网络空间安全攻防博弈与社会逻辑

李敬 Jing Li

May. 27, 2021

辛丑孟夏十六

Huairou, Beijing

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

分享知识（洗脑）
自我提升（征友）
利益互换（加分）

$ whoami

- 我叫李敬（@lix3on）
- 扬州大学2019届软件工程(NIIT)本科毕业生
- 现为2020级中国科学院信息工程研究所 / 中国科学院大学网络空间安全学院，硕博连读研究生，师从侯锐教授
- 所在科室：信息安全国家重点实验室
- 研究方向：智能芯片安全、体系结构安全、

存内计算安全

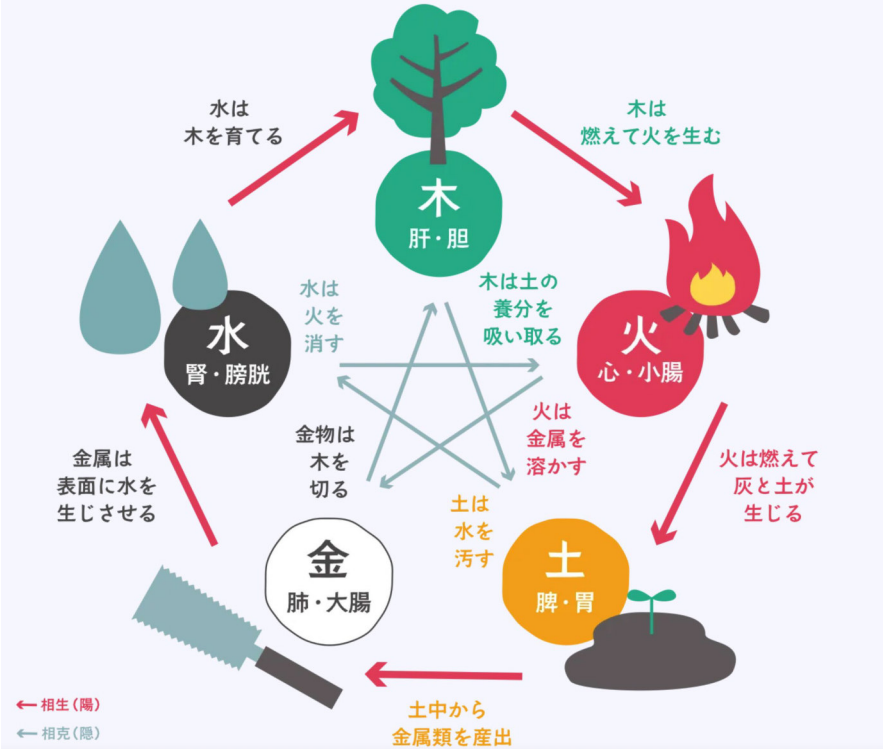
- 社会职任：中国计算机学会宣传员、华为HSD大使
- lixeon.com
- lixeon.lij@gmail.com

Contents

Source: https://www.infoq.cn/article/qhcjgLjhf1XB49SdpPod

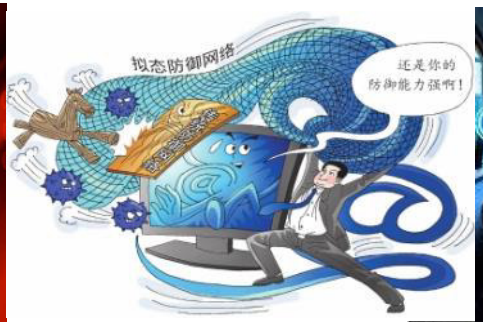
谁不想成双成对呢？

网络攻防
相生相克


水は
木を育てる
木は
燃えて火を生む
木
肝・胆
水
腎・膀胱
火
心・小腸
水は
火を
消す
木は土の
養分を
吸い取る
火は
金属を
溶かす
金物は
木を
切る
金属は
表面に水を
生じさせる
火は燃えて
灰と土が
生じる
土は
水を
汚す
金
肺・大腸
土
脾・胃
土中から
金属類を産出
←相生(陽)
←相克(隠)

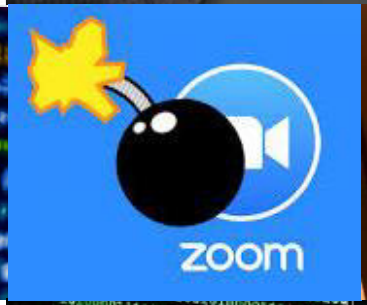
网络安全事件频出

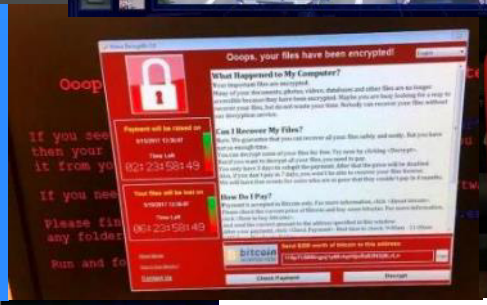

vunerabilty
SSLv3
warning
HACK

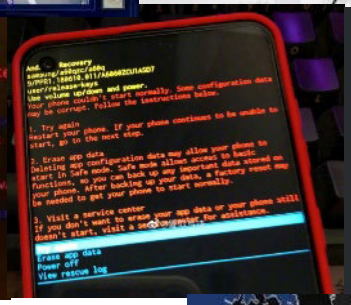

拟态防御网络
还是你的防御能力强啊！


SENSEVIDEO

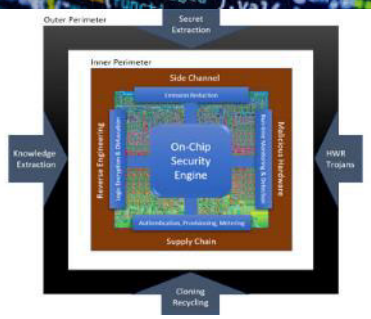

Web scraping


zoom


Ooops, your files have been encrypted!




ctf_


Outer Perimeter
Secret Extraction
Inner Perimeter
Side Channel
On-Chip Security Engine
Knowledge Extraction
HWR Trojans
Supply Chain
Cloning Recycling


Stuxnet
infected

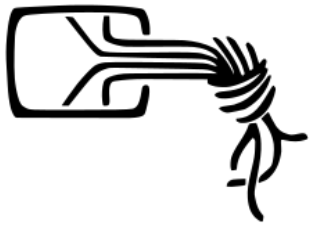

DDoS

网络安全生态圈


DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

公安部第三研究所
The Third Research Institute Of Ministry Of Public Security





中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

HERJAVEC GROUP



CYBERARK


网络空间安全成为一级学科

- 2015年6月，为实施国家安全战略，加快网络空间安全高层次人才培养，国务院学位委员会决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。

  - 这段“长征路”走了十余年；
  - 翻越了“没有信息安全本科专业”的“雪山”；
  - 爬过了“没有国家科技专项支持”的“草地”；
  - 摆脱了昔日各宗主学科出于善意或担心的围追堵截；
  - 克服了“张国焘”们的分裂主义和“王明”们的投降主义；
  - 战胜了各种“左倾”和“右倾”机会主义的干扰
  - 终于没有让“本不该由学者担负的舆论之山”压垮，并因感动“上帝”，而成功到达了“延安”

http://blog.sciencenet.cn/blog-453322-951389.html

网络空间安全是不是科学

- 网络空间安全没有基础理论体系？
  - 密码学是数学？
  - 国内外安全专家只不过是灵巧的“高级工匠”？
  - 实际上只是计算机等理论身上的区区“寄生虫”
  - 整个学科有魂无魄？

- 网络攻防是小孩子打打杀杀的游戏？
  - 科学与工程如何区别
  - 研究如何“对抗”难道不是科学？
  - 与智慧生命体相关的博弈值得研究

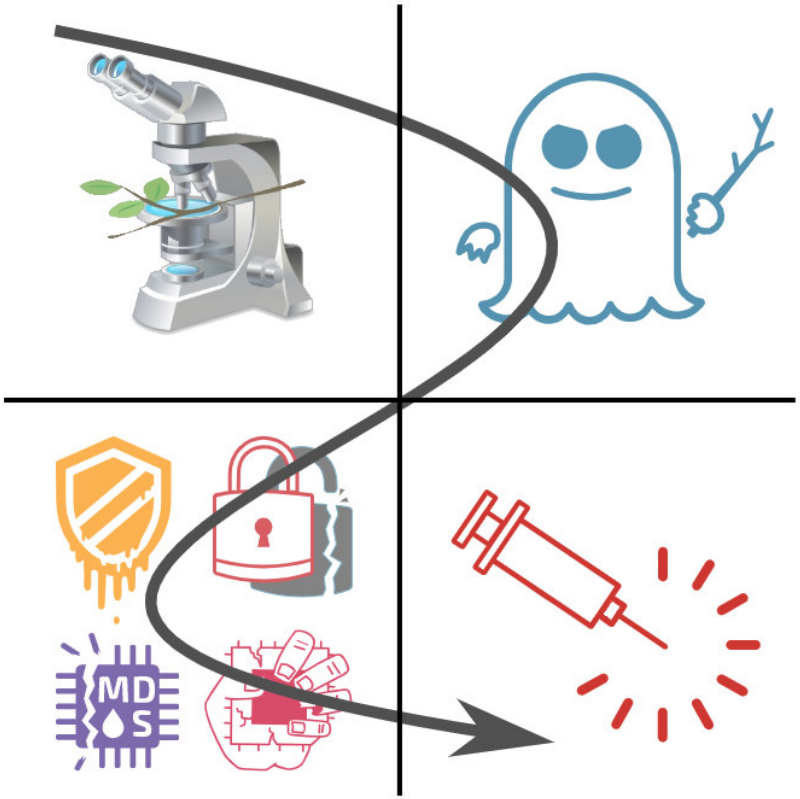
http://blog.sciencenet.cn/blog-453322-951389.html

拉高视角，从宏观看网络攻防

- 从微观来看，网络安全技术研究指的是针对某项或某几项指标的完善，是具体的技术研究。

- 网络安全中攻防对抗的**本质**可以抽象为攻防双方的**策略依存性**，而这种策略依存性正是**博弈论**的基本特征，因而可以考虑应用博弈论来解决网络安全攻防对抗的问题。

攻击的变化趋势



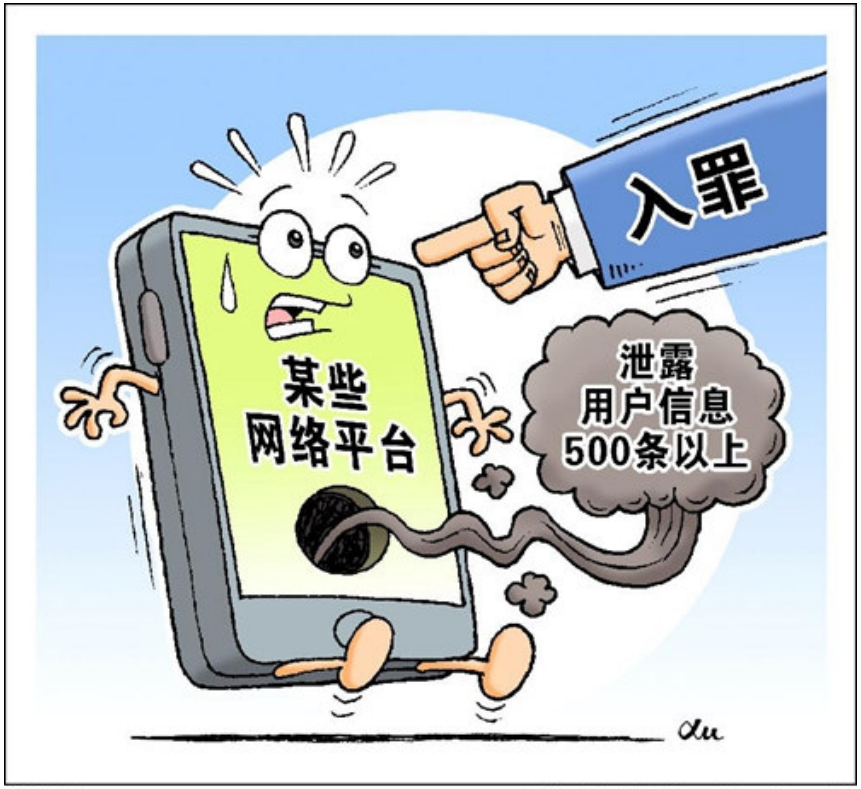
快速、专业、隐蔽、持久

https://www.slideshare.net/paulgoogle/20150326-02

博弈冲突
打破次元

隐私泄露导致各种问题

成批泄露　　新华社发　徐骏　作



新规　　新华社发　徐骏　作

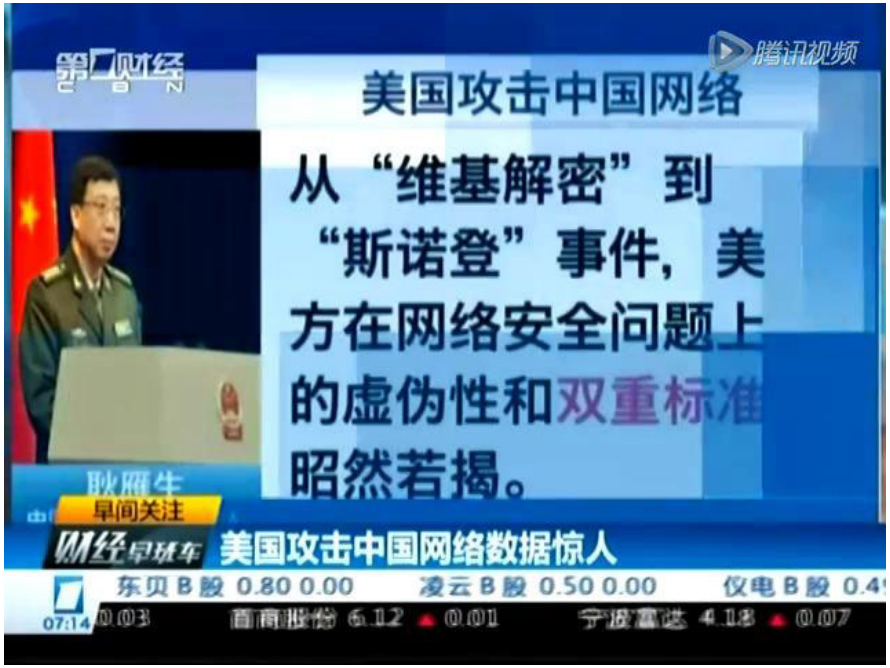

“大安全”时代网络安全的内涵与外延
网络安全
国家安全
关键基础设施安全
国防安全
城市安全
会安全
人身安全
CLINTON
Power Outage

万物互联意味着万物都有安全问题

BadPower并不像传统传统网络安全问题那样会导致数据隐私泄露，但可以实现**通过数字空间破坏物理世界**。

https://xlab.tencent.com/cn/2020/07/16/badpower/

人间真实
不得不防


第一财经
腾讯视频
美国攻击中国网络
从“维基解密”到
“斯诺登”事件，美
方在网络安全问题上
的虚伪性和双重标准
昭然若揭。
早间关注
财经早班车
美国攻击中国网络数据惊人
东贝B股 0.80 0.00
凌云B股 0.50 0.00
07:14

网络安全是一场没有硝烟的战争

现实冲突与网络空间冲突交织

赛博战就像核辐射，它不会让你流血，但它会摧毁一切

https://www.pishu.cn/pssjkxw/474178.shtml

美国对中国极限施压的现状

地缘政治施压

美国对华地缘政治施压		中方应对之策	
2017.3.6	以应对朝鲜核导威胁为由，韩国接受美国的协助下部署萨德反导系统	2017.2-2017.3	强烈反对，对在华韩企实施打压，不建议中国人赴韩旅游。未能阻止
2017.11.22	和解，达成“三不一限”承诺。1.不考虑追加萨德系统；2.不加入美国反导系统；3.不发展韩美日三方军事同盟；4.为了不损害中国战略安全利益而限制使用萨德。		
2013.1-2016.7	菲律宾就中菲南海争议提起国际仲裁，判“胜诉”且否定“九段线”	2016.7.13	菲南海仲裁庭作出无效裁决，中方不接受不承认
2016年	美国数次在南海“航行自由行动”	2016年底-2017年初	在南海建设三大军事岛屿基地
2019年	美国在南海针对中国的“航行自由行动”公开报道可查的就有八次之多，数十次出动航母及轰炸机、侦察机穿越南海，并针对性在黄岩岛等中国岛礁附近实施威慑和侦察		
2019.6	越南在南海万安滩增设钻井平台；对峙时期，得到美国口头支持	2019.7	中国派遣海洋地质8号勘探船和海警船在南沙群岛日积礁海域进行活动
2019年	2019年6月，美国防部发布《亚太战略报告》。美军在南海及周边地区的联合演习对象涉及到东盟各国以及日本、澳大利亚、新西兰、法国、印度、加拿大等多个域外国家，重点突出海上执法、海域态势感知及网络空间作战等方面。军事演练至少53次。		

美国对中国极限施压状态总结

美国对中国的极限施压是前所未有的

- 美国已经通过贸易战、科技战、地缘政治施压等手段对中国展开施压，这是从中美建交以来从未有的
- 2017年，特朗普政府《国家安全战略报告》公开把中国视为头号战略竞争对手

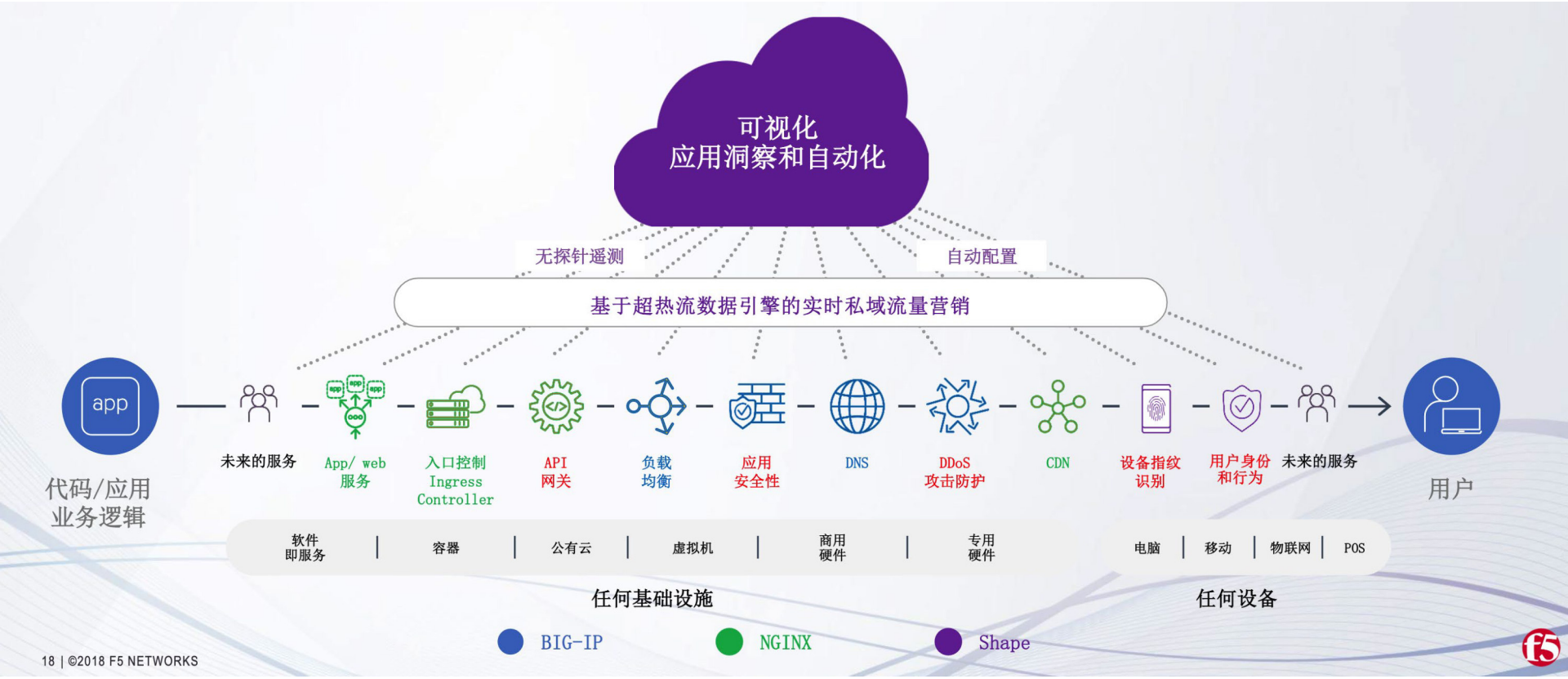
极限施压的空间还比较大

- 目前金融战、贸易战还未达到极限程度，这是由于中美已经形成“你中有我、我中有你”利益交融格局，但美国正在尝试脱钩，并且号召盟友，希望在部分行业中把中国排除在全球经济体之外
- 对中国的地缘政治施压还处于包围准备状态，未展开实际施压活动，比如阻断马六甲海峡等

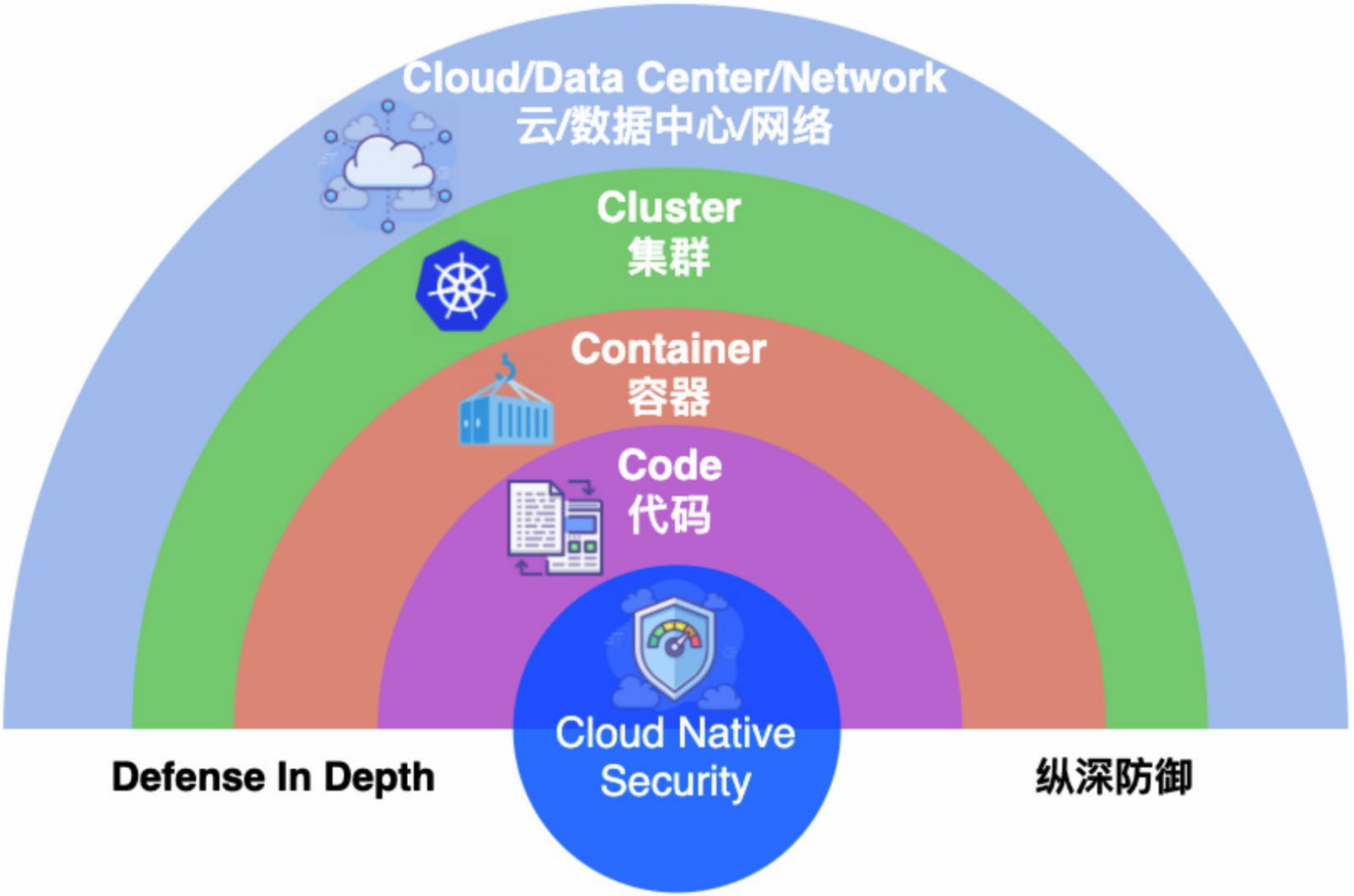
极限施压下的底线在哪？

- 2020年1月，中美签署第一阶段贸易协议内容并不平等，但中国做出了经济上的让步；关于地缘政治，底线一直很明确，比如台湾、马六甲海峡等；那网络空间的底线是否需要底线，若需要底线是什么？

防御应对措施——控制流完整性



防御应对措施——纵深防御


Cloud/Data Center/Network
云/数据中心/网络
Cluster
集群
Container
容器
Code
代码
Cloud Native
Security
Defense In Depth
纵深防御

以前防御措施较为被动

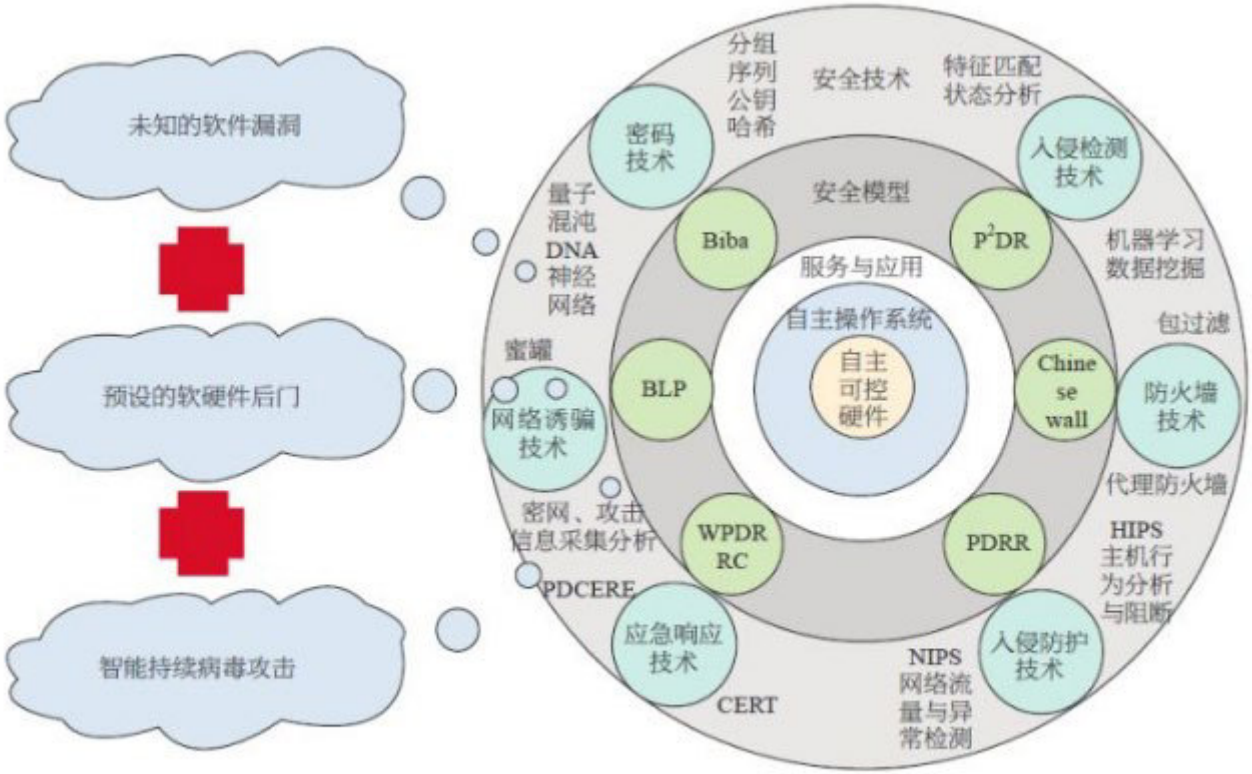


图1 现行的被动安全防御体系

防御应对措施——改变游戏规则

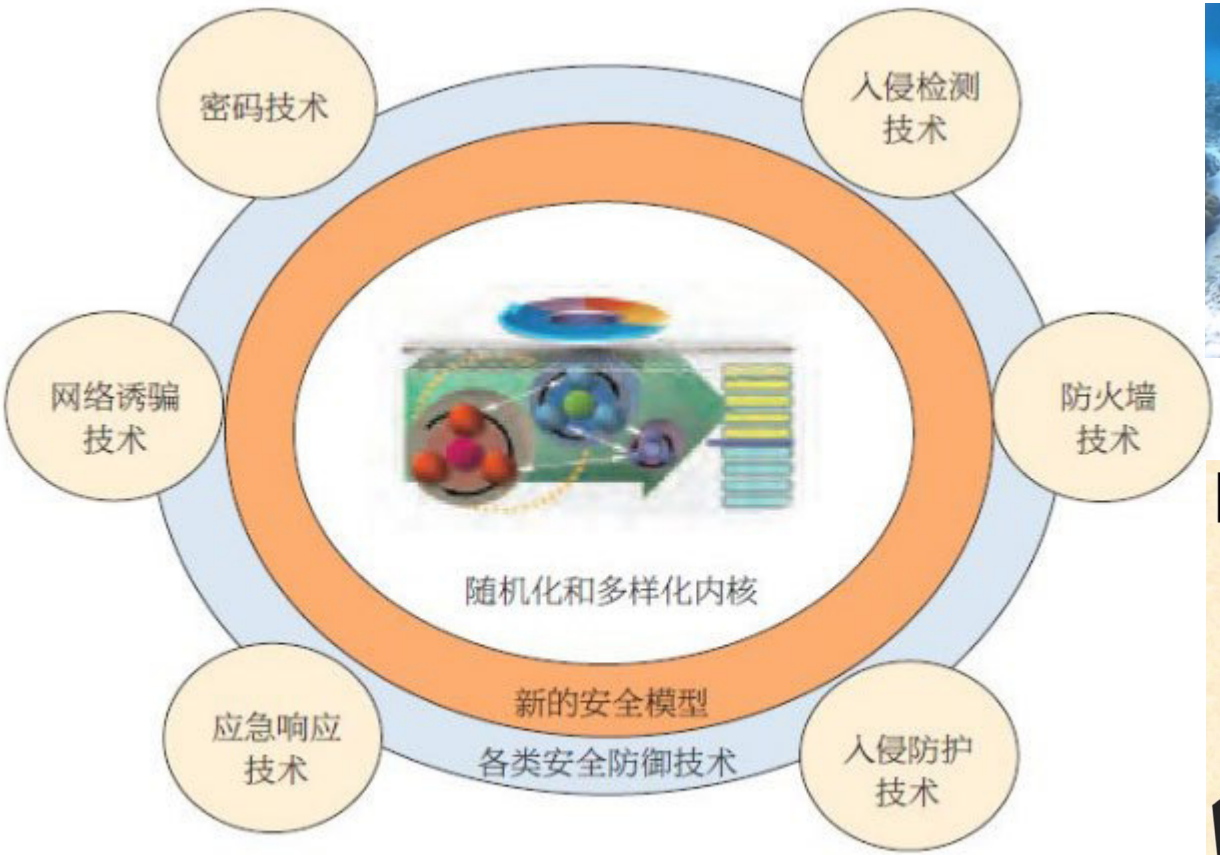
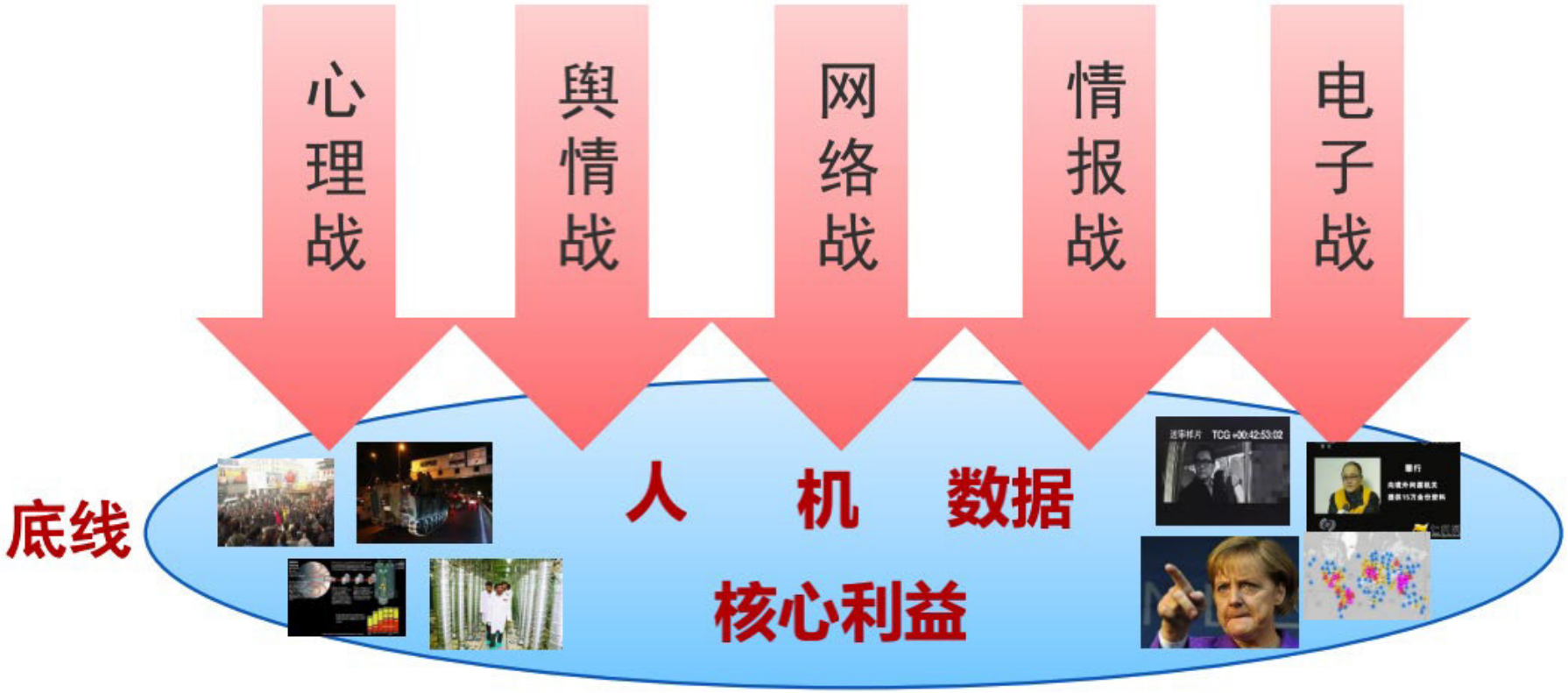


图2 拟态安全主动防御体系基础架构

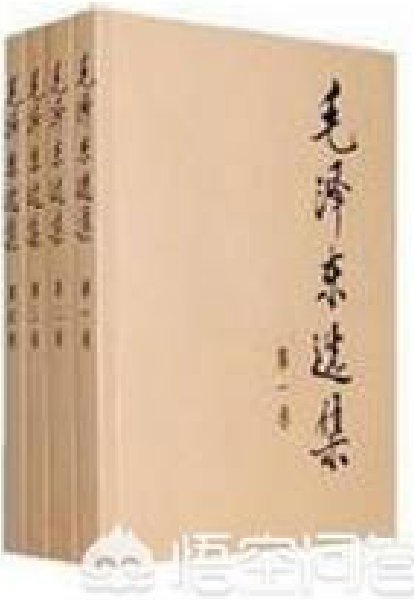
极限施压情况下的网络空间安全底线思维



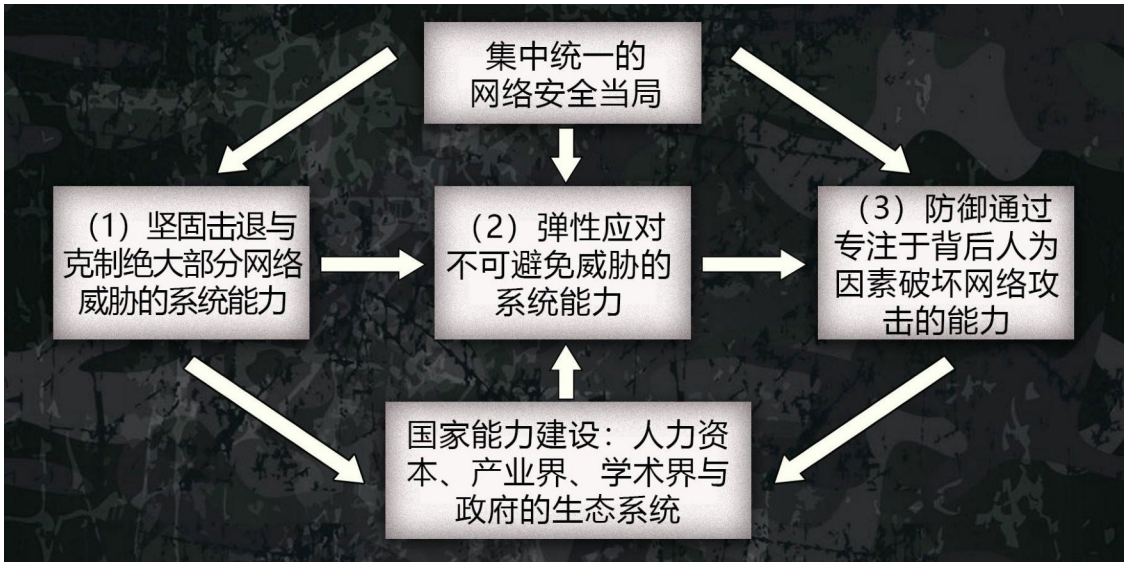
未来战争
破局之道

用魔法打败魔法
人机合一的信息安全
是构建未来大同世界的基石

武器是战争的重要因素，但不是决定性的因素，决定人不是物的因素是物。



以色列国家网络战略的三个层次



层次1：军事主导攻击性防御

国防军在以色列网络力量中有着绝对的主导权，“攻击型防御”战略，不可解的地缘政治冲突，让以色列网络战略极端地追求安全。

层次2：军政弹性防御体系

张弛有度，军政协同，对网络安全威胁进行不同层级的响应。

层次3：专注人为因素

网络安全，人是关键。以色列网络力量强大的根源，就是8200等部队不断输出技术型人才，反过来，就是以色列网络安全战略的第三个层次，即人的防御。 以色列通过严密的措施，防御以人本身为漏洞，进行的破坏性网络攻击。

---

https://mp.weixin.qq.com/s/LvLbzaTv8kyNOc65qnNwTQ

政府参与网络空间安全的必要性 (以色列2010年大规模开始)

「以色列与中东概览」、「以色列的创新和创业生态圈」、「从安全稜镜看以色列生态圈：人力资本、产业发展和国家基础建设」、「未来的网络安全：物联网、智慧城市、人工智能」、「国家网络安全：从策略到实践」、「国家网络安全生态圈」、「影响运营、线上社群媒体和资讯战」、「网络立法与欧盟一般资料保护法规」、「网络教育：培育网络专业人才」、「挑战：培育网络研发的人力资本」、「资助网络产业：经验教训与未来趋势」、「物联网安全与防护：风险和机会-私营部门的观点」、「网络解决方案的演进-进进退退」、「网络安全和国家安全」、「指挥你的思维迈向成功」，涵盖了以色列的文化及历史演进，导引该国走向高科技建国及推展高科技经济为国本的政策方向与处理原则，也论述了未来的走向。

- **National Security Concerns，国家安全的顾虑**
- **Systemic Impacts，系统化的影响**
- **Market Failures，市场的失败**
- **Beyond the Organization，超越单一组织**

https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10703303/001

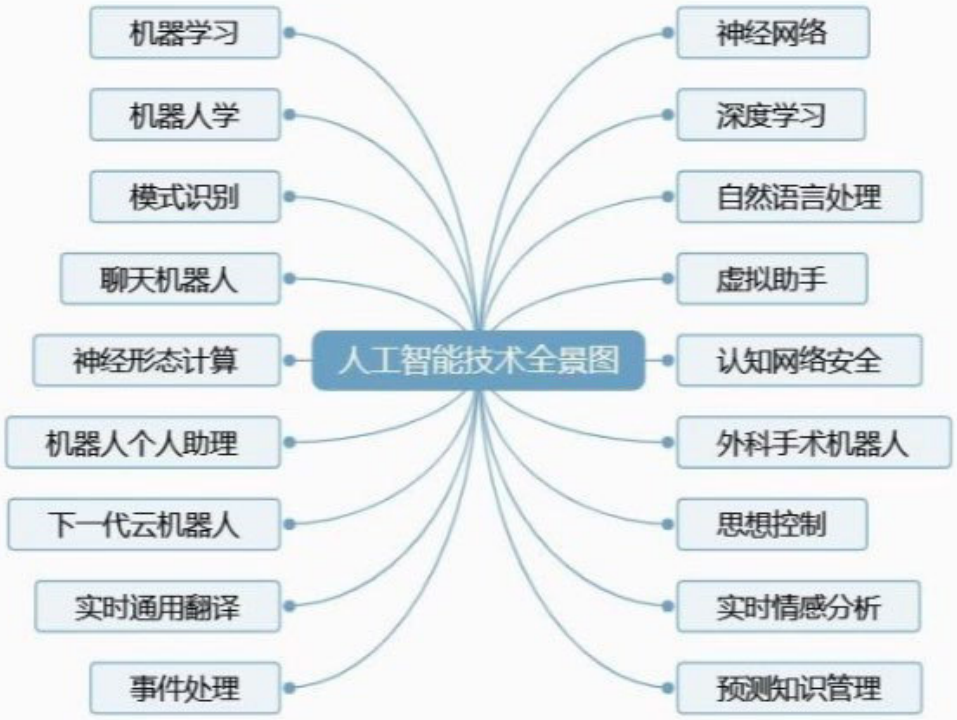
网络安全与国家主权

2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上发表讲话

坚持底线思维
把维护国家安全的战略主动权
牢牢掌握在自己手中

——习近平主持召开2017年2月17日国家安全工作座谈会

人工智能若掌控全局，人类何去何从



网络安全的未来是否掌握在AI手中
新一轮攻防博弈
人类是否有出手的机会

https://www.infoq.cn/article/qhcjgLjhf1XB49SdpPod

I. 网络攻防 相生相克

II. 博弈冲突 打破次元

III. 人间真实 不得不防

IV. 未来战争 破局之道

欢迎批评指正

THANKS