内，尤其是发展中国家更大程度地采取基于互联网的技术为经济和社会发展提供了越来越多的机会。这些发展已经或将要给像我们这样的网络联通社会带来显著优势。不过随着我们对英国国内外网络的依赖加剧，那些设法危害我们的系统和数据的人的机会也增多。同样，地缘政治格局也发生改变。恶意网络行为没有国界之分。各国正在试验进攻性网络能力。网络犯罪分子拓宽他们的犯罪行为和战略手法，以从英国公民、组织和机构实现更高的价值回报。恐怖分子及其支持者正在进行低级别攻击，渴望开展更重大的行动。我们在本章评估这些威胁的性质、我们的漏洞及其持续演化情况。

威胁

网络犯罪

3.2. 本战略涉及两种犯罪活动形式互相相关的网络犯罪：

- 依赖网络的犯罪——只能通过使用信息与通信技术（ICT）设备实施的犯罪，这些设备既是实施犯罪的工具，也是实施犯罪的目标（比如开发、传播恶意软件获取经济利益，进行黑客活动窃取、损害、篡改或销毁数据和/或网络或活动）；及
- 借助网络的犯罪——通过利用计算机、计算机网络或其他形式的信息与通信技术，犯罪规模或范围得以扩大的传统犯罪（比如借助网络进行的欺诈和数据窃取）。

3.3. 针对英国的最严重网络犯罪（主要为网络欺诈、窃取、勒索）很大一部分仍然主要是由东欧说俄语的有组织的犯罪集团出于经济目的进行，犯罪市场服务很多在东欧国家托管。不过，威胁还来自其他国家和地区及英国国内，南亚和西非出现威胁的担忧加剧。

3.4. 即便确定了对英国损害最严重的网络犯罪行为关键责任人，如果关键责任人身处引渡安排有限或没有引渡安排的司法辖区，那么英国和国际执法机构通常也很难起诉他们。

3.5. 这些有组织的犯罪集团主要负责开发、部署日益先进的恶意软件来感染英国公民的电脑和网络、英国行业和政府。其影响分散在英国各地，但累积起来影响很大。这些攻击愈发咄咄逼人挑衅十足，这从攻击者越来越多地使用勒索软件和分布式拒绝服务（DDoS）威胁进行勒索可见一斑。

3.6. 虽然有组织的犯罪集团可能对我们的共同繁荣和安全构成严重威胁，但同样令人担心的是针对个人或较小组织进行的不太复杂、但范围广泛的网络犯罪行为带来的持续威胁。

2015年互联网银行诈骗额增长64%，至1.335亿英镑，这包含利用网银渠道从客户银行账户诈骗钱财的做法。诈骗数量增速下降，为23%。英国反金融欺诈行动（Financial Fraud Action UK）组织称，这证明了犯罪分子对公司和高净值客户下手的趋势日益明显。

国家与国家资助的威胁

3.7. 我们经常发现国家和国家资助团体试图侵入英国网络，主攻政府、国防、金融、能源和电信业，以获取政治、外交、科技、商业和战略利益。

3.8. 这些国家网络项目的能力和影响各不相同。最发达的国家继续稳步提高他们的能力，将加密和匿名化服务与工具集成，以保持隐蔽。虽然这些国家具有部署复杂攻击的技术能力，但它们通常通过利用基本工具和技术打击脆弱目标来实现目的，因为它们的打击对象防御软弱。

3.9. 只有少数国家具有对英国整体安全和繁荣构成严重威胁的技术能力。不过其他很多国家正在开发近期有可能对英国利益构成威胁的复杂网络项目。很多寻求发展网络间谍能力的国家能够购买现成的计算机网络刺探工具，将其改装进行间谍行动。

3.10. 除了间谍威胁，一少部分敌对外国威胁分子已经开发、部署了进攻性网络能力，其中包括破坏性网络能力。这些能力对英国关键国家基础设施和工业控制系统构成威胁。部分国家也许会违反国际法利用这些能力，认为能够这样做而相对不受惩罚，从而鼓励其他国家效仿。虽然全球范围内破坏性攻击仍然罕见，但其数量和影响不断增长。

恐怖分子

3.11. 恐怖分子集团仍然渴望针对英国及其利益实行破坏性网络活动。据判断，恐怖分子目前技术能力不高。然而迄今为止针对英国的低能力网络破坏活动所产生的影响甚至也大得出奇：简单的篡改和 doxing 活动（被黑的个人详细信息在网上泄露）能使恐怖分子集团及其支持者吸引媒体注意和恐吓当事人。

> “恐怖分子利用互联网实现其目的不等于是网络恐怖主义。然而，由于网络空间参与增强且考虑到网络犯罪能作为一种服务提供，可以设想恐怖分子会有能力发动网络攻击。”
> 欧洲网络与信息安全局《2015 年网络威胁格局》（Threat Landscape 2015）

3.12. 目前的评估是，实体而非网络恐怖袭击仍将是近期恐怖组织的优先目标。随着越来越懂电脑的一代人参与极端主义，他们可能会交流提高技术能力，我们预计针对英国的低复杂度（篡改或分布式拒绝服务）破坏活动量会增加。出现数个有技术的极端主义个人的可能性也将增长，同时还将出现恐怖组织设法招募内部老手的风险。恐怖分子有可能会利用任何网络能力以尽可能实现最大效果。因此，即使恐怖分子的能力增长有限，也可能对英国及其利益构成重大威胁。

黑客分子

3.13. 黑客组织分散化，以问题为导向。他们组织、选择目标以发泄不满，他们的很多行动都很警惕。虽然绝大多数黑客网络活动都具有破坏性（网站篡改或分布式拒绝服务），但更有能耐的黑客分子能够对当事人造成更大和持久的损害。

“脚本小子”

3.14. 所谓“脚本小子”通常是技术不太高的个人，利用其他人开发的脚本或程序进行网络攻击。我们的评估认为这些人对经济和社会大环境不构成显著威胁。不过他们的确能访问互

联网上的黑客指南、资源和工具。由于很多组织所用的面向网络的系统中所发现的漏洞，某些情况下“脚本小子”的行动能对受到影响的组织造成大得多的损失影响。

内部人士

内部人士威胁仍然是英国组织的一项网络风险。心怀恶意的内部人士——组织内受到信任的、能够访问关键系统和数据的员工——构成的威胁最大。通过窃取敏感数据和知识产权，他们可造成公司的经济损失和声誉损失。如果他们利用自己的特有知识或特殊访问权限便利或发起攻击，以破坏或削弱其组织网络的关键服务，或删除该网络的数据，他们还可构成破坏性网络威胁。

同样值得担忧的还有那些偶然造成网络损失的内部人士或员工，他们由于疏忽误点钓鱼邮件、把已经感染的 USB 插入电脑，或者忽视安全程序、从互联网下载不安全内容。虽然他们没有故意损害组织的意图。但他们对系统和数据的访问权限意味着他们的行动可造成与恶意内部人士同样大的损失。这些个人通常是社交工程的受害者——他们无意中提供了对其组织网络的访问，或者善意地执行实际上有利于骗子的指令。

组织内部人士威胁带来的总体网络风险并不仅限于对信息系统及其内容的非法访问。保护这些系统不受不当访问、保护敏感数据或不同媒介形式上的专属信息不被删除的物理安全控制同样重要。与之类似，能够意识到不满员工所构成的威胁，意识到员工队伍中的欺诈、以及工业和其他形式的间谍活动的强大个人安全文化也是网络安全全面战略的重要因素之一。

个案研究 1：TALKTALK 受害

2015 年 10 月 21 日，英国电信服务商 TalkTalk 报告称受到一起成功的网络攻击，客户数据有可能被黑。后来的调查断定，内含客户详细信息的一个数据库被黑客通过公共互联网服务器访问，大约 15.7 万客户的记录存在风险，这些记录包括客户姓名、住址、银行账户等详细信息。

同一天，几位 TalkTalk 员工收到一封要求以比特币支付赎金的电子邮件。攻击者详细列出了该数据库的结构，以确凿证明该数据库已经被访问。

TalkTalk 的被黑报告帮助得到国家打击犯罪局（National Crime Agency，NCA）专家支持的警察在 2015 年 10 月和 11 月抓住了多名主要嫌疑人，这些嫌疑人都位于英国。

这次攻击表明，即使具备网络知识的大型公司也可能存在漏洞。就声誉损失和运营破坏而言，黑客破坏活动可造成大得多的影响。该事件引起了媒体的高度关注。TalkTalk 迅速报告被黑使得执法机关能够及时作出反应，公众和政府得以减轻敏感数据潜在损失。据估计，该事件给 TalkTalk 造成 6000 万英镑损失，失去了 9.5 万个客户，同时股价大跌。

个案研究 2：攻击孟加拉银行 SWIFT 系统

环球银行金融电信协会（SWIFT）提供能使全球金融机构以安全方式发送、接收金融交易相关信息的网络。由于 SWIFT 发送的支付指令必须由各金融机构彼此拥有的相应账户进行结算，长期以来，人们担心这一过程有可能被网络犯罪分子或其他恶意分子破坏，这些犯罪分子和恶意分子设法向该系统写入非法支付指令，或者在最糟糕的情形下，设法使 SWIFT 网络本身瘫痪或破坏其功能。

2016 年 2 月初，一位攻击者访问孟加拉银行 SWIFT 支付系统，指示纽约联邦储备银行从孟加拉银行账户向菲律宾的账户转账。这起诈骗企图总额为 9.51 亿美元。共计 8.50 亿美元的 30 起交易被 SWIFT 系统阻止。不过，总计 1.01 亿美元的五笔交易进行。追踪发现转至斯里兰卡的 2000 万美元后来得以追回，其余转到菲律宾的 8100 万美元通过赌场洗钱，其中部分资金而后被转到香港。

孟加拉银行后来的法庭调查发现，自己的系统被安装了恶意软件，恶意软件被用来收集该行国际支付和资金转移所用程序的情报。BAE Systems 对攻击相关恶意软件的进一步分析发现该软件与孟加拉银行基础设施运行的本地软件 SWIFT Alliance Access 进行交互的复杂功能。BAE Systems 总结道，“犯罪分子针对当事组织进行越来越复杂的攻击，这在网络入侵领域尤甚。”

个案研究 3：乌克兰电网攻击

2015 年 12 月 23 日，对乌克兰西部输电公司 Prykarpattya Oblenergo 和 Kyiv Oblenergo 的网络攻击造成大停电，输电网络的 50 多个变电站遭到破坏。据报道该地区停电数小时，很多其他客户和地区的电力供应经受了程度较小的破坏，逾 22 万消费者受到影响。

一些人将这次攻击归咎为恶意软件 BlackEnergy3 的使用，因为人们在网络上发现了一些样利。至少在攻击发生前六个月，攻击者向乌克兰电力公用事业公司的办公室发送内含恶意微软 Office 文件的钓鱼电子邮件。不过，打开断路器造成停电的责任有可能不在该恶意软件。也许该恶意软件使得攻击者能够获得允许其直接远程控制该电网各方面的认证，从而后来能让他们引发这次停电。

这次乌克兰事件是对电网进行破坏性网络攻击的首个确证事件。这类事件进一步表明，我们所有的关键国家基础设施（CNI）有必要采取良好的网络安全做法，以防止类似事件在英国发生。

漏洞

设备范围不断扩大

3.15. 当 2011 年最近一个国家网络安全战略公布时，绝大多数人认为网络安全就是保护他们的桌面电脑或笔记本电脑之类的设备。从那以来，互联网日益融入我们的日常生活，以至于我们基本上对此视而不见。“物联网”造成新的网络利用机会，加大网络攻击潜在影响，这些攻击有可能造成实际损失、个人伤害，在最严重的情况下造成生命死亡。

3.16. 能源、采矿、农业、航天等广泛行业迅速实施关键系统工业控制流程联网形成了工业物联网。这同时开启了过去从不会受到这类干扰伤害的设备和流程被黑客进攻破坏的可能性，有可能造成灾难性后果。

3.17. 因此，我们不再仅仅因为自己的设备网络安全性不够而易受网络伤害，还因为我们的社会、健康、福利领域基础性互联系统受到威胁而易受网络伤害。

网络健康与合规不够

3.18. 过去五年来，英国对软件、网络的技术漏洞和网络健康必要性的认识无疑得到增强。这一定程度上是实行诸如英国政府“网络安全 10 步”（10 Steps to Cyber Security）之类倡议的结果，还因为影响政府和公司的主要网络事件越来越受到公众注意。网络攻击并不一定很复杂或不可避免，常常是漏洞被利用的结果，然而这些漏洞很容易修补，所以网络攻击通常能够预防。在绝大多数情况下，仍然是被攻击者的漏洞而非攻击者的聪明才智是网络攻击得逞的决定性因素。公司和组织根据成本效益评估决定在哪些方面及如何投资网络安全，但他们最终要对自己的数据和系统安全负责。只有将关键系统和敏感数据所受网络攻击风险与对人员、技术和治理的充足投资加以平衡，公司受到潜在网络伤害的影响才会降低。

“不存在这样一个信息安全系统，能够阻止一百个人中的一个人打开钓鱼电子邮件，这就是所需要的。”
英国政府通信总部（GCHQ）网络安全主任塞伦·马丁（Ciaran Martin），2015 年 6 月

培训和技能不充分

3.19. 无论在公共部门还是私营部门，我们缺乏满足网络安全需要的技术和知识。在企业界，一定程度上由于缺乏正规培训，很多员工没有网络安全意识，不理解自己在这方面的责任。公众的网络安全意识也不够。

“在过去一年中，只有不到 1/5 的公司让员工参加了网络安全培训。”
2016 年网络安全破坏调查

3.20. 我们还需要发展能使我们跟上迅速发展的技术、管理相关网络风险的专门技能和能力。这种技能方面的差距是一个全国性弱点，必须解决。

遗留系统与未打补丁系统

3.21. 英国很多组织将继续使用有漏洞的遗留系统，直到下一次信息技术更新。这些系统所用软件通常将依赖

较老的、未打补丁的版本。这些老版本通常有多种漏洞，攻击者寻找这些漏洞，掌握利用漏洞的工具。另外一个问题是一些组织使用不受支持的软件，这类软件不存在打补丁机制。

“我们最近分析了 11.5 万个互联网思科设备和客户环境下使用的思科设备，以引起人们对老化基础设施和补丁漏洞注意不足安全风险的注意……我们发现，在这 11.5 万个设备中，有 10.6 万个设备所运行的软件存在已知漏洞。”

思科 2016 年年度安全报告

黑客资源容易获得

3.22. 互联网上有现成的黑客信息和便利用户使用的黑客工具，这使得那些希望发展黑客能力的人能够如愿。黑客为成功危害受害者所需的信息通常能够公开迅速获取。从普通家庭到董事会，每个人都需要了解自己的个人详细情况和系统在互联网上的暴露程度，以及多大程度上有可能受到恶意网络利用。

“99.9%的被利用漏洞是在漏洞公布一年多后遭到入侵。”

威瑞森 2015 年数据破坏调查报告

结论

3.23. 英国采取了多项政策，建立了多个机构，这些政策和机构加强了我们的防御，减轻了我们在网络空间面临的部分威胁。

3.24. 不过，面对威胁我们尚未抢占先机。我们必须打击的恶意网络分子类型及其动机长期延续，同时恶意软件数量和这类恶意分子人数也迅速增长。我们最精通技术的敌对分子即一部分国家和精英网络犯罪分子的能力已经增长。我们的共同挑战在于确保我们的防御与时俱进，足够灵活以反击他们，降低恶意分子攻击我们的能力，解决上述漏洞的根源。

4.我们的国家应对

4.1. 为了减轻我们面临的多重威胁，保卫我们在网络空间的利益，我们需要一个在今后五年支持我们在数字领域所有集体和单独行动的战略办法。本节将列出我们的愿景和战略办法。

我们的愿景

4.2. 我们的 2021 年愿景是，**让英国成为安全、能应对网络威胁的国家，在数字世界繁荣而自信。**

4.3. 为了实现这一愿景，我们将努力实现下列具体目标：

- **防御**。我们具有保卫英国不受日益发展的网络威胁、对事件做出有效反应，以及确保英国网络、数据和系统得到保护、具备韧性的各种手段。国民、企业和公共部门具有自我防御的知识和能力。
- **遏制**。英国将成为网络空间各种形式入侵难以得逞的硬目标。我们探测、了解、调查、破坏针对我们的敌对行动，追查、起诉侵犯者。我们具备在网络空间采取进攻行动的各种手段——如果我们选择这样做。
- **开发**。我们有一个创新且不断发展的网络安全行业，得到全球领先的科技研究与开发支持。我们有能够自我持续的人才输送渠道，这些人才提供各种技能满足公私领域的全国需求。我们先进的分析和专长使英国能应对、克服未来的威胁和挑战。

4.4. 为了支持这些目标，我们将通过投资于各类伙伴关系来寻求国际行动和施加影响力。我们将影响全球网络空间的发展，促进我们更广泛的经济和安全利益。

原则

4.5 在努力实现这些目标的过程中，英国政府将应用下述原则：

- 保护人民和增强繁荣的双重需求驱动我们的行动和政策；
- 我们将把对英国的网络攻击视为与常规攻击等同的严重攻击，必要时我们将自卫；
- 我们将根据英国法律和国际法行动，并希望他人同样照此行事；
- 我们将有力保护、促进我们的核心价值观。这些价值观包括民主、法治、自由、开放与负责任的政府和机构、人权和言论自由；
- 我们将维护、保护英国公民的隐私；
- 我们将合作行动。只有与相关分权管理部门、公共部门所有部分、企业、机构和公民个人合作，我们才能成功保障英国在网络空间的安全；
- 英国政府将履行其责任，牵头全国性应对措施，不过企业、组织和公民个人有责任采取合理举措在网络上保护自己，确保自己具有韧性，发生网络事故时能够继续运营；
- 公共部门各组织的安全责任，包括网络安全和在线数据与服务保护，相应各部、常务次官和管理委员会的安全责任；
- 我们不接受因企业和组织未能采取控制网络威胁所需举措而对公众和整个国家构成的重大风险；
- 我们认识到网络威胁无国界，将与那些和我们观点一致的国家、与那

些和我们安全利益重叠的国家密切合作。我们承认广泛合作的价值，还将与一系列国际合作伙伴广泛合作，对更广泛的社会造成影响；
- 为了确保政府干预对总体国家网络安全和韧性产生显著影响，我们将寻求定义、分析、呈报那些衡量我们共同网络安全状况、衡量我们实现战略目标成功与否的数据。

职责与责任

4.6. 保障国家网络空间安全要求大家共同努力。我们每一个人都发挥重要作用。

个人

4.7. 作为公民、员工和消费者，在现实世界，我们采取切实举措保护我们所看重资产的安全。在虚拟世界，我们也得这样做。这意味着履行我们的个人责任，采取各种合理举措，不仅保卫我们的硬件——我们的智能手机和其他设备——而且保护给我们私人和职业生活提供自由、灵活性和方便的数据、软件和系统。

企业与组织

4.8. 企业、公私部门组织和其他机构在数字领域掌握个人数据、提供服务和运营系统。信息联网使他们的运营发生革命性变化。不过伴随这种技术变革而来的是保卫他们所拥有的资产、维持他们提供的服务、使所售产品具备适当水平安全性的责任。公民、消费者与整个社会指望企业和组织采取所有合理举措保护其个人数据，建立他们所依赖系统和结构的韧性——经受打击并复苏的能力。企业和组织还必须明白，如果成为网络攻击的受害者，他们将为其后果负责。

政府

4.9. 政府的主要职责是保卫国家不受其他国家攻击，保卫公民和经济不受损害，制定保护我们的利益、保卫基本权利和把犯罪分子绳之以法的国内国际框架。

4.10. 作为重要数据拥有者和服务提供者，政府采取严格措施提供对其信息资产的保护。政府还承担建议、告知公民和组织在网上保护自己需要做什么，以及必要情况下制定我们希望重要公司和组织将遵守的标准。

4.11. 虽然我们的重要经济部门属于私营，但政府最终负责确保国家韧性，与政府各合作伙伴一道，维持整个政府的基本服务和功能。

推动变革：市场的作用

4.12. 2011 年战略和国家网络安全计划通过依赖市场推动正确行为而设法取得成果，并增强公私部门能力。我们期望商业压力和政府发起的激励确保在恰当网络安全领域获得充足商业投资，刺激投资流入我们的行业，鼓励足够的技术人才源源不断进入本行业。

4.13. 已经取得了相当大的成就。在各经济领域和更广泛的社会中，过去五年来风险意识和减轻网络风险所需行动的意识得以增强。但市场力量与政府鼓励相结合本身不足以以所需的速度保障我们在网络空间的长期利益。包括很多关键部门在内的太多网络如今仍然不安全。市场对网络风险仍然不重视，因而也未对其进行正确管理。太多组织的网络仍然被攻破，甚至是最基本水平的破坏。鲜有投资者愿意冒险支持本行业创业者。教育

和培训系统培养的具备合适技能的毕业生和其他人士太少。

4.14. 市场仍然有待发挥作用，在较长期限内所发挥的影响将比政府能够发挥的影响更大。然而，英国所面临威胁的紧迫性，以及我们的数字化环境脆弱性不断扩大，要求短期内政府加大行动。

推动变革：扩大政府职责

4.15. 政府因而必须在满足英国国家网络安全需求的过程中起带头作用。只有政府能够利用保卫国家不受最复杂威胁所需的情报和其它资产。只有政府能够推动公私部门的合作，确保公私部门信息共享。政府在与行业磋商时发挥领导作用，规定何为良好的网络安全行为并确保其实施。

4.16. 政府将在今后五年为我们的国家网络安全带来显著改善。这一宏伟的变革计划将专注于以下四大领域：

- **手段与激励。**政府将作出投资，以最大化真正创新的英国网络业的潜力。我们将通过支持创业公司和进行创新投资做到这点。我们还将设法提早在教育系统中鉴别和培养人才，发展进入有待进一步厘清的专业领域的更清晰路径。政府还将利用一切可用的手段，其中包括即将实行的《一般数据保护条例》（General Data Protection Regulation, GDPR），推动各经济领域网络安全标准提高，包括在需要的情况下通过监管手段提高。
- **扩大着眼于网络威胁的情报和执法。**情报机构、国防部、警察局和国家打击犯罪局与国际合作机构协调，将扩大鉴别、预计和破坏外国势力、网络犯罪分子和恐怖分子的敌对网络行为。这将改善情报收集和利用，以期预先获得有关敌对分子意图和能力的情报。
- 与有关行业合作**开发、部署技术**，其中包括推进“主动网络防御”（Active Cyber Defence）措施，以加深我们对网络威胁的理解，加强面对网络威胁的英国公私部门系统和网络的安全，破坏恶意行为。
- **国家网络安全中心。**政府已建立一个国家级网络安全单一中心机构。该机构将负责国家级网络事件，就网络安全发表权威言论，成为一个专长中心，对政府各部、地方分权政府、监管部门和企业提供定制化支持和建议。国家网络安全中心将分析、检测、了解网络威胁，还将提供自己的网络安全专长支持政府培育创新工作、支持欣欣向荣的网络安全业、激励网络安全技术发展。面向公众的国家网络安全中心独特之处在于其主管部门是英国政府通信总部（GCHQ），因而国家网络安全中心能够利用世界一流的专长和英国政府通信总部的敏感能力，加大国家网络安全中心能够向经济领域和更广泛的社会提供的支持。确保有效实施该网络安全建议仍将是政府各部门的责任。

“鉴于我们企业和大学的知识产权遭到大规模窃取，以及大量浪费时间和金钱的钓鱼与恶意软件欺诈，国家网络安全中心表示，英国将集中力量打击网络上存在的威胁。”

英国政府通信总部主任罗伯特·汉尼根（Robert Hannigan），2016 年 3 月

4.17. 我们的网络安全和韧性实现这些变革将需要追加资源。在《2015 年战略防御与安全评估》（Strategic Defence and Security Review 2015）中，政府为该五年战略拨款 19 亿英镑，以实现战略所述承诺和目标。

国家网络安全中心

国家网络安全中心于 2016 年 10 月 1 日成立，提供政府、行业和公众之间打造有效网络安全合作关系的独特机会，以确保英国网络更加安全。该机构将就网络事故做出响应，是英国网络安全方面的权威声音。各关键行业将首次能够直接与国家网络安全中心员工接触，在保障网络和系统不受网络威胁方面获得最佳建议和支持。

国家网络安全中心：

- 是政府网络安全威胁情报和信息保障的统一建议来源；
- 是政府打击网络威胁行动的有力公众形象，联合行业、学术界和国际合作伙伴，以保持英国防范网络攻击；
- 能获得英国政府通信总部后援以利用必要秘密情报和世界一流技术专长的公众形象机构。

本战略实施期内将逐步建设国家网络安全中心的能力。国家网络安全中心将综合英国政府通信总部信息安全部门 CESG、国家基础设施保护中心（CPNI）、国家计算机应急反应小组（CERT-UK）和网络评估中心（CCA）已开发能力，以使我们能够再接再厉，同时大大简化之前的安排。国家网络安全中心最初的工作重心将集中于：

- 应对及减少网络事件损害的世界级事件管理能力，这些事件从那些影响单个组织的攻击到全国性大规模攻击大小不等；
- 就公私部门如何才能解决网络安全问题提供沟通，促进网络威胁信息共享；及
- 继续向政府和电信、能源、金融之类的关键行业提供专家行业建议，向全英国提供网络安全建议。

国家网络安全中心提供政府实施本战略多项要素的有效方式。我们认为，随着国家网络安全中心的发展，其焦点和能力需要根据新挑战和吸取的经验教训调整。

实施计划

我们对今后五年英国的网络安全目标可谓宏大。实现这些目标要求我们在数字领域果断行动并有所得。实现该政府愿景的活动将推动本战略三个主要目标：防御我们的网络空间、遏制敌对分子和开发我们的能力，所有这些都得到有效国际行动的支持。

5.防御

5.0.1. 本战略的防御要素旨在确保英国在网络、数据和系统公共、商业和私营领域具有抵御和防范网络攻击的能力。正如我们难以绝对遏制犯罪，我们亦不可能制止每一次的网络攻击。然而，通过联合公民、教育机构、学术界、企业和其他政府机构，英国可以建立层层防御，大大减少我们在网络事件中的暴露程度，保护我们最宝贵的资产，让所有人都能在网络空间成功顺利的运作，促进国家间的合作和良好的网络安全实践，也将有利于我们的集体安全。

5.0.2. 政府将采取措施，确保公民、企业、公私部门组织和机构能够获得正确的防御信息来保护自己。国家网络安全中心为政府统一建议来源提供安全威胁情报和信息安全保障，确保我们能够为网络防御提供量身定制的指导意见以及能够对网络空间中的重大事件迅速有效地做出反应。政府将与行业和国际合作伙伴一道，对公私部门、最重要的系统和机构以及整个经济的网络安全进行界定。我们将默认在所有新的政府和关键系统内构筑安全。执法机构将与行业及国家网络安全中心密切合作，以提供动态的犯罪威胁情报，促进行业防御，增进保护性安全建议和标准。

5.1. 主动网络防御

5.1.1. 主动网络防御（ACD）是实施安全措施以加强网络或系统、增强网络攻击抵御能力的原则。在商业语境中，主动网络防御通常是指网络安全分析人员了解各自网络的威胁，然后制定和实施主动对抗或抵御这些威胁的措施。针对该战略，政府选择在更大规模上对同样的原则加以利用：政府将利用其独有的专长、能力和影响力来推动国家网络安全的重大变革，从而应对网络威胁。我们所试图捍卫的“网络”是整个英国的网络空间。拟议的活动体现了防御性行动计划，利用作为国家技术权威机构的国家网络安全中心的专长，在宏观层面对英国的网络威胁作出反应。

目标

5.1.2. 政府实施主动网络防御的目标是：

- 通过提高英国网络的韧性，使英国成为国家资助分子和网络犯罪分子较难得逞的硬目标；
- 通过阻止黑客与受害者之间的恶意软件通信，在英国网络上击败绝大多数数量巨大/复杂程度较低的恶意软件活动；
- 发展并壮大政府瓦解国家资助的重大网络犯罪威胁的能力的规模与范围；
- 保护我们的互联网和电讯免受恶意分子的攻击；

- 加强英国关键性基础设施和面向公民的服务设施对网络威胁的防范；及
- 破坏各类型攻击者的商业模式，使他们失去动力，减少攻击造成的伤害。

做法

5.1.3. 为了实现这些目标，政府将会：

- 与行业、特别是通信服务提供商（CSP）展开合作，加大其攻击英国互联网服务和用户的难度，大大降低其对英国可能造成的持续影响。这将包括处理网络钓鱼、阻止恶意域名和 IP 地址等瓦解恶意软件攻击的举措，以及加强英国电信和互联网路由基础设施安全的相关措施；
- 增加英国政府通信总部、国防部和国家打击犯罪局的规模和发展能力，以破坏英国最严重的网络威胁，包括复杂的网络犯罪分子和外国敌对分子；及
- 更好地保护政府系统和网络，帮助行业为关键国家基础设施供应链打造更强大的安全保障，使英国的软件生态系统更加安全，为公民提供政府在线服务的自动保护。

5.1.4. 在可能的情况下，这些举措将与行业伙伴一起或者通过行业伙伴关系付诸实施。对许多行业来说，政府将提供关键的专家支持、咨询和思想指导，由行业进行设计和牵头实施。

5.1.5. 政府还将采取具体行动落实这些措施，其中包括：

- 与通信服务提供商共同阻止恶意软件攻击，限制对已知恶意软件来源的特定域或网站的访问，即域名系统（DNS）封锁/过滤；
- 通过在政府网络上部署电子邮件验证系统作为标杆以及鼓励行业实施类似举措，来防止依赖域名“欺骗”的网络钓鱼活动（电子邮件看似来自银行或政府部门等特定发件人，而实际上这些发件人是欺诈性的）
- 通过对域名系统进行协调的互联网名称与数字地址分配机构（ICANN）、国际互联网工程任务组（IETF）和欧洲地区级互联网注册机构（RIPE）等多利益攸关方网络治理组织促进安全最佳实践，并与联合国互联网治理论坛（IGF）的利益攸关方进行接洽；
- 与执法渠道合作，避免英国公民成为海外无保护基础设施的网络攻击的目标；
- 努力实施控制措施，保护政府部门的互联网流量路由，使之不会被恶意分子非法重编路由； 及
- 投资国防部、国家打击犯罪局和英国政府通信总部的各类计划，以增强这些组织应对、瓦解针对英国网络的国家资助的严重网络犯罪活动的能力。

随着威胁的不断发展，我们将会开发这些技术性干预措施，以确保英国公民和企业在大多数大规模商用网络攻击中受到默认保护。

对成功的衡量

5.1.6. 政府将通过评估以下成果的进展来衡量其在建立有效的主动网络防御方面取得的成绩：

- 英国是“网络钓鱼”的硬目标，因为我们对恶意域名采取大规模防御措施，积极开展规模更大的反网络钓鱼保护活动，同时使“电话钓鱼诈骗”和短信欺骗等其他通讯形式对社交工程的攻击行为更加难以得逞；
- 遏止更大比例的网络攻击和开发相关的恶意软件通信和技术伪装；
- 英国的互联网和电信流量更加不易受到恶意分子重新路由的影响；
- 英国政府通信总部、武装部队和国家打击犯罪局应对严重的由国家资助的犯罪威胁的能力得到极大增强。

5.2. 建立更加安全的互联网

5.2.1. 技术变革使我们能够确保未来所使用的在线产品和服务是“默认安全的”，进而有机会大大降低对手在英国进行网络犯罪的能力。这意味着要确保将我们使用的软件和硬件内置的安全控制由制造商设置为默认激活，以最大限度地提供安全的用户体验，除非后者主动决定关闭该激活设置。所面临的挑战是实现变革性变化，为终端用户提供支持以及商业上可行的、安全的产品或服务——所有这些都是在维护互联网的自由和开放背景下进行的。

“网络联通事物增长迅速。2015 年我们看到许多概念验证和对现实世界的攻击，以及汽车、医疗器械等方面存在的严重漏洞。制造商需要优先考虑安全性，以降低产生严重的个人、经济和社会后果的风险。”

赛门铁克 2016 年《互联网安全威胁报告》

5.2.2. 政府有潜力发挥主导作用，探索新技术以更好地保护我们自己的系统，帮助行业在供应链上建立更强大的安全保障，确保软件生态系统以及为在线访问政府服务的公民提供自动保护。政府必须测试和实施为政府在线产品和服务提供自动保护的新技术。如果可能，应向私营部门和公民提供类似的技术。

目标

5.2.3. 到 2021 年，绝大多数在线产品和服务为“默认安全”。消费者将被授权选择将内置安全保障作为默认设置的产品和服务。个人可以选择关闭这些设置，但那些希望以最安全的方式从事网络空间活动的消费者，将被自动保护。

我们的做法

5.2.4. 我们将进行以下行动：

- 政府将率先垂范，不依赖互联网本身的安全来提供网络安全保障服务；

- 政府将探讨不同的行业合作方式，为软硬件“在默认情况下更加安全”开发前沿方法；及
- 我们将在政府中采用具有挑战性的新型网络安全技术并鼓励地方管理部门采取的同样行动，以减少可识别的采用风险。这将提供概念验证，展示新技术和方法的安全优势，同时也将安全列为新产品开发的核心，消除被犯罪分子利用的机会，从而保护终端用户。

5.2.5. 为此，我们将：

- 继续鼓励软硬件供应商销售带有默认激活安全设置的产品，要求用户主动禁用这些设置，以保障安全。部分供应商已经将此付诸行动，但也有一些供应商尚未采取必要的措施；
- 持续开发互联网协议（IP）信誉服务，以保护政府的数字服务（这将允许在线服务获取连接到其 IP 地址的信息，帮助行政部门更实时地做出更明智的风险管理决策）；
- 在政府网络上安装产品，以确保软件运行正常、不受恶意干扰；
- 寻求扩展到 GOV.UK 域之外的、可以告知用户其运行的浏览器过期的其他数字服务措施；及
- 投资可信平台模块（TPM）和新兴行业标准（如线上快速身份验证（FIDO））等不依赖密码而是使用用户拥有的机器和其他设备进行身份验证的技术。政府将在安全性和整体用户体验方面对创新的认证机制进行测试，藉以证明这些机制的用途。

5.2.6. 政府还将通过提供新产品的安全评级来探索如何鼓励市场，使消费者了解哪些产品和服务为其提供最大的安全保障。政府还将探索如何将这些产品评级与新的和现有的监管机构联系起来，以及在消费者进行危害其安全性的在线行动之际对其进行提醒的方法。

对成功的衡量

5.2.7. 政府将通过评估以下成果进展来衡量其在建立安全互联网方面取得的成绩：

- 2021 年英国的大多数商品和服务使得英国更具安全性，因为它们的默认安全设置默认启用或将安全性集成到其设计中；及
- 国家、地方、地方分权政府提供的所有政府服务都得到英国公众的信任，因为它们的实施最大可能地保障了安全性，其欺诈程度在可接受的风险参数之内。

5.3. 保护政府

5.3.1. 英国政府、地方分权政府和广大的公共部门持有大量敏感数据。它们向公众提供基本服务，运作对国家安全和韧性至关重要的网络。政府的系统是社会运作的基础。公共部门服务现代化仍将作为英国“数字化战略”的基石——英国政府志在让英国成为世界领先的数字化国家。为了保持公民对在线公共部门系统和机构的信任，必须保护政府所持有的数据。面对敌对分子获得政府和公共部门网络和数据的持续企图，政府各级部门必须实施适当水平的网络安全保障。

目标

5.3.2. 我们希望取得以下结果：

- 公民可以充满信心地使用政府在线服务：相信自己的敏感信息具有安全保障，反过来也理解自己以安全的方式在线提交敏感信息的责任；
- 政府将制定并遵守最适宜的网络安全标准，以确保政府各部门了解和履行其保护各自网络、数据和服务的义务；及
- 保护政府的关键资产——包括最高级别的资产——免受网络攻击。

我们的做法

5.3.3. 英国政府将继续提供更多在线服务，使英国成为真正的“默认数字化国家”。政府数字服务（GDS）、皇冠商业服务（CCS）和国家网络安全中心（NCSC）将确保政府提供或购买的所有新数字化服务也是“默认安全”的。

5.3.4. 政府的网络非常复杂，在许多情况下仍然存在遗留系统，以及供应商不再支持的一些商业可用的软件。我们将确保这些遗留系统和不被支持的软件没有非托管风险。

5.3.5. 我们将提高政府和广大的公共部门抵御网络攻击的韧性。这意味着确保对所有系统、数据和有权访问它们的人员具备准确和最新的了解。通过实施国家网络安全中心设定的最佳做法，可以最大限度地减少网络事件发生的可能性和产生的影响。政府也将确保能够通过事件演习方案和政府网络的定期测试，有效应对网络事件。我们将邀请地方分权政府和地方当局酌情参加这些活动。通过自动扫描，我们将确保对政府的在线安全状况有较好的了解。

5.3.6. 网络安全不仅仅关乎技术。几乎所有成功的网络攻击都有人为因素。因此，我们将继续对人进行投资，确保每个在政府工作的人对网络风险都有良好的认识。我们将在风险变强的领域开发具体的网络专长，确保我们有正确的流程来有效地管理这些风险。

5.3.7. 国家网络安全中心将形成世界领先的网络安全指导，与时俱进，跟上威胁以及新技术的发展步伐。我们将采取措施，确保政府机构轻松获取威胁信息，以了解自己的网络风险并采取适当行动。

5.3.8. 我们将继续完善我们的最高级别网络，为政府最敏感的通信提供保护。

5.3.9. 医疗保健系统对网络安全构成了独特的挑战。该行业 4 万多个组织雇用了约 160 万人，每个组织的信息安全资源和能力差异巨大。国家健康和医疗数据守护者（National Data Guardian for Health and Care）为英格兰的健康和社会保健系统制定了全新的数据安全标准，并为患者提供了新的数据同意/选择退出模式。政府将与医疗和社会保障机构合作执行这些标准。

“英国在网络安全方面世界领先，但其面临的威胁与日俱增。新的网络安全运营中心将确保我们的武装部队能够继续保持安全运行。我们不断增加的防务预算意味着在进行传统能力投资的同时，我们有能力在网络空间领域领先竞争对手。”

国防大臣迈克尔·法伦（Michael Fallon）议员阁下，2016 年 4 月

5.3.10. 网络安全对我们的国防至关重要，我们在英国和世界各地的武装部队依赖信息和通信系统。国防部（MoD）的基础设施和人员是主要的网络攻击对象。国防系统经常被犯罪分子、外国情报机构和其他恶意分子寻求利用人员、破坏业务与运作、破坏和窃取信息的目标。我们将通过开发使用最先进的防御性网络功能的网络安全运营中心（CSOC）来加强对网络威胁的认识、侦测和反应职能，以保护国防部的网络空间并应对威胁。网络安全运营中心将与国家网络安全中心紧密合作，共同面对国防部的网络安全挑战，推进更大范围的国家网络安全。

对成功的衡量

5.3.11. 政府将通过评估以下成果进展来衡量其在保护政府网络、系统和数据方面的成绩：

- 政府对整个政府和广大的公共部门的网络安全风险水平有深入了解；
- 各政府部门及其他机构按照其风险水平和约定的政府最低标准对自身进行保护；
- 政府部门和广大的公共部门具有韧性，能够有效应对网络事件、维护各自职能及迅速恢复；
- 由政府部署的新技术和数字服务默认为网络安全；
- 我们意识到并积极减轻政府系统和机构中所有已知的互联网漏洞；及
- 政府的所有供应商都达到适当的网络安全标准。

5.4. 保护关键国家基础设施和其他优先部门

背景

5.4.1 某些英国组织的网络安全尤其重要，成功攻击这些组织的网络将对本国国家安全构成最严重的威胁，可能会影响到英国公民的生活、英国经济的稳定和实力或者英国的国际地位和声誉。这些公共和私营部门的重要公司和组织包括为国家提供基本服务的关键国家基础设施。确保关键国家基础设施的安全以及对抗网络攻击的韧性是政府的头等大事。在关键国家基础设施之外，还有其他的公司和组织需要给予较多的支持，包括：

- 经济瑰宝——英国最成功的公司以及那些在研究和知识产权的价值方面掌握英国未来经济实力的公司；
- 数据持有方——不仅包括拥有大量个人资料的组织，还包括慈善机

构等那些持有国内外弱势群体数据的组织；
- 高威胁的目标——例如媒体组织，对媒体组织的攻击可能会损害英国的声誉、破坏公众对政府的信任或危及言论自由；
- 数字经济的试金石——使电子商务和数字经济得以实现的、依赖消费者信任的数字服务提供商；及
- 那些通过市场力量和权威、可对整个经济产生影响以提升网络安全的组织，如保险、投资、监管和专业咨询公司。

5.4.2. 需要做更多的工作来保护我们经济中的这些关键部分，为具有重要影响力的组织提供支持。我们的关键国家基础设施，无论是在私营还是公共部门，仍然被作为攻击对象，而在这些和许多其他优先领域中，即使网络威胁高涨且日趋多样，网络风险仍然没有被正确的理解或管理。

目标

5.4.3. 在适当情况下，英国政府与地方分权政府和其他负责机构合作，确保包括关键国家基础设施在内的英国最重要的组织和公司在网络攻击发生时具有足够的安全性和韧性。政府和其他公共机构均不会负责管理私营部门的风险，而是由其董事会、所有者和经营者负责。但是，政府将为这些公司和组织提供与其面临的威胁以及遭到攻击的后果相适应的支持和保证。

“网络安全是启动创新和扩张的关键，通过与网络安全相适宜的组织和以风险为中心的方法，各组织可以再次将机会和探索作为重点。建立对物联网内成功运作业务的信任，以及对个人及其移动设备（从简单的手机到医疗保健设备，从智能家电到智能汽车）提供全面的支持和保护，是一种关键的竞争优势，需要优先对待。”

《2015 年安永全球信息安全调查》

我们的做法

5.4.4. 组织机构和公司董事会负责确保其网络安全。他们必须明确关键系统，并定期评估其在不断变化的技术环境和威胁下的安全漏洞。它们必须对技术和员工进行投资，以减少当前和未来系统及其供应链中的漏洞，保持与风险成比例的网络安全，必须对攻击发生时的应对能力已经进行了测试。对于关键国家基础设施，它们必须与政府机构和监管机构合作开展这项工作，从而使我们对网络风险的妥善管理保有信心，否则网络风险则会干预国家安全利益。

5.4.5. 因此，政府将了解关键国家基础设施的网络安全水平，并采取措施在必要时进行干预，以推动符合国家利益的改进措施。

5.4.6. 政府将：
- 与行业分享只有政府才能获得的威胁信息，让后者有针对性地采取保护措施；

- 就如何管理网络风险给出建议和指导，并与行业和学术界合作，对良好的网络安全性进行界定；
- 促进对保护关键国家基础设施所需的高端安全保障的采用，如培训设施、测试实验室、安全标准和咨询服务；及
- 与关键国家基础设施公司进行演习，协助后者管理网络风险和漏洞。

5.4.7. 国家网络安全中心将为英国最重要的公司和组织（包括关键国家基础设施）提供这些服务，与那些确保本单位网络风险得到管理、符合国家利益要求的各部门和监管机构展开合作。

5.4.8. 政府亦会确保网络安全监管框架得到落实，其中包括：

- 确保行业保护自身免受威胁；
- 专注结果、充分灵活以确保领先于威胁，或者带来合规而不是健全的风险管理；
- 足够灵活以促进增长和创新，而非领导；
- 与其他司法管辖区的制度相协调，使英国公司所采纳的方法不至于分散和累赘；及
- 结合政府的有力支持，为英国提供竞争优势。

5.4.9. 我们的许多行业已经进行网络安全管理。尽管如此，我们必须确保整个经济体（包括关键国家基础设施）采取正确的步骤来管理网络安全风险。

对成功的衡量

5.4.10. 政府将通过评估以下成果进展来衡量其保护关键国家基础设施和其他优先部门的成绩：

- 我们了解关键国家基础设施网络安全的水平，并采取措施在必要时进行干预以推动做出符合国家利益的改善；及
- 我们最重要的公司和组织了解威胁级别并实施相应的网络安全措施。

“去年，大型企业的平均安全漏洞成本为 36500 英镑，小公司的安全漏洞成本为 3100 英镑。65%的大型机构报告说，他们过去一年经历了信息安全漏洞，其中 25%的人每月至少一次遇到安全漏洞问题。接近 70%的攻击涉及病毒、间谍软件或恶意软件，而这些本可以通过政府的网络要素（Cyber Essentials）计划来避免。”

《2016 年政府网络健康检查和网络安全漏洞调查》

5.5. 不断变化的公共和商业行为

5.5.1 成功的英国数字经济依赖于企业和公众对在线服务的信心。英国政府业已与行业和公共领域的其他部门合作，以提高对威胁的认识和理解。政府也向公众和企业提供了他们用来保护自己的一些工具。虽然有很多机构能够极好地保护自己并为他人提供在线服务，其中部分甚至能够达到世

界水平，但是大多数企业和个人仍然没有妥善管理网络风险。

目标

5.5.2. 我们的目标是确保个人和组织，无论其规模如何以及属于哪个行业，都在采取适当措施，保护自己和他们的客户免受网络攻击伤害。

我们的做法

5.5.3. 政府会提供经济保护需要的建议。我们将改进建议提供的方式，以最大限度地发挥其作用。对于公众来说，政府会利用“值得信赖的声音”来增加信息的覆盖面、公信力和相关性。我们将向那些使用在线服务、面临网络风险的公众提供一些易于采取行动的、与个人相关的建议，在适当的情况下，使地方分权政府和其他当局参与其中。

5.5.4. 对于企业，我们将通过诸如保险公司、监管机构和投资公司等组织，对公司施加影响，以确保他们管理网络风险。在这种情况下，我们将强调明确的商业利益和市场意见领袖对网络风险的定价。我们会努力找出许多机构难以充分保护自己的原因，与专业标准机构等组织合作，劝说公司采取行动，而不仅仅是提高他们的认识。同时，我们还将确保有适当的监管框架来管理市场未能解决的网络风险问题。其中一个举措是力求使用诸如《一般数据保护条例》等手段来提高网络安全标准、保护公民的合法利益。

5.5.5. 英国的个人和组织将可以获得保护自己所需的信息、教育和工具。为了确保我们在公共行为中交付重大改革，我们将使政府和合作伙伴网络安全指导信息保持连贯和一致。国家网络安全中心将对这些指导信息提供技术建议支持，反映业务和公共优先事项和做法，使之明确、易于访问和一致，跟上网络威胁的变化。执法部门将与业界和国家网络安全中心紧密合作，分享最新的犯罪威胁情报，支持各行业防范威胁，减轻攻击对英国受害者的影响。

对成功的衡量

5.5.6. 政府将通过评估以下成果的进展来衡量其保护关键国家基础设施和其他优先部门的成绩：

- 英国经济的网络安全水平能够匹敌、甚至优于先进经济体的网络安全水平；
- 由于网络安全标准的改善，英国企业受网络攻击成功的次数、严重程度和影响已经减少；及
- 由于各组织和公众了解其网络风险级别以及管理这些风险所需的网络安全步骤，英国的网络安全文化有所改善。

网络须知（Cyber Aware）

“网络须知”运动，即曾经的 Cyber Streetwise，向公众提供保护自己免受网络犯罪分子侵害所需的建议，通过社交媒体、广告以及企业合作传递针对性信息：

- 使用三个随机单词来创建高安全系数密码；及
- 总是下载最新的软件更新。

专家认为采取这些行动有利于保护小企业和个人免受网络犯罪侵害。“网络须知”目前由 128 家跨部门合作伙伴提供支持，其中包括警察部门、零售、休闲、旅游和专业服务行业企业。在 2015/16 年度，估计有 1000 万成年人和 100 万小企业表示“网络须知”使他们更有可能维持或实施重要的网络安全行为。

如需了解更多信息，请访问 cyberaware.gov.uk

网络要素（Cyber Essentials）

“网络要素”计划旨在向组织展示如何保护自身免受低级“商用威胁”，它列出了组织应该具备的五项技术控制（访问控制、边界防火墙与互联网网关、恶意软件保护、补丁管理和安全配置）。绝大多数网络攻击使用相对简单的方法，即利用软件和计算机系统中的基础漏洞。利用互联网上公开提供的工具和技术，甚至技能低劣的恶意分子都能够利用这些漏洞。正确实施“网络要素”计划将会抵制绝大多数常见的互联网威胁。

5.6. 管理事故,了解威胁

5.6.1. 由于整个公私部门影响组织的网络事件的数量和严重性都可能会增加，因此我们需要确定私营部门和公众与政府共同应对网络事件的方式，确保英国政府对每个部门的支持水平——考虑到其网络成熟度——得到明确界定和理解。政府对威胁信息的收集和传播方式与速度必须适用于各个组织类型。目前，私营部门、政府和公众可以访问多种有关网络安全的信息来源、指导方针和协助措施。这个过程必须简化。

5.6.2. 无论是对事件做出响应，还是提供指导意见，我们必须确保政府不是孤军奋战，而是与私营部门联合行动。事件管理流程应该反映整体的事件处理方式，进而从合作伙伴中学习并分享缓解技巧。我们还将继续发挥与其他计算机应急小组（CERT）和盟友的关系，作为事件管理职能的一个组成部分。

5.6.3. 当前的事件管理在政府部门仍然有些分散，而这一战略将创造统一的方法。国家网络安全中心发挥精简有效的政府主导的事件响应职能。在发生严重的网络事件时，确保武装部队能够提供协助，比如以传统形式解决事件的实际影响，或者由常规或后备网络人员提供专家支持。虽然我们会提供资源所允许的一切支持，但仍会继续强调业界、社会和公众采取行动维护基本网络安全的重要性。

目标

5.6.4. 我们的目标如下：

- 政府将基于对网络威胁增强的理解和意识以及针对我们采取的行动来提供单一或联合的事件管理方法。其中，国家网络安全中心将作为关键的推动者，与私营部门、执法机构和其他政府部门、当局和机构的伙伴关系也将成为关键推动因素；
- 国家网络安全中心将根据受害者的情况明确事件的报告程序；及
- 我们将防止最常见的网络事件，建立有效的信息共享结构以提供“事前”规划相关信息。

我们的做法

5.6.5. 无论在公共还是私营部门，确保网络安全、实施事件应急方案都是组织和公司管理的责任。在发生重大事件的情况下，政府事件管理过程将反映网络事件的三个不同要素：前兆原因、事件本身和事后响应。

5.6.6. 为了向政府和私营部门实施有效的事件管理，我们将密切合作，审查和界定政府响应的范围，确保增进合作力度。利用对威胁理解和意识的增强，我们将以国家网络演练计划为基础，加强对公私部门合作伙伴的支持。

5.6.7. 我们将为事件咨询、协助和保险创造一个值得信赖和可靠的政府身份，进而提高英国数字社会的网络安全意识，更好地发现趋势、采取积极主动的措施并最终防止事件的发生。

5.6.8. 在实现自动信息共享（即网络安全系统对事件或攻击自动做出提醒）的同时，我们将提供更有效的服务，使组织机构能够针对相关威胁信息迅速采取措施。

对成功的衡量

5.6.9. 政府将通过评估以下成果的进展来衡量其在事件管理方面的成绩：

- 更高的事件报告比例，从而更好地了解威胁的大小和规模；
- 国家网络安全中心作为一个集中的事件报告和响应机制，能够更有效、高效、全面地管理网络事件；及
- 我们将在国家层面从根本上解决攻击产生的原因，减少涉及多个受害者和部门事件的发生和反复。

6.遏制

6.0.1. 国家安全战略规定，防御与保护始于遏制，网络空间也不例外。要实现网络威胁下的网络安全与韧性、在数字世界发展繁荣并充满信心等国家愿景，我们必须对那些试图伤害我们和我们利益的人进行劝阻和遏制。为了实现这一点，我们需要继续提高网络安全水平，使得攻击我们的网络空间——无论是通过窃取还是破坏——既不能轻而易举，也要付出高昂代价。我们必须让对手知道，他们不能逍遥法外：我们能够找到他们，能够使用一切可用的工具对他们的行为进行最恰当的反击。我们将继续建立全球联盟，促进国际法在网络空间的应用。我们还将采取更加主动的措施，破坏所有威胁网络空间的活动以及他们所依赖的基础设施。要实现这一抱负，我们需要具备世界一流的主权能力。

6.1.网络的遏制作用

6.1.1. 网络空间只是我们必须维护自身利益和主权的一个领域。正如我们在现实领域的行动与我们的网络安全和遏制息息相关，我们在网络空间中的行动和态度必须有助于更广泛意义上的国家安全。

6.1.2. 适用于现实领域的遏制原则，同样适用于网络空间。英国明确表示，其将全力以赴遏制对手，不给他们任何攻击的机会。然而，我们认识到网络安全和韧性本身就是对利用漏洞进行攻击的一种遏制手段。

6.1.3. 我们将采取国家层面的全面网络安全和遏制措施，使英国成为更加难以攻击的目标，进而降低对手的不法利益、提高攻击成本——无论这些利益和成本是就政治、外交、经济还是战略而言。我们必须确保我们的能力和回应意图被潜在的对手所理解，以影响他们的决策。我们必须具备所需的工具和能力，以不给对手轻而易举损害我们网络和系统的机会、了解他们的意图和能力、大规模打击商用恶意软件威胁、以及应对网络空间威胁、保护国家安全。

6.2.减少网络犯罪

6.2.1. 我们需要提高成本、提高风险成本、降低网络犯罪分子犯罪活动的非法所得。在加强英国对网络攻击的防御能力及减少漏洞的同时，我们还必须坚决追捕持续瞄准英国的犯罪分子。

6.2.2. 执法机构将重点追捕持续将英国公民和企业作为攻击目标的犯罪分子。我们将与国内外合作伙伴一道，共同应对所有地区的犯罪分子，拆除其基础设施和便利化网络，与国家网络安全中心合作，不断提高网络安全意识和标准。

6.2.3. 本战略对《2013 年严重及有组织犯罪战略》进行了补充，其中规定

了英国政府对网络犯罪以及其他类型的严重和有组织犯罪的战略应对。国家打击犯罪局内的国家反网络犯罪单元（National Cyber Crime Unit, NCCU）负责领导和协调国家对网络犯罪的应对。反诈骗行动处（Action Fraud）提供了一个国家级的欺诈和网络犯罪报告中心。反区域有组织犯罪单元（Regional Organised Crime Units，ROCU）内的打击网络犯罪单位网络提供了区域一级的专家网络能力，为国家反网络犯罪单元和地方部队提供支持。

目标

6.2.4. 我们将通过遏制网络犯罪分子针对英国的不法行为、持之不懈地追捕反复将英国作为攻击目标的犯罪分子，以降低网络犯罪对英国及其利益的影响。

我们的做法

6.2.5. 为了降低网络犯罪的影响，我们将：

- 提高英国在国家、区域和地方层面的执法能力和技能，以查明、追捕、起诉和遏制英国和海外的网络犯罪分子；
- 更好地了解网络犯罪商业模式，从而知道从何处入手，实施针对性干预措施，以对犯罪活动产生最具破坏性的影响。通过运用这些知识，我们将：
  - 使英国成为针对本国犯罪活动的高成本、高风险国家，与业界合作，降低犯罪分子利用英国基础设施的能力；及
  - 通过拆除其基础设施、摧毁其金融网络，在上游打击网络犯罪、加大对犯罪商业模式的冲击，并尽可能将罪犯绳之以法。
- 建立国际伙伴关系，结束针对英国的网络犯罪分子的有罪不罚现象，将海外司法管辖区的罪犯绳之以法；
- 通过早期的干预措施，阻止个人被吸引或参与网络犯罪；
- 加强与行业的合作，主动向他们提供有关威胁的情报，由他们向我们提供他们掌握的上游情报，以协助我们的上游干预工作；
- 建立反诈骗行动处全天候报告和应急分配能力，与国家网络安全中心、国家打击犯罪局下的国家反网络犯罪单元及广大的执法部门联系起来，改善对网络犯罪受害者的支援，更加迅速地对所报告的犯罪进行回应，加强安全防护建议。执法部门将建立一个新的报告制度，实时共享网络犯罪与威胁信息；
- 与国家网络安全中心及私营部门合作，降低可能被网络犯罪分子大规模利用的英国基础设施漏洞；及
- 与金融部门合作，例如破坏不法分子网络，使得其盗窃证书换取金钱的企图在英国难以得逞。

对成功的衡量

6.2.6. 政府将通过评估以下成果的进展来衡量其在减少网络犯罪方面取得的成绩：

- 对攻击英国的网络犯罪分子有更大的破坏性影响、对较多的不法分子进行逮捕和定罪，以及通过执法干预摧毁较大数量的犯罪网络；
- 执法能力有所提高，其中包括专业专家和主流官员的能力和技能，提高海外合作伙伴的执法能力；
- 早期干预措施劝阻和改造罪犯的效力得到提高、规模进一步扩大；及
- 由于难以获得网络犯罪服务且预期效果低下，低级网络犯罪行为减少。

如果您是网络犯罪的受害者，该怎么办？

作为公众，如果您认为自己是网络犯罪或网络欺诈的受害者，应联系反诈骗行动处。

您可以运用反诈骗行动处的在线反诈骗工具，在一天的任何时间报告诈骗事件，亦可以拨打 0300 123 2040。如需更多信息，请访问 www.actionfraud.police.uk

反诈骗行动处服务由伦敦金融城警察局运作。

6.3. 反击外国敌对分子

6.3.1. 我们需要具备全面的政府能力，以应对日益威胁到我们政治、经济和军事安全的外国敌对分子的威胁。与国际合作伙伴展开合作将是我们取得成功的关键，我们将更加重视与他们的联系，共同对抗网络安全威胁，其中大部分内容不会在公共领域。我们对主权能力、行业及私营部门的合作关系的投资将继续巩固我们发现、观察和识别不断变化的对抗活动的能力。

目标

6.3.2. 我们将针对每个对手制定战略、政策和优先事项，以确保采取积极主动、协调一致和有效的方法来应对威胁、减少未来网络事件的数量和严重性。

我们的做法

6.3.3.为了减少外国敌对分子的网络威胁，我们将：

- 除了促进达成自愿、非约束的负责任国家行为规范、制定和实施信心提升措施之外，加强国际法在网络空间中的应用；
- 与国际伙伴合作，尤其是作为北约成员国进行集体防御、协作安全、加强遏制；
- 识别对手网络活动的独特性和一般性特征；
- 利用各种政府能力，制定和探索遏制及反击网络威胁的所有可用选择。我们将充分考虑其他相关因素，其中包括具体国家战略、国际网络优先事项、网络犯罪和繁荣目标；
- 利用现有网络和主要国际合作伙伴关系来分享当前和新生威胁信息，增加现有见解和专长价值；及
- 在符合国家利益的情况下，公开具体的网络身份。

对成功的衡量

6.3.4. 政府将通过评估取得以下成果的进展情况来衡量其在打击外国敌对分子的行动方面取得的成绩：

- 我们与国际伙伴建立的更加强有力的信息共享网络以及支持各国合法和负责的行为的更广泛的多边协议极大地促进我们对威胁的理解和反应能力，进而建立英国更强大的防御体系；及
- 我们的防御和遏制措施，以及针对具体国家的战略，使英国成为外国敌对分子较难得逞的硬目标。

6.4. 预防恐怖主义

6.4.1. 恐怖分子的技术能力目前仍然很有限，但他们依然野心勃勃地破坏英国的计算机网络，以公开和破坏为主要目标。政府将查明使用以及意图使用网络实现此目的的恐怖分子并对其进行干预。我们将尽量降低他们的影响，阻止恐怖分子网络能力的提升，避免其进一步威胁英国的网络和国家安全。

目标

6.4.2. 通过查明和瓦解对英国国家安全造成威胁的、目前有能力而且企图建立这种能力的恐怖主义网络分子，降低恐怖主义分子利用网络的威胁。

我们的做法

6.4.3. 为确保网络恐怖主义威胁保持较低水平，我们将：

- 侦查网络恐怖主义威胁、找出企图针对英国及其盟友实施破坏性网络操作的不法分子；
- 调查和瓦解这些网络恐怖主义分子，防止他们利用网络能力对英国及其盟友进行攻击；及
- 与国际伙伴密切合作，以更好地应对网络恐怖主义威胁。

对成功的衡量

6.4.4. 政府将通过评估以下成果的进展来衡量其在防止恐怖主义方面的成绩：

- 通过识别和调查英国的网络恐怖主义威胁来充分了解网络恐怖主义造成的风险；及
- 尽早地密切监测和瓦解恐怖主义网络能力，以防止该等恐怖主义能力的长远增长。

6.5. 加强主权能力 – 进攻性网络

6.5.1. 进攻性网络能力涉及故意侵入对手的系统或网络，意图将其破坏、瓦解或摧毁。进攻性网络是我们全方位能力的组成部分，以遏制对手、剥夺他们在网络空间和现实空间攻击我们的机会。通过国家进攻性网络计划（National Offensive Cyber Programme，NOCP），我们拥有在网络空间开展行动的专门能力，并将调拨资源进一步发展和提升这一能力。

目标

6.5.2. 我们将确保具备适当的可支配进攻性网络能力，可以根据国家和国际法，在我们选择的时间和地点进行部署，以实现遏制和行动之目的。

我们的做法

6.5.3. 为此，我们将：

- 投资国家进攻性网络计划——国防部与政府通信总部的合作伙伴关系，利用两个组织的技能和人才提供所需的工具、技能和谍报技术；
- 发展利用进攻性网络工具的能力；及
- 壮大武装力量，将进攻性网络能力部署为作战整体能力的一部分，以增强军事行动的整体效果。

对成功的衡量

6.5.4. 政府将通过评估以下成果的进展情况来衡量其建立进攻性网络能力的成绩：

- 英国的进攻性网络能力世界领先；及
- 英国已经建立起一系列发展和部署其主权进攻性网络能力的技能和专长。

6.6. 提升主权能力 – 密码学

6.6.1. 加密能力是保护我们最敏感信息、选择如何部署武装力量和国家安全能力的基础。为了维持这一能力，我们需要由政府通信总部保证的私营部门的技能和技术。这可能需要持有必要安全许可、在准备与政府通信总部开诚布公讨论设计和实施细节的公司工作的英国公民完成相应的工作。国防部和政府通信总部基于当前的市场情况，与目前能够提供此类解决方案的公司合作，以充分了解维护该等主权加密能力的长期成本影响。

目标

6.6.2. 我们有信心相信英国将始终具备对国家安全至关重要的加密能力进行政治控制的能力，也即保护英国机密的手段。

我们的做法

6.6.3. 我们将选择适当的方法，与盟友有效共享信息，确保在需要的时间和地点具备可用的、可信的信息和信息系统。政府通信总部和国防部与其他政府部门和机构紧密合作，共同界定主权要求以及如何在供应商必须为国内供应商的条件下，最好地满足这些要求。这将通过一个用来确定业务优势和行动自由要求的新的联合框架来实现。

7.开发

7.0.1. 本战略的开发部分阐述了英国如何获得和增强用来保护自己免受网络威胁的工具和能力。

7.0.2. 英国需要更多出色、合格的网络安全专业人士。政府将立即采取行动，解决关键的网络安全专业人士供需之间不断扩大的缺口，为该领域的教育和培训注入新的活力。这是一个长期且具有变革意义的目标，本战略将启动这项必然要持续到2021年之后的重要工作。技术精湛的员工队伍是充满活力、领先世界的网络安全商业生态系统的命脉。这个生态系统将确保网络初创公司走向繁荣并获得他们所需要的投资和支持。这种创新和活力只能由私营部门提供，但政府将采取行动支持其发展，积极推动更广大的网络安全部门走向世界市场。需要一个充满活力和蓬勃发展的科学研究部门对高技能人才的发展提供支持，并确保将新思想转化为尖端产品。

7.1. 加强网络安全技能

7.1.1. 英国需要解决网络技能短缺的核心系统性问题：缺乏进入该职业的年轻人、目前缺乏网络安全专家、电脑课程中网络和信息安全概念不足、缺乏合格教师、没有进入该行业的既定的职业和培训途径。

7.1.2. 这就要求政府迅速干预以解决目前的短缺问题，制定连贯一致的长期战略，以利用这些干预措施来弥补技能缺口。然而必须认识到，要产生深远的影响，这项工作必须协作完成，需要各地方分权政府、公共部门、教育机构、学术机构和行业的参与者及意见领袖的广泛参与。

目标

7.1.3. 政府的雄心是确保本国网络安全最优人才的持续供应，同时在短期内资助具体的干预措施，以帮助弥补已知的技能缺口。我们还将明确和发展整个人口和劳动力所需的网络安全技能，以确保网络安全运行。

7.1.4. 这需要未来二十年的行动，而不仅仅是五年。我们将明确政府、行业、教育机构和学术界所需的长期、协调一致的行动，以实现合格的、满足必要标准和认证、能够自信有把握地从事相应工作的网络安全专业人员的持续供应。

7.1.5. 我们将缩小国防部的技能缺口，吸引那些既得到有效培训、又志在维护国家安全的网络专家到政府工作。这包括了解网络空间对军事行动的影响。

我们的做法

7.1.6. 我们将制定和实施一项基于现有工作的独立技能战略，将网络安全纳入教育体系，继续完善计算机科学整体教学现状，将网络安全纳入课程。每个学习计算机科学、技术或数字技能的人都将学习网络安全的基础

知识，并能将这些技能带入工作。作为这项工作的一部分，我们将解决以网络为中心的职业的性别不平衡，吸引更多样化背景人才，确保从最广大的人才库中汲取人才。我们将与地方分权政府密切合作，以促进全英国采取一致的网络安全做法。

7.1.7. 我们将更清晰地列出政府、行业以及随着时间的推移参与其中的各方的角色。英国政府和地方分权政府在创造合适的网络安全技能环境、提升教育体系以反映工业和政府不断变化的需求方面发挥关键性作用。另外，雇主也有重要责任明确表达自己的需求，培养和发展员工和青年人进入这个行业。行业与学术界、专业机构和行业协会合作，在建立多元化、有吸引力的职业和培训路径方面发挥重要作用。

7.1.8. 认识到我们弥合技能缺口面临的集体挑战，我们将建立由政府、雇主、专业团体、技能团体、教育机构和学术界组成的技能咨询小组，以加强这些关键部门之间的协调。该小组将支持制定一项长期战略，该战略将会把广泛的数字技能领域考虑进去，确保网络安全考量协调一致，贯穿始终。该小组还将与英国的类似机构展开合作。

7.1.9. 除了这项工作，政府将会投资一系列可以迅速提升的举措，为发展长远的技能战略提供信息，其中包括：

- 创办学校课程，就针对有天赋的 14 至 18 岁青少年提供的专家网络安全教育与培训进行重大变革（包括课堂活动、由专家指导的课后活动、具有挑战性的项目和暑期学校）；
- 在能源、金融和运输领域创办更高的学位水平的学徒制课程，以解决重要领域的技能缺口；
- 设立资金，对在网络安全行业中显露极高潜力的员工队伍进行再培训；
- 识别优质的网络研究生，支持研究生教育，找出并填补所有专业技能缺口——确认大学在技能培养中的关键作用；
- 支持教师职业发展网络安全认证，以帮助教师和其他进行相关学习支持的人士了解网络安全教育，并为这部分人群提供进行外部认证的方法；
- 通过到 2020 年实现皇家特许（Royal Chartered）、加强行业内公认的网络安全卓越体系并提供一个可以为国家政策提供咨询、计划和信息的焦点中心，发展网络安全职业；
- 在国防部和更广大的政府机构成立国防网络学院（Defence Cyber Academy）作为网络培训和训练的卓越中心，解决专业技能和更广泛的教育问题；
- 发展政府、武装部队、业界和学术界之间的培训、教育合作机会，运用相关设施保持并进行技能练习；及
- 我们将与业界合作，壮大 CyberFirst 项目，以发现和培育多元化的年轻人才队伍、捍卫国家安全；及

- 将网络安全和数字技能作为从小学到研究生阶段教育系统相关课程的组成部分，制定标准、提高质量、为该专业领域向前发展提供坚实的基础。

由于教育权利下放的问题，部分举措主要适用于英格兰，但是我们将与地方分权政府合作，鼓励整个英国教育系统采用一致的做法。

对成功的衡量

7.1.10. 政府将通过评估以下成果的进展来衡量我们在加强网络安全技能方面的成绩：

- 具备进入网络安全职业的有效、清晰路径，能够吸引各个人群；
- 到 2021 年，将网络安全作为从小学到研究生阶段相关课程的一个组成部分进行有效教授；
- 网络安全作为既定职业被广泛认可，具有明确职业发展路径并取得皇家特许；
- 适当的网络安全知识成为相关非网络安全专业人士职业持续发展的一个组成部分，及
- 政府和武装部队可以接触到能够维护英国安全和韧性的网络专家。

7.2. 促进网络安全行业的发展

7.2.1. 生机勃勃的创新网络安全行业是现代数字经济必不可少的组成部分。英国网络安全公司为行业和政府提供世界领先的技术、培训和咨询。尽管英国世界领先，但是要保持其领先地位，仍然面临激烈的竞争，政府也要解决诸多障碍。英国公司和学者开发尖端技术，但有些技术则需要获得支持，以形成实现繁荣所需的商业和创业技能。在成长和扩展到新的市场和领域的过程中，中小企业因遭遇资金缺口受阻。那些有潜力使我们摆脱威胁的、最具突破性的产品和服务，尚需努力寻找愿意成为早期采用者的客户。要克服这些挑战，需要政府、行业和学术界的有效合作。

目标

7.2.2. 政府将支持英国建立一个迅速崛起、勇于创新和蓬勃发展的网络安全行业，以创建有如下特征的网络安全生态系统：

- 安全行业公司生机勃勃，而且能够获得成长需要的投资；
- 政府、学术界和私营部门的顶级人才密切合作、激励创新；及
- 政府和业界的客户有充分的自信并做好了充分的准备去采用先进的服务。

我们的做法

7.2.3. 为了建立这样的生态系统，我们将：

- 将学术创新商业化以及向学术界提供培训和指导；
- 建立两个创新中心，以推动尖端网络产品和动态新型网络安全公司的发展，它们是为初创企业提供支持、帮助他们获得第一批客户并吸引进一步投资这一举措的核心；

- 拨出 1.65 亿英镑的国防和网络创新基金中的一部分，为国防和安全领域的创新采购提供支持；
- 为公司开发产品提供测试设施，为下一代网络安全产品和服务提供快速评估，使客户有信心使用产品；
- 利用行业-政府网络发展伙伴关系的集体专长，以帮助形成和聚焦进一步的增长和创新干预；
- 帮助各种规模的公司扩大并进入国际市场；及
- 促进商定的国际标准，支持进入英国市场。

7.2.4. 我们还将利用政府采购的力量来刺激创新。政府面临着网络安全的最艰难挑战以及部分最大威胁，我们能够而且必须寻求这些问题的最有效解决方案。这意味着小公司可以更容易与政府做生意，另外，政府在测试和使用新产品方面必须减少风险规避。这是一个双赢的解决方案：一方面，政府将会获得最好的服务；另一方面，创新技术将会被尽早采用，进而更好地吸引投资和较大的客户群。我们会鼓励包括地方分权政府在内的政府各组成部分采取类似的做法。

对成功的衡量

7.2.5. 政府将评估取得以下成果的进展情况以衡量其在刺激网络安全行业发展方面的成绩：

- 英国网络行业规模同比增长高于全球平均增幅；
- 早期公司投资大幅增加；
- 政府采用更多更具创新性和更有效的网络安全技术。

“我们希望创建一个网络生态系统，让网络初创企业的数量能够迅速攀升，获得在全球范围内赢得业务所需的投资和支持，并提供一个创新渠道，在私营部门、政府和学术界之间输送创意。”

数字和文化部部长马特 •汉考克（Matt Hancock）议员阁下

7.3. 促进网络安全科技的发展

7.3.1. 英国蓬勃发展的科技及其尖端的研究领域为其世界领先的网络安全能力奠定了基础。为了维持和提升英国作为前沿研究领域全球领先国家的声誉，需要学术研究机构继续吸引网络安全领域最优秀和最出色的人才，推动卓越中心吸引最有能力和最有活力的科学家和研究人员，加深学术界、政府和业界之间的积极伙伴关系，其中，政府将发挥其桥梁作用，鼓励此类协作。我们将成功建立一个自我维持的生态系统，使思想和人才以互利的方式得以在这三个领域流通。

目标

7.3.2. 到 2021 年，英国将进一步巩固其在网络科技领域的世界领先地位。高等院校和行业之间的灵活伙伴关系能够将研究转化为商业上成功的产品和服务。英国将继续保持其卓越

创新声誉，包括金融等具有特殊国力的领域。

我们的做法

7.3.3. 为实现这一目标，政府将鼓励以合作、创新和灵活的融资模式进行研究，促进研究的商业化。政府将确保对网络领域的人和行为方面给予足够的关注，而超出技术层面的系统，如业务流程和组织结构，则被纳入网络科技的范畴。

7.3.4. 对“默认安全”的产品、系统和服务提供支持，从一开始以及安全性成为用户有意识的“选择退出”之处，将恰当的安全保障考虑在内。

7.3.5. 在与合作伙伴和利益攸关方进行深入磋商后，我们将发布详细的《网络科技战略》，其中明确政府、业界和学术界认为重要的科学和技术领域，以及目前英国在这些领域的网络安全能力缺口。

7.3.6. 政府将继续为卓越学术中心、研究所、博士生培养中心提供资助和支持，此外，在富有战略意义的学科领域成立一个新的研究所，在即将发布的《网络科技战略》所明确的能力缺口方面提供科研资助。纳入考虑范畴的重要领域包括：大数据分析、自治系统、可信赖的工业控制系统、网络物理系统和物联网、智慧城市、自动化系统验证以及网络安全科学。

7.3.7. 我们将继续资助英国卓越学术中心的国家博士生，增加具备网络专长的英国公民的数量。

7.3.8. 政府将与包括创新英国和研究理事会在内的机构合作，鼓励业界、政府和学术界之间的合作。为支持此合作，我们将审查有关安全分类的最佳做法，确定包括学者在内的安全调查专家，确保无论是不保密领域还是保密领域的工作，都尽可能协作完成。

7.3.9. 政府将资助一个“大挑战”，以确定并提供创新的解决方案，解决网络安全方面的一些最紧迫问题。网络投资（CyberInvest）作为一项新的行业和政府合作伙伴关系，将支持尖端的网络安全研究、在网络空间保护英国，并将成为我们建立学术界-政府-业界合作关系的做法的组成部分。

对成功的衡量

7.3.10. 政府将通过评估以下成果的进展来衡量其在促进网络安全科技方面的成绩：

- 显著增加能够将学术网络研究成果成功商业化的英国公司的数量，采取有效措施降低并弥补英国网络安全研究能力的公认缺口；
- 英国被视为网络安全研究与创新的全球领军者。

7.4. 有效的水平检视

7.4.1. 政府必须确保在制定政策时，将不断变化的网络、地缘政治和技术格局纳入考虑范畴。为此，我们需要有效利用水平检视和评估工作，通过投资抵抗未来威胁，同时预测五到十年内可能影响我们的网络韧性的市场变化。需要通过水平检视项目来给出

建议，为当前和未来的政府政策和项目规划提供信息。

目标

7.4.2. 政府将确保严格评估网络风险，与全源评估和其他现有证据一起，纳入网络安全和其他技术政策开发领域。我们将联合国家安全与其他政策领域的水平检视，对新出现的挑战和机遇进行整体评估。

我们的做法

7.4.3. 我们将：

- 明确当前的工作差距，协调跨学科工作，制定整体的网络安全水平检视方法；
- 促进网络安全技术方面与行为科学更好结合；
- 严格监测网络犯罪市场，发现可能使技术转让给敌对国家、恐怖分子或不法分子的新工具和服务；
- 分析紧急互联网过程控制技术；
- 预测数字货币漏洞；及
- 监测电信技术的市场趋势，发展针对未来预期攻击的早期防御。

7.4.4. 我们认识到水平检视在技术之外，还包含政治、经济、立法、社会和环境维度，网络安全只是有效的水平检视可以帮忙解决的问题的一个方面。因此，我们将确保在其他政策领域进行水平检视时，考虑到所有网络安全的影响。

7.4.5. 我们还将确保网络政策的制定遵循循证方法，并考虑到所有可用来源的评估，其中包括，例如：

- 具体的技术证据，例如物联网或先进材料的未来作用；及
- 国际战略、社会趋势及其对网络的影响。

7.4.6. 我们将确保在跨政府新兴技术与创新分析小组（ETIAC）的职权范围内考虑网络安全。ETIAC 的建立旨在确定与国家安全相关的技术威胁和机会，将网络安全考虑纳入现有的水平检视结构，包括政府未来小组（Government Futures Group）以及内阁大臣的水平检视咨询小组（CSAG）。

对成功的衡量

7.4.7. 政府将通过评估以下成果的进展来衡量其建立有效水平检视职能所取得的成绩：

- 将跨政府水平检视和全源评估纳入网络政策制定过程；及
- 将网络安全的影响作为所有跨政府水平检视因素。

8.国际行动

8.1. 我们的经济繁荣和社会安康日益依赖超出我们自己国境的网络开放和安全。我们必须与国际合作伙伴密切合作，确保实现上述益处的网络空间持续免费、开放、和平与安全。随着全球下一批 10 亿用户上网，确保实现上述益处的网络空间持续免费、开放、和平与安全只会变得更加重要。

8.2. 网络问题国际合作已成为更广泛全球经济与安全讨论的基本内容。这是政策迅速变化的领域，没有一致同意的单一国际目标。英国及其盟友已成功确保基于规则的国际体系具备部分要素：达成网络空间的国际法适用协议、线上和线下同样适用人权、就多利益攸关方治理是管理互联网治理复杂性的最佳办法取得广泛一致。不过，由于对如何应对国家安全与个人权利和自由调和的共同挑战分歧日增，任何达成的全球共识仍然脆弱。

“我们必须进行国际合作，就确保英国未来网络空间安全和繁荣途径的规则达成一致。”
鲍里斯•约翰逊（Boris Johnson）议员阁下
外交大臣

目标

8.3. 英国希望保卫网络空间的长期自由、开放、和平与安全，推动经济增长、支撑英国国家安全。在此基础上，英国将继续：倡导多利益攸关方治理互联网模式、反对数据本地化、努力建设合作伙伴改善其自身网络安全的能力。为了减少相当部分源自海外的对英国和我们利益的威胁，我们将寻求影响那些参与打击网络犯罪、网络间谍、破坏性或毁灭性网络活动决策的人士，继续建设支持国际合作的框架。

我们的做法

8.4. 为此我们将：

- 加强、牢记对网络空间负责任政府行为的共同理解；
- 达成网络空间国际法适用协议；
- 继续促进达成自愿、非约束的负责任国家行为规范；
- 支持信任建立措施的制定与实施；
- 增强我们破坏、起诉国外犯罪分子，尤其是在难以抵达司法辖区的犯罪分子的能力；
- 帮助培育一种环境，在此环境下我们的执法机关能够合作以确保犯罪分子能够采取行动而无惧调查和起诉的场所越来越少。
- 通过影响新兴技术（包括加密）全球管理的技术标准促进网络空间的韧性，使网络空间增强“设计安全”，并促进最佳做法；
- 努力在志同道合的国家中打造强加密之类能力的通用方式，产生跨境影响；
- 打造其它国家的能力以解决对英国和我们海外利益的威胁；
- 继续帮助我们的合作伙伴发展自身网络安全——既然我们同属一个网络空间，当各国完善自身防御时我们全体才变得更加强大；
- 确保北约为 21 世纪的这些冲突做好准备。这些冲突不仅将在战场，还将在网络空间展现。
- 与我们的盟友合作，以使北约在网络空间行动像在海陆空行动一样高效；
- 确保“网络空间全球大会”（Global Conferences on Cyberspace）的

《伦敦进程》（London Process）继续促进全球对免费、开发、和平与安全网络空间的共识。

8.5. 有一系列我们将继续投入资源的关系和工具，以实现和支持我们的全部国际网络目标；我们无法单独实现我们的目标。这些关系和工具包括：

- 与传统盟友和新合作伙伴协调一致，建立、维持强大积极的政治军事关系；创造建设强大全球联盟的政治条件；
- 利用我们在多边组织和全球开发社会的影响，这些多边组织包括联合国、二十国集团、欧盟、北约、欧洲安全与合作组织、欧洲理事会、英联邦等；
- 与业界、公民社会、学术界、科技界等非政府界建立更牢固的关系。他们对了解和质疑国际政策制定、强化一系列广泛网络问题的政治讯息至关重要。我们世界一流的学术联系提供一个与国际合作伙伴合作的中立合作平台。

对成功的衡量

8.6 政府将通过评估以下成果进展来衡量其在推进我们网络国际利益方面取得的成绩：

- 国际合作加强减少对英国和我们海外利益的网络威胁；
- 对网络空间负责任政府行为取得共同理解；
- 国际合作伙伴增强其网络安全能力；及
- 对于免费、开放、和平与安全网络空间益处的国际共识加强。

9.指标

9.1. 就成果与影响衡量——通常指各种指标——而言，网络安全仍然是相对不成熟的领域。网络安全科学已经因为夸大其词而令人费解，并因缺乏标准化数据而发展受阻。这既是决策者，同样也是企业感到沮丧的一个原因。企业难以衡量投资与投资所产生的成果。政府认为，对指标的有效使用对实现本战略以及集中支持本战略的资源必不可少。

9.2. 我们将确保本战略建立在一套严格的综合指标基础之上，我们根据这些指标衡量我们迈向需要实现的成果的进度。国家网络安全中心不仅是本战略的主要独立实现力量，还将在使政府其他部门、各行业和社会实现本战略内所有战略成果的过程中发挥至关重要的作用。

9.3. 附录 3 说明了本战略列出的成果衡量指标将如何有助于实现战略成果。这些指标每年将进行评估，以确保准确反映了我们的国家目标和要求。重要的战略成果如下所述：

1. 英国有能力有效检测、调查、反击我们敌对分子网络行为造成的威胁。

2. 网络犯罪对英国及其利益的影响显著降低，遏制网络犯罪分子针对英国采取行动。

3. 英国具备有效管理、响应网络事件以降低网络事件对英国造成的伤害，以及反击网络敌对分子的能力。

4. 我们与各行业在主动网络防御方面的合作意味着大规模钓鱼和恶意软件攻击不再有效。

5. 由于科技产品和服务具备网络安全设计并默认激活，英国更加安全。

6. 战略实施伊始政府网络和服务将做到尽可能安全。公众将能够满怀信心地使用政府数字服务，相信其信息安全。

7. 在监管和激励恰当并举的支持下，英国无论大小组织有效管理其网络风险，得到国家网络安全中心设计的高质量建议支持。

8. 在英国有恰当的生态系统，以发展、维持能够满足我们国家安全需求的网络安全行业。

9. 英国持续提供本国培养的网络技能专业人才，满足公私部门和国防部门日益数字化经济不断发展的需求。

10. 英国被普遍认可为网络安全研发全球领军者，得到英国各行业和学术界高水平专家知识的支持。

11. 英国政府已计划、准备实施领先未来技术和威胁的政策，面向未来。

12. 由于国际共识和在一个免费、开放、和平、安全的网络空间实现负责任政府行为的能力增

强，英国和我们的海外利益所受威胁减少。

13. 简化英国政府政策、组织和结构，以最大化英国对网络威胁响应的一致性和效果。

9.4. 我们认识到，我们本战略的部分宏伟目标超过了五年战略期。为了让2021年之后的任何网络投资能够继续实现最大变革效果，随着网络安全风险有效管理被纳入大家的标准管理活动，我们打算把2021年后实现的长期目标分配给业界、监管部门、审计领域、保险公司和公私部门的其它组成部分。

结论：2021 年之后的网络安全

10.1. 随着技术演变和我们的敌对分子设法加以利用，网络格局的迅速演变将不断提出新挑战。不过，本战略旨在提供将确保我们能够对所出现的每一项新挑战做出迅速、灵活反应的一系列政策、工具和能力。

10.2. 如果我们未能有效行动，威胁将继续超过我们保护自己不受威胁的能力。可以预计，各水平威胁能力将急剧增长。

10.3. 相反如果我们实现这些宏伟目标，英国政府各部门、企业和社会将各行其职，实现本国整体网络安全。如果我们能够确保商用技术具有安全设计并默认内置安全，消费者和企业将较少担心网络安全。要是英国巩固其网络经营环境安全的声誉，更多全球性公司和投资者将选择落户英国。关键国家基础设施网络安全和重点行业将更加有效。希望发展针对掌握关键功能和数据系统的工具和攻击方法的潜在攻击者反过来将不得不更加努力，以攻克围绕这些系统的层层安全保护。这将改变网络犯罪分子和恶意分子的风险回报比，他们料将面临与进行传统犯罪同样的国际起诉风险。如果我们能够成功使网络安全在社会各方面成为主流，那么这也许意味着政府本身可从如此突出的地位抽身，让市场和技术推动网络安全在经济与社会领域的发展。

10.4. 即便是在最乐观的情形之下，英国在网络领域面临的部分挑战——无论是大规模的挑战还是复杂的挑战——或将需要不止五年的时间才能解决。尽管如此，本战略为我们提供了在数字时代改变我们未来安全状况和保卫我们繁荣的途径。

附录 1：首字母缩略词

CCA – 网络评估中心，隶属国家网络安全中心，为英国政府各部门提供网络威胁评估以资政策参考。

CERT – 国家计算机应急反应小组。

CERT-UK – 英国国家计算机应急反应小组。

CESG – 英国国家信息保障技术局，代表英国政府就信息安全提供可信、专业、独立、研究性和情报性服务。

CNI – 关键国家基础设施。基础设施中至关重要的部分（即资产、设施、系统、网络或流程，以及运营、推动关键国家基础设施的基本员工），其损失或危害有可能导致：

a. 基本服务（包括那些完整性如果受损有可能导致重大伤亡的服务）的可得性、完整性和实现遭受重大损害——考虑重大经济或社会影响；及/或
b. 显著影响国家安全、国防或政府运行。

CPNI – 国家基础设施保护中心，提供旨在增强国家基础设施各组织应对恐怖主义和间谍活动能力的建议。该中心还将与国家网络安全中心合作，就网络空间威胁提供整体保护性安全建议。

国家基础设施保护中心已与国家基础设施各私营部门组织建立了牢固合作关系，打造了信息能够互利共享的可信任环境。包括政府其它部门和专业服务机构的扩展网络增强了直接关系。

DDoS - 分布式拒绝服务攻击。信息系统的泛滥，请求数超出系统的处理能力，导致授权用户无法进入该系统。

GCHQ - 政府通信总部；政府的信号情报活动中心和国家网络技术权威机构（NTA）。

ICT - 信息与通信技术。

MOD - 国防部

NATO - 北约。

NCA - 国家打击犯罪局；一个非内阁政府部门。

NCSC - 国家网络安全中心。

OSCE - 欧洲安全与合作组织。

SME - 中小企业。

附录 2：词汇表

反诈骗行动处 - 英国的国家诈骗与网络犯罪举报中心，为公众和企业提供一个联络中心。

主动网络防御 - 实施安全措施，以加强网络或系统安全，使其更加强劲地对抗攻击。

匿名化 - 用加密匿名工具在互联网上隐藏或掩饰一个人的身份。

身份验证 - 验证用户、程序或设备身份或其它属性的过程。

自动系统验证 - 确保软硬件按预期方式工作而不发生错误的方法。

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。

大数据 - 过大的数据集，以至于难以使用商用软件工具及时处理和管理，并且要求具备定制处理能力以管理其数量、传输速度和来源多样性。

比特币 - 一种数字货币与支付系统。

商用恶意软件 - 可广泛购买或免费下载的恶意软件，非定制，被各种不同的威胁源所使用。

计算机网络刺探 - 网络间谍；利用计算机网络渗透到目标计算机网络并收集情报。

网络犯罪市场 - 支持网络犯罪生态系统的所有产品与服务的总和。

密码学 - 分析与破译代码和密码的科学或研究；密码分析。

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。

网络投资（CyberInvest） - 一项 650 万英镑的行业与政府计划，用以支持前沿网络安全研究，在网络空间为英国提供保护。

网络物理系统 - 将计算与物理组成部分相结合的系统；“智慧”系统。

网络韧性 - 系统和组织抵御网络事件，并从网络事件伤害中恢复的整体能力。

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造成的伤害，或意外伤害。

网络安全挑战赛 - 鼓励人们测试自己的技能并考虑开启网络职业生涯的竞赛。

网络空间 - 相互依存的信息技术基础设施网络，包括互联网、电信网络、计算机系统、联网设备和嵌入式处理器与控制器。还指作为一种成熟现象或抽象概念的虚拟世界或域。

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

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。

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。

域名系统 - 以域的层级为基础的计算机和网络服务命名系统。

Doxing - 在互联网上调查或窃取一个人的身份识别信息，然后发布该信息。

电子商务 - 通过互联网进行的贸易，或通过互联网促成的贸易。

加密 - 对信息（即“明文”）的密码转换，将信息转换为另一种形式（即“密文”），隐藏数据的原意，防止他人获知或使用该数据。

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。

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可危害或损害系统或网络的不良网络事件。

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。

工业控制系统 - 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。

工业物联网 - 物联网在制造与工业中的使用。

内部人士 - 对组织的数据和信息系统拥有受信任的访问权限，并故意、意外或无意构成网络威胁的人员。

完整性 - 信息未被意外或蓄意变更，且保持准确和完整的性质。

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

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。

伦敦进程 - 2011 年伦敦网络空间大会上提议的措施。

恶意软件 - 恶意的软件或代码。恶意软件包括病毒、蠕虫、木马和间谍软件。

网络（计算机） - 一批主机及其用以交换数据的子网和互联网络。

进攻性网络 - 利用网络功能扰乱、禁用、降级或破坏计算机网络和联网设备。

打补丁 - 更新软件以修复故障和漏洞的过程。

渗透测试 - 由被测试组织授权或发起的活动，旨在测试网络或设施应对黑客时的韧性。

网络钓鱼 - 利用貌似来自可信任来源的电子邮件欺骗收件人点击恶意链接或带有恶意软件的附件，或与未知第三方分享敏感信息。

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。

侦查 - 攻击的一个阶段，其中攻击者收集网络上的信息，映射网络，并且探测网络上可利用的漏洞以非法侵入网络。

风险 - 特定网络威胁利用信息系统漏洞并造成危害的可能性。

路由器 - 基于 IP 地址将信息转发至其它网络从而连接各逻辑网络的设备。

脚本小子 - 技术较差的人利用互联网上的已有脚本或程序进行网络攻击，比如网页篡改。

默认安全 - 解锁商用技术的安全使用，安全为用户默认设置。

设计安全 - 从头至尾采用安全设计的软件、硬件和系统。

短信欺骗 - 一项用字母数字文本替换原手机号（发件人 ID）来掩饰短信来源的技术。发件人可以用其姓名、公司名等替换其手机号，从而合法使用该技术。或者有人非法使用该技术，例如冒充他人实施诈骗。

社交工程 - 攻击者用来欺骗和操纵受害者做出某种行为或泄露保密信息的方法。一般来说，这些行为包括打开恶意网页，或运行不想要的文件附件。

可信平台模块 - 一项关于安全加密处理器的国际标准，该加密处理器是一种通过在设备上整合加密密钥来保护硬件安全的专用微处理器。

用户 - 访问系统（无论是否经过授权）的个人、组织实体或自动化程序。

病毒 - 病毒指可传播至其他文件的恶意计算机程序。

语音钓鱼 - 或称“声讯诈骗”，指利用语音技术（固定电话、手机、语音邮件等）哄骗个人向未经授权的实体泄露敏感财务信息或个人信息，通常用于支持欺诈活动。

漏洞 - 可能被攻击者利用的软件程序故障。

附录 3：总体实施方案

2016-2021 年国家网络安全战略

愿景：英国面对网络威胁能够保持安全和韧性；在数字世界表现出繁荣和自信

战略成果	衡量成功的指示性标准（至 2021 年）	有助于
1.英国有能力有效检测、调查、反击我们敌对分子网络行为造成的威胁。	• 我们在“遏制”方面与国际合作伙伴建立的信息共享网络更加强大，各国间签订的以支持合法和负责任行为的多边协议更加广泛，这些都大大增强了我们了解和应对威胁、建立更安全英国的能力。 • 我们的防御与遏制设施及具体国家战略使英国成为外国敌对分子和网络恐怖分子较难得逞的目标。 • 通过对英国网络恐怖主义威胁的鉴别和调查进一步了解来自外国敌对势力和恐怖分子的网络威胁。 • 通过密切监控恐怖分子的网络能力和尽快破坏恐怖主义的网络潜能与网络活动，确保将恐怖分子的网络能力长期保持在较低水平。 • 英国成为进攻性网络能力的世界领军者。 • 英国已建立一条技能和专长渠道，来开发和部署我们的主权进攻性网络能力。 • 我们的主权加密能力可以有效保护我们的机密和敏感信息，防止未经授权的披露。	遏制
2.网络犯罪对英国及其利益的影响显著降低，遏制网络犯罪分子针对英国采取行动。	• 随着被捕和定罪人数的增加，以及通过执法干预瓦解了更多的犯罪网络，我们对于攻击英国的网络犯罪产生了更大的破坏性影响。 • 执法能力增强：包括专家和主流官员能力与技能提高；海外执法能力增强。 • 早期干预（预防）措施有效性增强、规模扩大，对不法分子不断起到阻止和改造作用。 • 因网络犯罪服务的获取变难、网络犯罪服务有效性降低，使得低水平网络犯罪减少。	遏制
3.英国具备有效管理、响应网络事件以降低网络事件对英国造成的伤害，以及反击网络敌对分子的能力。	• 向防御部门举报的网络事件的比例提高，加深了对于威胁大小和规模的了解。 • 因创建国家网络安全中心，将其作为集中的事件举报和应对机制，使得网络事件的管理变得更加有效、高效和全面。 • 我们将从国家层面解决攻击的根源，减少对多名受害者和多个部门的反复利用。	防御

4.我们与各行业在主动网络防御方面的合作意味着大规模钓鱼和恶意软件攻击不再有效。	• 由于我们针对恶意域名的使用采取了大规模“防御”，采用了更加主动的规模化反网络钓鱼防护，再加上利用“语音钓鱼”和短信欺骗等其他通信方式进行社交工程攻击的难度加大，使针对英国的“网络钓鱼”难度增大。 • 阻止了更多与网络攻击和网络刺探相关的恶意软件通信与技术产品。 • 恶意分子重新路由对英国互联网和通信流量的影响大大降低。 • 极大增强了政府通信总部、国防部和国家打击犯罪局应对严重的国家资助犯罪威胁的能力。	防御
5. 由于科技产品和服务具备网络安全设计并默认激活，英国更加安全。	• 2021 年，具有防御功能的大量商用产品与服务将使英国更加安全，因为这些产品与服务默认启用默认安全设置，或在设计中集成了安全性能。 • 英国公众信任政府服务，因为政府服务的实施能够尽可能实现安全，且针对这些服务的欺诈水平处于可接受的风险参数内。	防御
6.战略实施伊始政府网络和服务将做到尽可能安全。公众将能够满怀信心地使用政府数字服务，相信其信息安全。	• 政府对于整个政府和更加广泛的公共领域的防御网络安全风险有着深入了解。 • 单个政府部门和其他机构会根据其风险等级和公认的政府最低标准为自身提供保护。 • 政府部门和更加广泛的公共领域具有韧性，可有效应对网络事件，维护其功能，并迅速恢复。 • 政府部署的新的技术与数字服务将默认保障网络安全。 • 我们已经意识到，并在积极减少政府系统与服务中所有已知的面向互联网的漏洞； • 所有政府供应商都能达到合适的网络安全标准要求。	防御
7.在监管和激励恰当并举的支持下，英国无论大小组织有效管理其网络风险，得到国家网络安全中心设计的高质量建议支持。	• 我们了解关键国家基础设施的网络安全水平，做出防御，必要情况下，会执行干预措施，以推动加强国家利益。 • 多数公司与组织都了解受威胁程度，并会实施相应的网络安全实践。 • 与相当的发达经济体相比，英国经济的网络安全水平与之相当或者更高。 • 由于网络健康标准的实施，对位于英国的企业成功实施的网络攻击的次数、严重程度和影响均有所下降。 • 由于组织和公众均了解其网络风险水平，并知道需要采取哪些网络健康措施以管理这些风险，英国的网络安全文化在不断加强。	防御

8.在英国有恰当的生态系统，以发展、维持能够满足我们国家安全需求的网络安全行业。	• 英国网络行业规模同比增速高于全球平均水平。 • 对早期公司的投资出现大幅增长。	开发
9.英国持续提供本国培养的网络技能专业人才，满足公私部门和国防部门日益数字化经济不断发展的需求。	• 有进入网络开发安全行业的有效、清晰路径，吸引着各种各样的人们。 • 到 2021 年，从小学生到研究生，在教育系统内网络安全将作为相关课程中必不可少的组成部分得到有效教授。 • 网络安全被公认为一个已经成型的行业，拥有清晰的职业发展路径，并获得了皇家特许。 • 相应的网络安全知识将成为整个经济体内各相关非网络安全专业人员谋求持续职业发展时必不可少的组成部分。 • 政府和武装部队可以利用网络专家维护英国的安全与韧性。	开发
10.英国被普遍认可为网络安全研发全球领军者，得到英国各行业和学术界高水平专家知识的支持。	• 成功开发商业化学术网络研究的英国公司数量大幅上升。公认、确定的英国网络安全研究能力的缺口减少，且英国已采取有效措施来弥合这些缺口。 • 英国被看作是网络安全研究与创新的全球领军者。	开发
11. 英国政府已计划、准备实施领先未来技术和威胁的政策，面向未来。	• 在网络政策的制定中结合跨政府水平扫描工作和全源评估。 • 在所有的跨政府水平扫描工作中均考虑网络安全影响。	开发
12. 由于国际共识和在一个自由、开放、和平、安全的网络空间实现负责任政府行为的能力增强，英国和我们的海外利益所受威胁减少。	• 国际合作的增强削弱了对英国及我们海外利益的网络威胁； • 对网络空间内负责任的国家行为达成共识； • 国际合作伙伴的网络安全能力有所增强； • 对于营造自由、开放、和平和安全网络空间的好处，形成越来越多的国际共识。	国际行动与影响力
13. 简化英国政府政策、组织和结构，以最大化英国对网络威胁响应的一致性和效果。	• 政府的网络安全职责得到了解，且其服务具有易用性。 • 我们的合作伙伴了解如何最好地与政府就网络安全问题进行互动。	整合