护网行动（HW）普及

目录

CONTENT

01

背景介绍

POWERPOINT

护网行动的定义与目标

01

护网行动的定义

护网行动是国家级网络安全实战演练，模拟真实网络攻击与防御场景，提升网络安全防护能力。
旨在通过红蓝对抗，发现并修复网络安全漏洞，增强关键信息基础设施的防护水平。

02

护网行动的目标

短期目标是发现并修复网络安全漏洞，提升关键信息基础设施的防护水平。
中期目标是培养网络安全人才，推动网络安全技术的发展与创新。

03

护网行动的长期目标

长期目标是构建国家网络安全防护体系，提升国家整体网络安全防护能力，维护国家网络空间安全。

护网行动的主要活动

红蓝对抗组织

红队由网络安全专家组成，负责模拟攻击，发现漏洞；蓝队由被测单位组成，负责防御。

红蓝对抗是护网行动的核心，通过模拟真实攻击场景，检验被测单位的网络安全防护能力。

实战攻防演习

实战攻防演习是护网行动的重要环节，模拟真实网络攻击场景，检验被测单位的应急响应能力。

演习过程中，红队利用各种攻击手段对被测单位进行攻击，蓝队则进行防御和应急响应。

漏洞扫描与应急响应

漏洞扫描是护网行动的基础工作，通过扫描被测单位的网络系统，发现存在的漏洞。

应急响应是护网行动的关键环节，当发现漏洞或遭受攻击时，被测单位需迅速采取措施进行修复和应对。

技术交流与经验分享

01

技术交流活动

技术交流是护网行动的重要组成部分，通过举办技术研讨会、培训课程等活动，促进网络安全技术交流。
技术交流活动邀请网络安全专家、学者和企业代表参加，分享最新的网络安全技术和研究成果。

02

经验分享环节

经验分享是护网行动的重要环节，通过分享成功案例和经验教训，提升被测单位的网络安全防护能力。
经验分享环节邀请被测单位代表分享在网络安全防护方面的经验和教训，促进各单位之间的交流和学习。

03

评估与排名机制

评估与排名是护网行动的重要环节，通过评估被测单位的网络安全防护能力，进行排名和表彰。
评估与排名机制包括技术评估、管理评估和应急响应评估等多个方面，全面评估被测单位的网络安全防护能力。

02

HW历程和发展阶段

POWERPOINT

2016年：HW的开始

护网行动的诞生

护网行动于2016年正式诞生，标志着我国网络安全实战演练的开始。

护网行动的诞生是网络安全领域的一次重大创新，为提升我国网络安全防护能力奠定了基础。

《网络安全法》的颁布

2016年，《网络安全法》正式颁布，为护网行动提供了法律依据和保障。

《网络安全法》的颁布是我国网络安全领域的重要里程碑，标志着我国网络安全进入法治化时代。

2017年：规模的扩展

01

大规模实战演练

2017年，护网行动规模进一步扩大，开展大规模实战演练，覆盖多个行业和领域。

大规模实战演练检验了被测单位的网络安全防护能力，发现并修复了大量网络安全漏洞。

02

重点行业信息系统安全检查

2017年，护网行动对重点行业的信息系统进行安全检查，提升重点行业的网络安全防护水平。

重点行业信息系统安全检查包括金融、能源、通信等关键领域，保障国家关键信息基础设施安全。

2019年：HW的普及

各行各业的广泛参与

2019年，护网行动在各行各业广泛开展，参与单位数量大幅增加。

各行各业的广泛参与提升了全社会的网络安全意识，推动了网络安全防护能力的整体提升。

技术创新与人才培养

2019年，护网行动注重技术创新与人才培养，推动网络安全技术的发展和创新。

技术创新与人才培养为护网行动的持续开展提供了有力支持，提升了我国网络安全防护能力。

2020年：特殊历程

01

疫情期间的专项检查

2020年，护网行动在疫情期间开展专项检查，保障疫情防控期间网络安全。

疫情期间的专项检查发现并修复了大量网络安全漏洞，保障了疫情防控期间网络系统的稳定运行。

02

网络安全防护能力的提升

2020年，护网行动通过专项检查和应急响应，提升了被测单位的网络安全防护能力。

疫情期间的专项检查和应急响应为被测单位积累了丰富的网络安全防护经验，提升了其网络安全防护能力。

2021年：数据安全成为重点

《数据安全法》的实施

2021年，《数据安全法》正式实施，数据安全成为护网行动的重点。

《数据安全法》的实施是我国网络安全领域的重要里程碑，标志着我国数据安全进入法治化时代。

数据安全防护措施的加强

2021年，护网行动加强了数据安全防护措施，提升被测单位的数据安全防护能力。

数据安全防护措施的加强保障了被测单位的数据安全，防止数据泄露和滥用。

2022年至今：持续改进和深化

01

常态化演练的推进

2022年至今，护网行动推进常态化演练，提升被测单位的网络安全防护能力。

常态化演练使被测单位在日常工作中保持高度警惕，提升其网络安全防护能力。

02

技术创新与个人信息保护

2022年至今，护网行动注重技术创新与个人信息保护，推动网络安全技术的发展和创新。

技术创新与个人信息保护为护网行动的持续开展提供了有力支持，提升了我国网络安全防护能力。

03

关键信息基础设施的保护

2022年至今，护网行动加强了关键信息基础设施的保护，保障国家关键信息基础设施安全。

关键信息基础设施的保护是护网行动的重要任务，保障国家关键信息基础设施安全是护网行动的重要目标。

03

护网行动的现状分析

POWERPOINT

主要成果

网络安全防护能力的提升

护网行动通过实战演练和应急响应，提升了被测单位的网络安全防护能力。

被测单位在网络安全防护方面的投入不断增加，网络安全防护能力显著提升。

网络安全意识的普及

护网行动通过技术交流和经验分享，普及了网络安全意识。

社会各界对网络安全的重视程度不断提高，网络安全意识深入人心。

法律法规的完善

护网行动推动了网络安全法律法规的完善，为网络安全防护提供了法律依据。

《网络安全法》《数据安全法》等法律法规的颁布实施，标志着我国网络安全进入法治化时代。

关键信息基础设施的保护

护网行动加强了关键信息基础设施的保护，保障国家关键信息基础设施安全。

关键信息基础设施的保护是护网行动的重要任务，保障国家关键信息基础设施安全是护网行动的重要目标。

面临的挑战

新型网络攻击手段

新型网络攻击手段不断涌现，给网络安全防护带来巨大挑战。
被测单位需不断提升网络安全防护能力，应对新型网络攻击手段。

技术瓶颈

网络安全技术存在瓶颈，制约了网络安全防护能力的提升。
被测单位需加强技术研发和创新，突破技术瓶颈，提升网络安全防护能力。

国际合作与竞争

网络安全领域的国际合作与竞争日益激烈，给我国网络安全带来挑战。
我国需加强国际合作，提升国际竞争力，保障国家网络安全。

网络安全人才短缺

网络安全人才短缺，制约了网络安全防护能力的提升。
我国需加强网络安全人才培养，提升网络安全人才数量和质量。

现状与趋势

护网行动的常态化

护网行动将常态化开展，提升被测单位的网络安全防护能力。

常态化演练使被测单位在日常工作中保持高度警惕，提升其网络安全防护能力。

技术升级与国际合作

护网行动将注重技术升级与国际合作，推动网络安全技术的发展和创新。

技术升级与国际合作为护网行动的持续开展提供了有力支持，提升了我国网络安全防护能力。

长期战略规划

护网行动将制定长期战略规划，明确未来发展方向和目标。

长期战略规划为护网行动的持续开展提供了指导，保障国家网络安全。

04

护网行动的影响与启示

POWERPOINT

对国家网络安全的影响

提升国家整体网络安全防护能力

护网行动通过实战演练和应急响应，提升了国家整体网络安全防护能力。国家网络安全防护能力的提升保障了国家关键信息基础设施安全，维护了国家网络空间安全。

增强国家网络空间主权

护网行动增强了国家网络空间主权，提升了我国在网络空间的影响力。国家网络空间主权的增强保障了我国在网络空间的合法权益，维护了国家网络空间安全。

对企业与机构的影响

推动企业网络安全建设

护网行动推动了企业网络安全建设，提升了企业的网络安全防护能力。

企业网络安全防护能力的提升保障了企业的正常运营，降低了网络安全风险。

促进企业供应链安全

护网行动促进了企业供应链安全，保障了企业供应链的稳定运行。

企业供应链安全的保障降低了企业的运营成本，提升了企业的竞争力。

对个人用户的影响

01

促进个人隐私保护

护网行动促进了个人隐私保护，提升了个人用户的网络安全意识。

个人隐私保护的提升保障了个人用户的合法权益，维护了个人用户的网络安全。

02

增强个人网络安全技能

护网行动增强了个人用户的网络安全技能，提升了个人用户的网络安全防护能力。

个人网络安全技能的提升保障了个人用户的网络安全，降低了网络安全风险。

对全球网络安全的启示

提升中国在全球网络安全领域的影响力

护网行动提升了中国在全球网络安全领域的影响力，展示了我国网络安全防护能力。

中国在全球网络安全领域的影响力提升为全球网络安全治理提供了中国方案，贡献了中国智慧。

01

应对全球网络威胁

护网行动为应对全球网络威胁提供了经验借鉴，提升了全球网络安全防护能力。

全球网络安全防护能力的提升保障了全球网络空间的稳定运行，维护了全球网络安全。

02

05

护网行动的未来展望

POWERPOINT

技术发展趋势

人工智能的应用

人工智能将在网络安全领域广泛应用，提升网络安全防护能力。

人工智能技术可实现自动化威胁检测和响应，提升网络安全防护效率。

01

大数据分析的应用

大数据分析将在网络安全领域广泛应用，提升网络安全防护能力。

大数据分析技术可实现威胁情报共享和态势感知，提升网络安全防护能力。

02

量子计算的影响

量子计算将对网络安全产生深远影响，推动网络安全技术的变革。

量子计算技术可实现高效加密和解密，提升网络安全防护能力。

03

政策与法规的完善

法律法规的细化

网络安全法律法规将不断细化，为网络安全防护提供更完善的法律依据。法律法规的细化将明确网络安全责任和义务，保障网络安全。

国际法中的定位与发展

网络安全在国际法中的定位将不断明确，推动网络安全国际合作。

国际法中的定位与发展将为网络安全国际合作提供法律依据，保障网络安全。

国际合作与竞争

国际合作的新机遇

网络安全领域的国际合作将面临新机遇，推动网络安全技术的发展和创新。

国际合作的新机遇将促进网络安全技术交流和共享，提升全球网络安全防护能力。

国际竞争的新挑战

网络安全领域的国际竞争将面临新挑战，制约我国网络安全发展。

国际竞争的新挑战将促使我国加强网络安全技术研发和创新，提升国际竞争力。

长期战略

常态化与可持续发展

护网行动将实现常态化与可持续发展，提升我国网络安全防护能力。

常态化与可持续发展将保障我国网络安全防护能力的不断提升，维护国家网络空间安全。

在国家安全战略中的定位

护网行动将在国家安全战略中占据重要地位，保障国家关键信息基础设施安全。

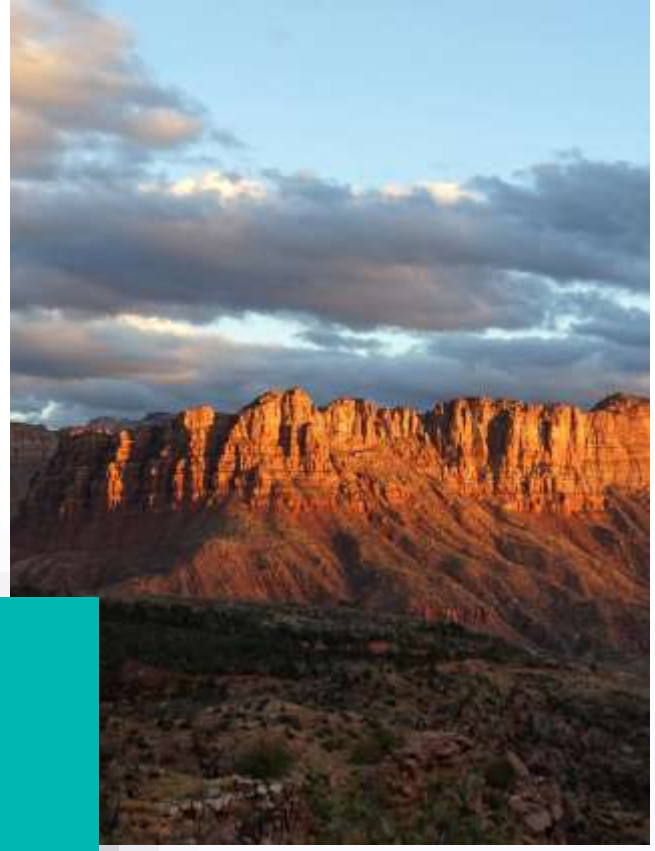
在国家安全战略中的定位将明确护网行动的重要性和必要性，保障国家网络安全。

06

总结与问答环节

POWERPOINT

总结护网行动的意义与价值



01.

护网行动是我国网络安全领域的重要实践，提升了我国网络安全防护能力。

02.

护网行动推动了网络安全技术的发展和创新，培养了大量网络安全人才。

谢谢大家