Use the force—responsibly

文章导读：“黑客攻击”是指：通过未经授权访问帐户或计算机系统来入侵数字设备和网络的行为。黑客攻击并不总是恶意行为，但通常与网络罪犯的非法活动和数据窃取有关。黑客攻击是指滥用计算机、智能手机、平板电脑和网络等设备，目的是损坏或破坏系统，收集用户信息，窃取数据和文档，或者破坏数据相关活动。他们会使用网络安全软件和 IT 团队完全无法察觉的隐秘攻击方法。他们还擅长创建攻击向量，诱骗用户打开恶意附件或链接，还会让用户心甘情愿地提供敏感的个人数据。因此，现代的黑客攻击并非只是一群乌合之众的恶作剧，而是一个价值数十亿美元的行业，拥有极其精湛和成功的技术。

<table>
<tr><td>【1】State hackers need to wield[1] their weapons with precision and care</td><td>【1】国家黑客需要精确而谨慎地使用他们的武器</td></tr>
<tr><td colspan="2">一、重点词汇
1. Wield /wi:ld/ v. 挥，操，使用（武器、工具等）；运用（权力），施加（影响）</td></tr>
</table>

<table>
<tr><td>【2】Russia’s cyberwar in Ukraine has been as reckless[1] as its physical one. Its cyber-attack on satellites[2] on the first day of fighting mistakenly spilled over into almost 6,000 German wind farms. It sprayed[3] “wiper” malware[4] across the country, irreversibly destroying data. And it directed attacks at civilian power and water infrastructure, adding to the misery of its shells and rockets. It has been one of the most intensive cyber-campaigns ever conducted—and perhaps the most irresponsible.</td><td>【2】俄罗斯在乌克兰的网络战和实体战一样鲁莽。在战斗的第一天，它对卫星的网络攻击错误地波及了近 6000 个德国风电场。它在全国范围内散布“雨刷”恶意软件，不可逆转地破坏数据。它还将攻击目标对准了民用电力和供水基础设施，这增加了其在炮弹和火箭弹中的痛苦。这是有史以来最密集的网络活动之一也许也是最不负责任的。</td></tr>
<tr><td colspan="2">一、重点词汇
1. Reckless/ˈrekləs/ adj. 鲁莽的，不计后果的；粗心大意的</td></tr>
</table>

2. Satellite/ˈsætəlaɪt/ n. 卫星；人造卫星；卫星国，附属国；卫星城镇
3. Spray /spreɪ/ n. 喷雾液体，喷剂；v. 喷，喷洒（液体）；（使）飞溅，（使）飞散；
4. Malware /ˈmælwer/n. 恶意软件

二、同义表达

1. 表达"蔓延、波及"

（1）Spread：表示"扩散、传播"。例如：

The virus may spread to the neighboring city if no actions are taken.（如果不采取措施，这种病毒可能会传播到附近的城市。）

The disease has been spreading rapidly in recent weeks.（这种疾病最近几周一直在迅速扩散。）

(2) Extend：表示"延伸、蔓延"。例如：

The influence of the epidemic extends beyond the medical field.（这次流行病的影响超出了医学领域。）

The fire extended to the nearby houses.（火势蔓延到了附近的房屋。）

(3) Reach：表示"到达、扩及"。例如：

The epidemic reached Europe and caused widespread panic.（这次流行病传到欧洲，引起了广泛的恐慌。）

The impact of the disaster has reached every corner of the country.（这场灾难的影响已经扩及了全国各地。）

【3】But what is a responsible cyber power? On April 4th Britain's National Cyber Force (NCF) sought to answer that question by publishing a document setting out how it views the purpose and principles of "offensive cyber"—the disruption[1] of computer net works, as distinct from cyber-espionage[2]. It also revealed the identity of the NCF's commander[3], James Babbage, who has given his first interview, to The Economist (see Britain section).	【3】但是什么是负责任的网络强国呢?4 月 4 日，英国国家网络部队(NCF)试图通过发布一份文件来回答这个问题，该文件阐述了它如何看待"进攻性网络"的目的和原则，"进攻性网络"是指与网络间谍活动不同的对计算机网络的破坏。它还透露了 NCF 指挥官詹姆斯·巴贝奇的身份，他第一次接受了《经济学人》的采访(见英国部分)。

一、重点词汇

1. Disruption /dɪsˈrʌpʃn/ n. 扰乱，中断
2. Espionage /ˈespiənɑ：ʒ/ n. 间谍行为，谍报活动
3. Commander /kəˈmændər/ n. 指挥官，长官；海军中校；英国高级警官；高级骑士（或爵士）

二、表达积累

1. 美国军官不同头衔的英文称谓

General of the Army （五星上将）、General （上将）、Lieutenant General （中将）、Major General（少将）、Brigadier General （准将）、Colonel （上校）、Lieutenant Colonel （中校）、Major （少校）、Captain （上尉）、First Lieutenant （中尉）、Second Lieutenant （少尉）、Chief Warrant Officer （一级

准尉）、Warrant Officer （二级准尉）

【4】Britain's transparency is a welcome step forward. Cyber operations are shrouded[1] in secrecy[2].They can spill over[3] into the computer networks that modern economies and societies depend on—a Russian cyber-attack in 2017 caused more than $10bn of damage. Their potential is also poorly understood. Many political leaders mistakenly view them as strategic weapons to deter[4] enemies.	【4】英国的透明度向前迈出了可喜的一步。网络行动是保密的。它们可能会蔓延到现代经济和社会所依赖的计算机网络中，2017 年俄罗斯的一次网络攻击造成了逾 100 亿美元的损失。人们对它们的潜力也知之甚少。许多政治领导人错误地将核武器视为威慑敌人的战略武器。

一、重点词汇

1. Shroud /ʃraʊd/n. 裹尸布，寿衣；<文>覆盖物，遮蔽物；（技）护罩，管套；v. 覆盖，隐藏；隐瞒，保密；用布裹（尸体）
2. Secrecy /ˈsiːkrəsi/n. 秘密，保密
3. Spill over 溢出；被迫使出来
4. Deter /dɪˈtɜːr/v. 使打消念头，防止，威慑

【5】The NCF's new paper is important because it spells out a realistic and circumscribed[1] view of cyber power. It says that its main purpose is not so much kinetic[2]—a digital substitute for air strikes—as cognitive. Russia's cyber-enabled disinformation[3] is often aimed at entire populations. Britain says its targets are typically individuals and small groups. A cyber-attack might, for example, tinker[4] with their communications so they are paralysed by confusion, or turn on one another	【5】NCF 的新资料很重要，因为它阐明了对网络权力的现实而有限的观点。它说它的主要目的与其说是动力学——空袭的数字替代品——不如说是认知。俄罗斯利用网络制造的虚假信息往往针对全体民众。英国表示，其目标通常是个人和小团体。例如，网络攻击可能会修补他们的通信，使他们因混乱而瘫痪，或者相互攻击

一、重点词汇

1. Circumscribed /ˈsɜːrkəmˌskraɪb/adj. 外接的；局限的；受限制的
2. Kinetic /kɪˈnetɪk/ adj. [力] 运动的；活跃的
3. Disinformation/ˌdɪsˌɪnfərˈmeɪʃn/n. 故意的假情报；虚假信息
4. Tinker /ˈtɪŋkər/ n. 补锅匠；（经验不足的）修补匠；焊锅；v. （徒劳地或马虎地）小修补

二、同义表达

1. 表达"修补"的地道英文表达

（1）Revamp

I had to revamp the car's engine to get it running again.（我不得不重新整修汽车引擎以使其重新运转。）

（2）Mend

She mended the hole in her shirt with a needle and thread.（她用针线把衬衫上的洞修好了。）

（3）Patch

He used duct tape to patch the leak in the pipe.（他用防水胶带来修补漏水的管子。）

（4）Repair

The mechanic was able to repair the damage to my car's bumper.（修车工人成功地修复了我的车子保险杠的损伤。）

（5）Fix （口语用法较多）

I need to fix the broken window before it rains.（我得在下雨前修好破损的窗户。）

【6】The British example suggests several criteria[1] to judge whether cyber power is being used responsibly. The first is what sort of targets are chosen. North Korean hackers once attacked an American film studio because it released an unflattering[2] movie about Kim Jong Un, the country's leader. Iran has attacked American banks in response to sanctions. Russia has used cyber tactics to meddle in[3] elections in America and Europe.

【6】英国的例子为判断网络权力是否被负责任地使用提供了几个标准。首先是选择什么样的目标。朝鲜黑客曾经攻击过一家美国电影制片厂，因为该制片厂发布了一部关于朝鲜领导人金正恩(Kim Jong Un)的不讨喜的电影。作为对制裁的回应，伊朗攻击了美国银行。俄罗斯利用网络策略干预美国和欧洲的选举。

一、重点词汇

1. Criteria /kraɪˈtɪriə/n. （评判或做决定的）标准，准则，尺度 （criterion 的复数）
2. Unflattering adj. 不吸引人的，不好看的；耿直的；有损形象的；不奉承的；贬损的
3. Meddle in 干涉

二、同义表达

1. 表达“干预、干涉”

（1）Intervene

The UN decided to intervene in the conflict to prevent further violence.（联合国决定干预这场冲突，以防止进一步的暴力事件。）

（2）Interfere

She accused her colleague of interfering with her work.（她指责同事在干扰她的工作。）

（3）Intrude

Intrude into other's room [house; garden; territory]（闯入别人的房间[屋子；花园；领土]）

（4）Intercede

The mediator tried to intercede between the two parties during the negotiation.（调解员试图在谈判期间在两方

之间斡旋。）

（5）Butt in / Barge in (口语用法较多)

I was trying to talk to my friend when he suddenly butted in and interrupted us.（当我正与我的朋友交谈时，他突然插了进来打断了我们的谈话。）

【7】Another is how well attacks are calibrated[1]. Are they precise in their effects and mindful of escalation? Or do they hurl[2] malicious[3] code around wildly? Officials and experts have spent years debating how international law, including the laws of armed conflict, apply to cyberspace. The Tallinn Manual, associated with NATO, is one such guide. Russian intelligence services do not pay much attention to this sort of thing, but responsible cyber commanders need lawyers by their side.	【7】另一个问题是攻击的准确程度。他们的效果是否精确，是否注意到升级?或者他们到处乱扔恶意代码?多年来，官员和专家一直在争论包括武装冲突法在内的国际法如何适用于网络空间。与北约有关的《塔林手册》就是这样一个指南。俄罗斯情报机构不太注意这类事情,但负责任的网络指挥官需要律师在身边。

一、重点词汇

1. Calibrate /ˈkælɪbreɪt/v. 校准，标定（测量仪器等）；准确估量；调整（实验结果），调节
2. Hurl /hɜːrl/ v. 猛扔，猛摔；大声说出（辱骂或斥责等）；呕吐
3. Malicious / məˈlɪʃəs/adj.恶意的；恶毒的

【8】A third test is how well cyber forces protect their arsenals[1].The hacking tools used by states are often powerful and dangerous. They can cause coniderable[2] harm if they become widely available.In 2017 a North Korean cyber-attack spread ransomware[3] worldwide in part by repurposing malicious code that had leaked out of America's National Security Agency (NSA). As more countries embrace offensive cyber operation, the security of their tools will become a bigger issue.	【8】第三个考验是网络部队如何保护他们的军火库。各国使用的黑客工具往往是强大而危险的。如果它们被广泛使用，可能会造成相当大的伤害。2017 年，朝鲜的一次网络攻击在全球范围内传播勒索软件，部分原因是重新利用了从美国国家安全局(NSA)泄露出来的恶意代码。随着越来越多的国家采取进攻性网络行动，其工具的安全性将成为一个更大的问题。

一、重点词汇

1. Arsenals /ˈɑrsənəlz/兵工厂
2. Coniderable 巨大的；可以考虑的
3. Ransomware /ˈrænsəmwer/ 勒索软件

【9】Finally, cyber forces need accountability. Britain’s view of offensive cyber as a means of targeted psychological[1] disruption,rather than an all-purpose weapon of power projection, has much to commend it. But it also pushes cyber power into the murky[2] realm of covert[3] action. Oversight of this is doubly hard: the work is both highly secret and also highly technical. Lawmakers and judges often struggle to grasp the details.	【9】最后，网络部队需要问责制。英国认为进攻性网络是一种有针对性的心理干扰手段，而不是一种万能的力量投送武器，这一点值得称赞。但这也将网络力量推向了秘密行动的阴暗领域。监督这一点是加倍困难的:这项工作既高度机密，又高度技术性。立法者和法官往往难以把握细节。

一、重点词汇

1. Psychological /ˌsaɪkəˈlɑːdʒɪk(ə)l/ adj. 心理的，精神的；心理学的，关于心理学的
2. Covert /ˈkʌvərt/ adj. 隐蔽的，秘密的；（动物可藏身的）矮树丛；覆羽；隐藏处

【10】For the time being, Britain’s approach is to be welcomed. Ten years ago Edward Snowden, a former NSA contractor[1], sent shock waves through the NSA and GCHQ, its British counterpart[2], by publicly revealing their industrial-scale intelligence collection in cyberspace. A decade on, the spooks[3] seem to have learned that responsibility requires scrutiny[4].	【10】就目前而言，英国的做法是受欢迎的。10年前，美国国家安全局(NSA)前承包商雇员爱德华•斯诺登(Edward Snowden)公开披露了NSA和英国政府通信总部(GCHQ)在网络空间收集的工业规模情报，令两家机构震惊不已。十年过去了，间谍们似乎已经明白，责任需要仔细审查。

一、重点词汇

1. Contractor /ˈkɑːntræktər/ n. 承包商，立约人
2. Counterpart /ˈkaʊntərpɑːrt/ n. 对应的人（或事物）；（法律文件的）副本
3. Spooks / spuːks/ n.鬼；间谍；特工 v.吓；惊吓；受惊
4. Scrutiny /ˈskruːtəni/n. 仔细观察，详细审查