看不见的战争——网络战

做个好人 @IDF实验室

关于我们

- IDF实验室（www.idf.cn），全称**互联网情报威慑防御实验室**（INTELLIGENCE DEFENSE FRIENDS LABORATORY），是一个由信息安全从业人员、专家及信息安全爱好者组成的第三方独立机构。

- **成立于……**

  2005年-2006年

- **致力于……**

  普及信息安全知识

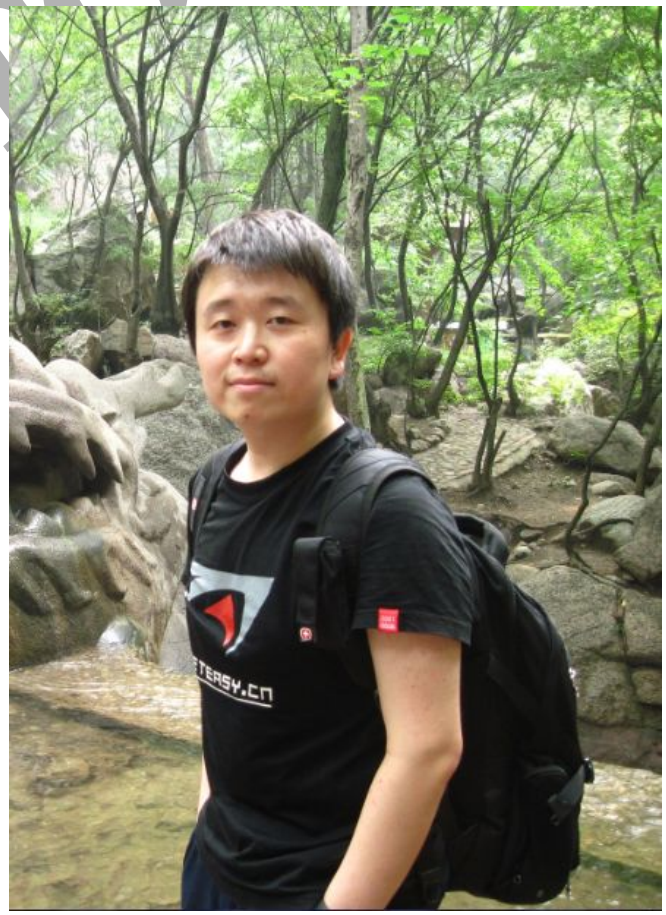
  致力安全人才培养

  促进技术文化交流

关于本人

裴伟伟（做个好人）

项目经理&研发工程师&安全工程师



- 中地数码：研发工程师
- 神州数码：数据库开发及维护工程师
- 益云公益：项目经理
- IDF实验室：项目经理&研发工程师&安全工程师

- 博客：http://www.repoog.com
- 微博：@repoog
- 邮箱：repoog#idf.cn

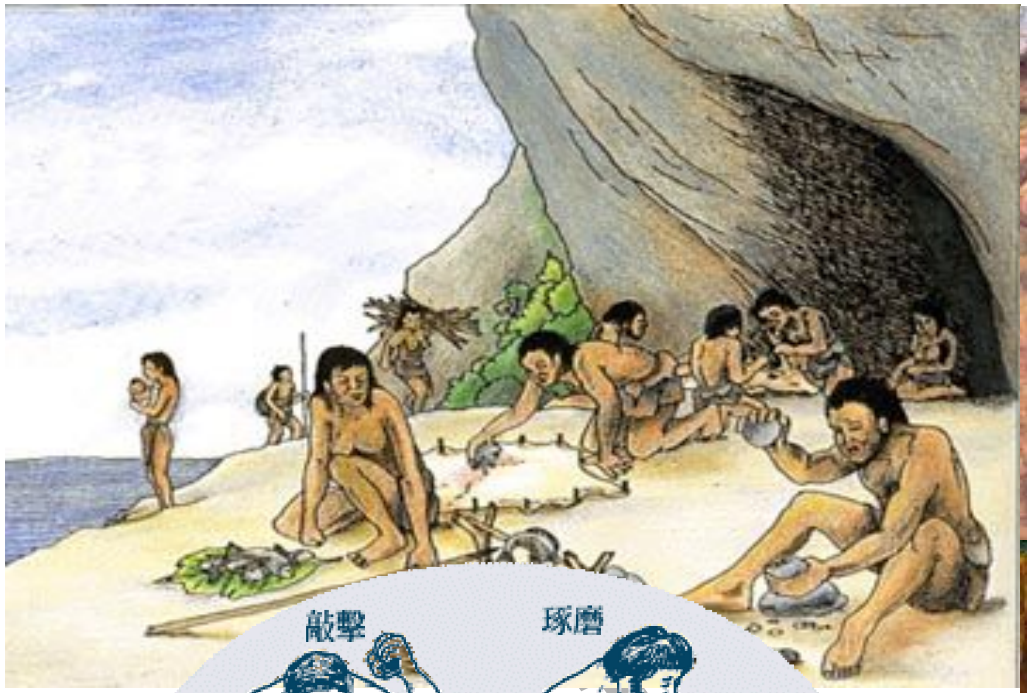
什么是战争

A country does not have permanent friends, only permanent interests.

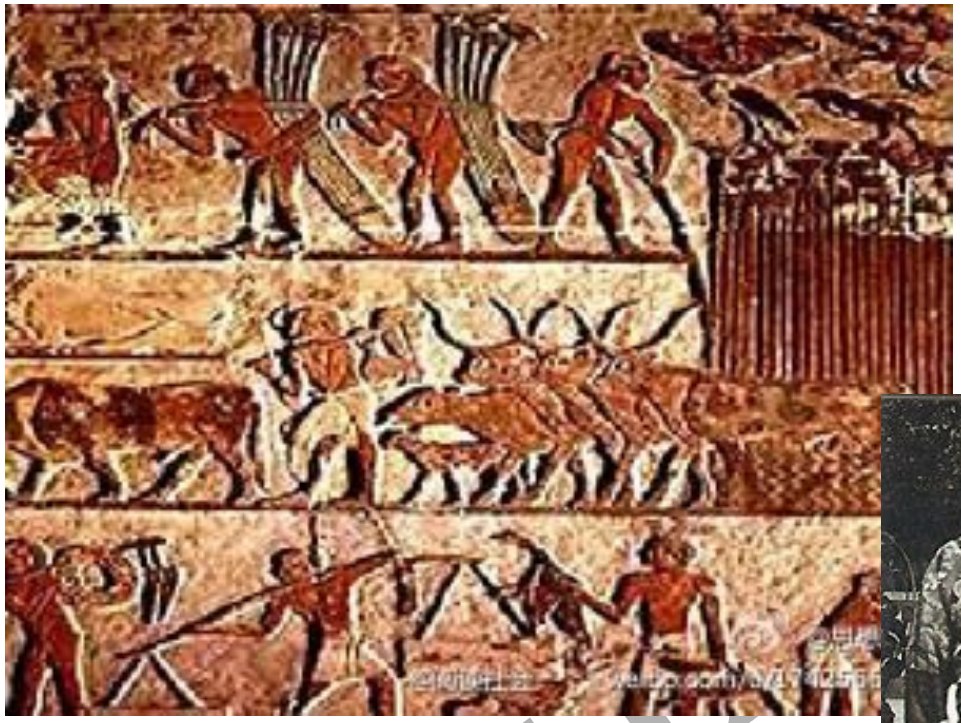
国家没有永远的朋友，只有永远的利益。

——十九世纪 英国首相帕麦斯顿

远古争战——战争起源



奴隶社会&封建社会——冷兵器时代



财富积累

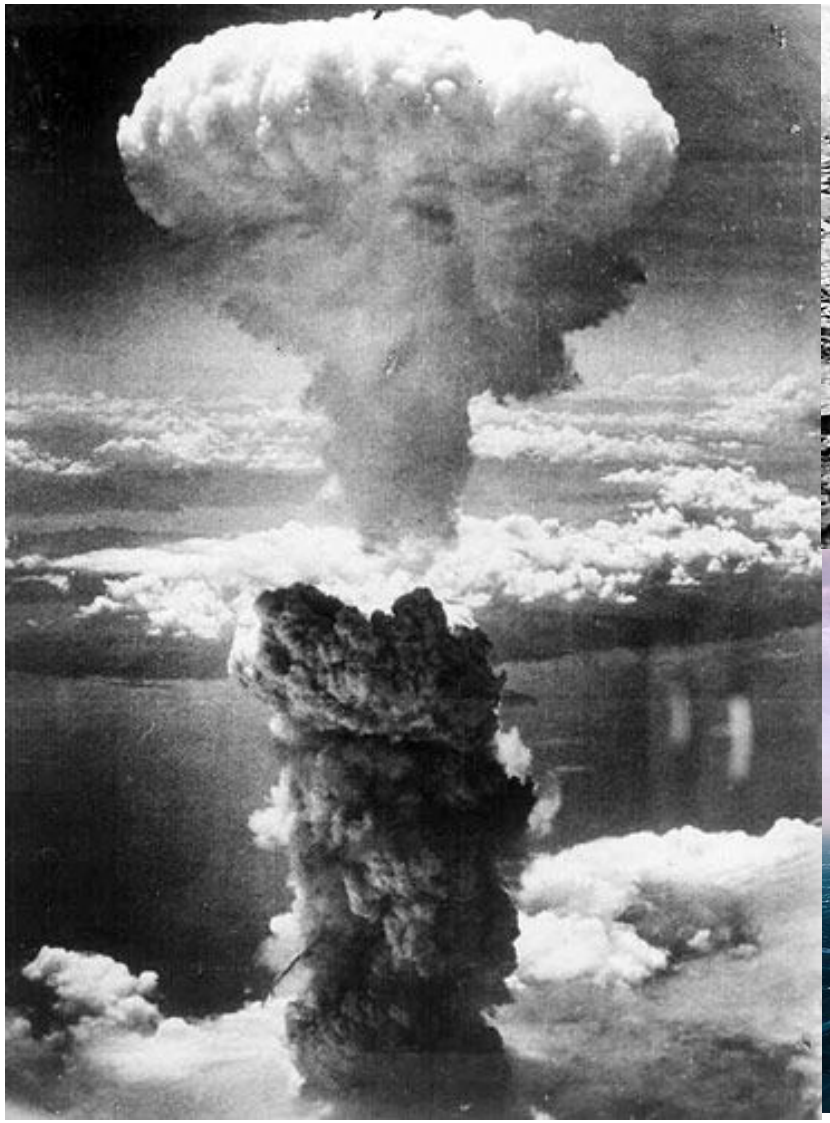
政治手段

冷兵器战争特点

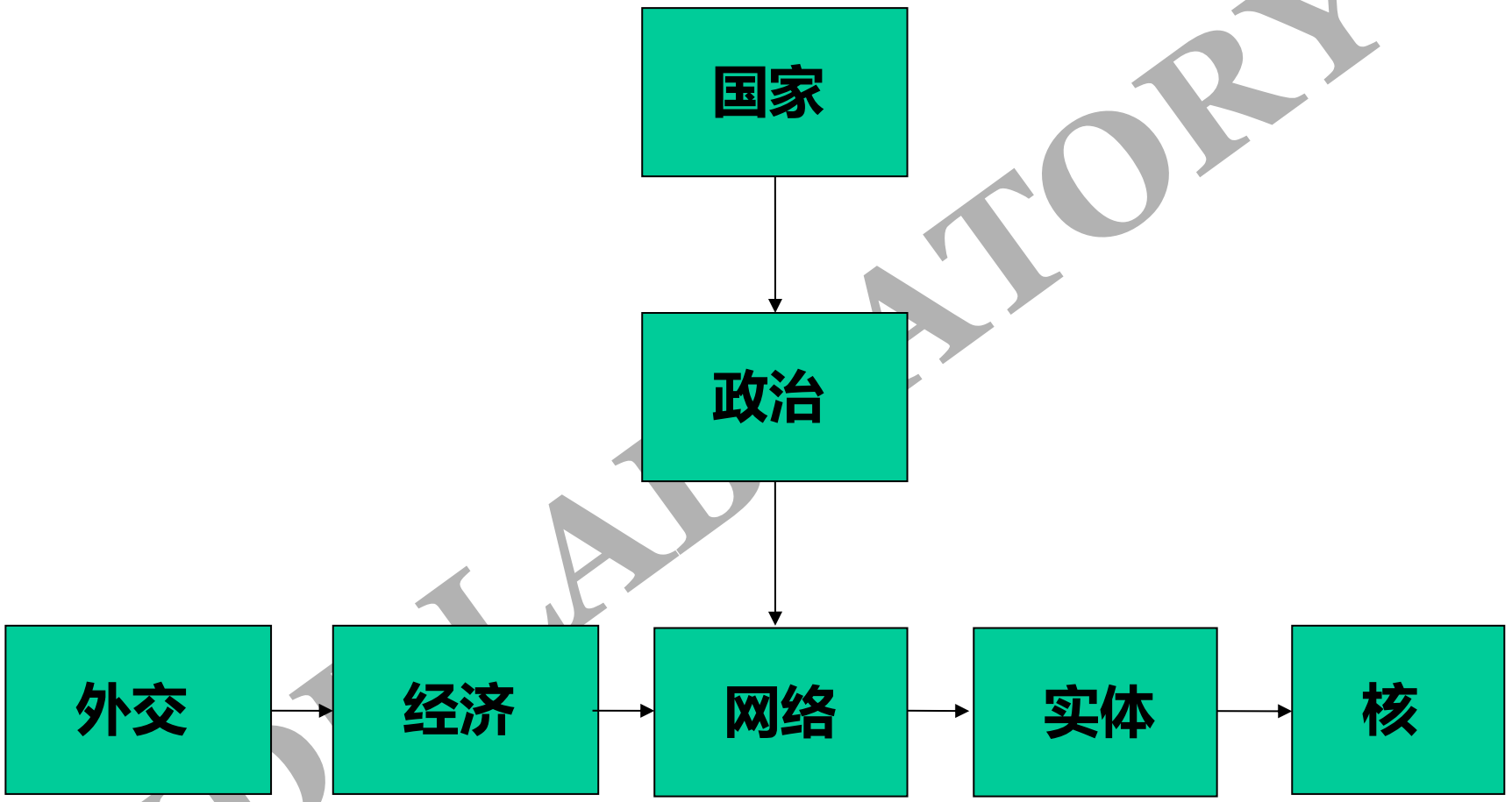
工业革命之后——热兵器时代

热兵器战争特点

冷战之惧——核战争



看不见的战争——网络战



攻击（威胁）手段二分化

外部威胁

内部威胁

网络攻击形式

渗透/腐蚀：难以察觉的攻击

破坏：“显而易见”的攻击

网络威慑之重要

“谁干的……”

“没看到哇……”

溯源之难

国家行为？

组织行为？

个人行为？

哪个国家？哪个组织？哪个人？

什么国籍？所在地哪？幕后主使？

反击之难

能否进行多次反击？

攻击方没有可攻击资产？

如何阻止事态升级？

如果有第三方帮忙怎么办？

二次反击的容忍度是什么？

如何通过反击传递攻击缘由？

攻击目的与范围之难

攻击方无心之举？攻击方反咬一口？操作不当？

指挥与控制问题……

攻击后的反应策略

- 公布受攻击事件？——一家之言，谁信？
- 推迟公布受攻击事件？——另有其人，谁知？
- 进行网络报复？——意欲何为，谁明？

网络战之战略、战术

战略：

对目标国进行挑衅；

与目标国升级为实体战争；

对目标国进行施压；

战术：

辅助实体战争；

打击民间资产；

网络战的防御

防御目标

体系结构

政策

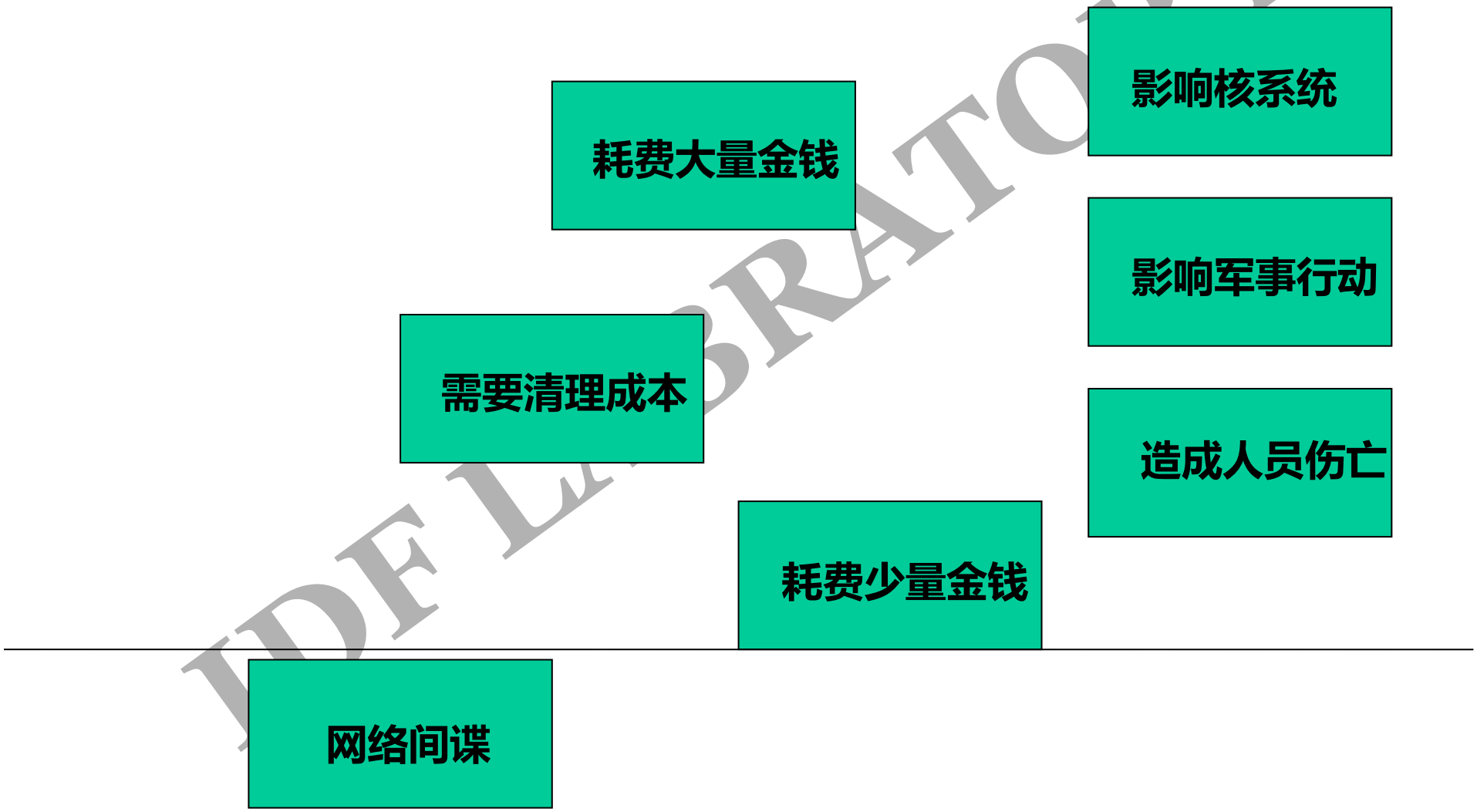
策略

操作

硬件

……

网络战“杀伤”等级



网络战案例之一

1982年1月，里根总统亲自批准了当时的中央情报局局长威廉·凯西递交的一份绝密计划。计划要求当局同意，通过向前苏联转让带瑕疵的技术破坏其经济，从而让其无法成为美国的对手。当时，美国正设法阻止西欧进口前苏联的天然气。同时，也有迹象显示，苏联人正在设法窃取种类繁多的西方技术。就在这个节骨眼上，一位克格勃的内幕人士披露了前苏联的一份特殊的购物单，于是，中情局就将计就计将一份带缺陷的软件在苏联人毫无察觉的情况下塞给了苏联人。

——《在深渊：一个内幕人的冷战历史》 托马斯·里德

网络战案例之二

背景 [编辑]

爱沙尼亚共和国是东北欧波罗的海三国之一。19世纪被俄罗斯吞并，俄国十月革命后独立，二次大战时再被斯大林吞并，直至1991年苏联解体后，再次独立。

2007年4月，爱沙尼亚决定将首都塔林的苏俄时代军事纪念像移到军人坟场，该建议最先由首相安德鲁斯·安西普提出，原意是利用爱国情绪，在三月国会大选中争取中间偏右的选民，支持拥护自由市场的改革党。但人口只有130万人的爱沙尼亚，约有30万俄人聚居，当苏俄时代的纪念像在4月底被封时，数以百计的人群上街示威，攻击剧院及艺术学院，大叫“俄罗斯！俄罗斯！”、“苏联万岁”等口号，多间商铺被掠夺，逾千人被捕，一人被斩死。[3]

事后爱沙尼亚监察间谍的人员指，俄国领事馆人员在骚乱前，曾与示威领袖会面；同一时间，俄国政府组织的青年团亦包围爱沙尼亚在莫斯科的大使馆，扬言要堵毁大使馆。当爱沙尼亚抗议后，俄罗斯外交部指责爱沙尼亚一手促成紧张局面；5月1日，俄国以“铁路维修”为由，停止向爱沙尼亚出口石油和煤；俄国媒体报道事件时，形容一群“反法西斯”的学童正阻止爱沙尼亚摧毁纪念铜像，遭受到“野蛮的警察虐待”。[4][5]

网络战 [编辑]

2007年4月27日，爱沙尼亚多个网站开始受到攻击。大量网站被迫关闭，一些网站的首页被换上俄国宣传口号及伪造的道歉声明，该国总统的网站同样倒下。

在连串攻击浪潮中，最先报纸和电视台受袭，之后到学校，最后蔓燃至银行。近年爱沙尼亚正推动电子政府，高度倚赖电子网络支持日常运作，攻击爆发后，在当地引起巨大震动。一些网站原本每月只有1000人浏览，但遇袭期间，每秒已有2000人登入。

攻击的第一次高峰出现在5月3日，当天莫斯科爆发最激烈的示威抗议。另一次高峰是5月8日和9日，欧洲各国纪念战胜纳粹德国，攻击同步升级，最少六个政府网站被迫停站，当中包括外交和司法部。最后一次攻击高峰是15日，该国最大的几家银行被迫暂停国外连线。[6]

三轮网络攻击的焦点目标包括：爱沙尼亚总统和议会网站、政府各部门、各政党、六大新闻机构中的三家、最大两家银行以及通讯公司。[7]

该国官员指他们已变成首个网络战争的受害国。[8]爱沙尼亚两大报之一的《邮政时报》的编辑直指：“毫无疑问，网攻源自俄罗斯，这是一次政治攻击。”该报网站受到攻击后，已经关闭了国外用户通道有一周时间。

包括爱沙尼亚首相在内均指，虽然今次攻击看似来自世界各地的电脑，但国防官员追查攻击时，发现原始攻击直接来自俄罗斯，部分域名还以俄罗斯总统普京的名义登记[9]，但俄罗斯多次否认与事件有关，并抨击爱沙尼亚虚构指控[10]。俄罗斯驻爱沙尼亚大使弗拉基米尔·奇若夫向《卫报》指：“说攻击来自俄罗斯或俄政府是严重指控，你必须拿出证据来。网络空间无处不在。我个人不支持这种行为，但人们应该先搞清楚袭击者来自哪里，为什么发动攻击。”[11]

北约指今日爱沙尼亚面对的情况，可能是其他人明日的遭遇，对事件表示关切。国际先驱论坛报亦指，两名北约资深专家已联同美国成员，赶到爱沙尼亚了解事故。来自北约成员国和北约的“反网络恐怖”组织NCSA的专家在美国西雅图举行了专门会议，相讨对策。

事发期间，网络上流传一批文件，教人如何攻击爱沙尼亚网站，文章亦呼吁网民推动这次全球首见的网络战争。

网络战案例三

请参考：

《俄罗斯：兵马未动 黑客先行》

http://article.yeeyan.org/view/translation/12408

《采访》引发的“血案”


전쟁은
시작될것이다

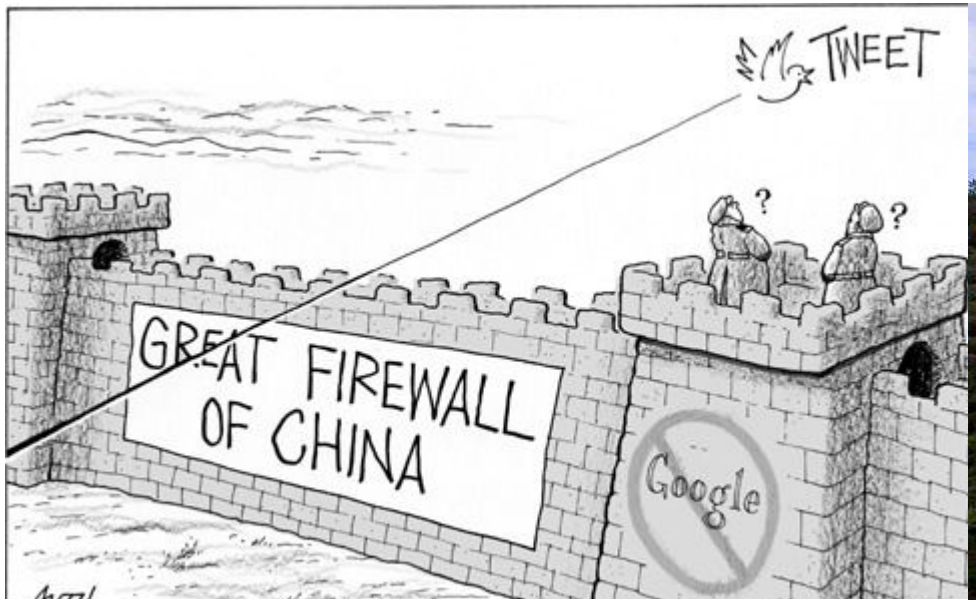

SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE INTERVIEW

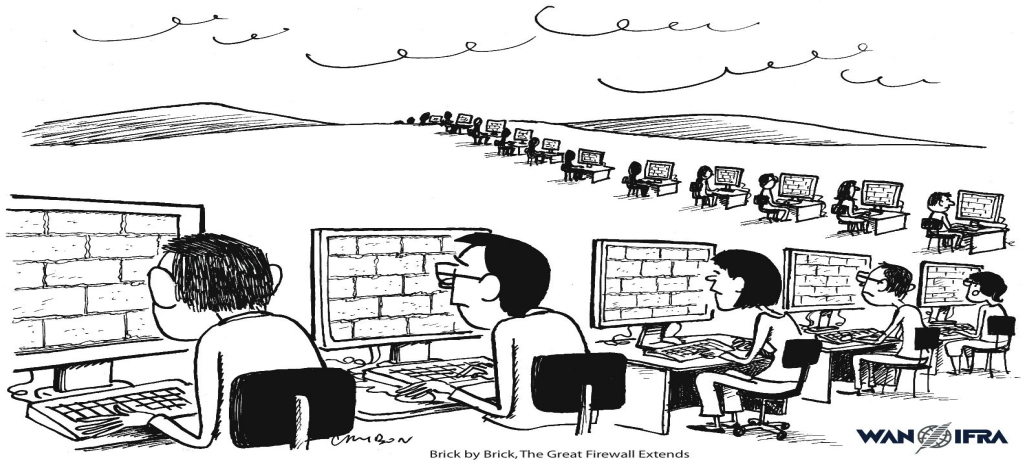

WILL CALL
SETH ROGEN JAMES FRANCO
THE INTERVIEW

另一种网络战定义

2009年8月，俄罗斯起草的上海合作组织协议把“信息战”界定为两个或更多国家之间在信息空间的对抗，目标是动摇政治、经济、社会系统，或者对民众进行洗脑，以破坏社会与国家的稳定。在协议中，把“信息威胁”说成是传播有害他国的精神道德和文化方面的信息。

另一种网络战案例


TWEET
GREAT FIREWALL OF CHINA
Google


WAN IFRA
Brick by Brick, The Great Firewall Extends


SHANGHAI Internet Cafe
Uh oh, He searched 'Human Rights' one time too many.
The Net in China

关注我们

IDF官网/论坛：

http://www.idf.cn

http://bbs.idf.cn

邮箱联系：

idf#idf.cn

关注微博

新浪微博：@IDF实验室

腾讯微博：@NeteasyIDF