从案件看国内DDOS现状

The Present Situation of Domestic DDOS in View of Criminal Cases

江苏公安　童瀛

CONTENTS

网警的职责定位与主要承担的工作

什么是网络警察

网络警察

根据《中华人民共和国人民警察法》第6条的规定，人民警察应当依法履行“监督管理计算机信息系统的安全保卫工作”的职责。即此而言，目前正在从事公共信息网络安全监察工作的人民警察当称之为“网络警察”。

挑战

网警的职责定位

网安

保卫网络安全
维护网络社会
稳定健康发展

网络警察，在中国正式的名字应该是国际互联网安全监察专业警察。它的诞生也是社会发展、技术提高有效打击犯罪的必然要求。网络警察主要有两个方面的责任：

一是计算机信息系统安全管理，
二是计算机犯罪侦查。

打击网络犯罪

利用计算机实施盗窃罪
在线传播计算机病毒
利用计算机实施贪污
DDos攻击
非法网络集会
广西南宁
网络招嫖
袭击网站
非法侵入计算机信息系统罪
网络谣言
网上侵犯商业秘密
电子邮件攻击
网上诽谤
网上洗钱
网上毁损名誉
网上诈骗
网络黑色产业链
电子讹诈
网上走私
电信诈骗
网上组织邪教组织
电子取证
网络色情传播
网络侮辱、诽谤
破坏计算机系统软件
网络战争
电子盗窃
利用计算机实施金融诈骗罪
网络核武
网络版权侵权
入侵金融系统
恶意软件
网上刺探、提供国家机密的犯罪
利用计算机窃取国家秘密罪
网络钓鱼
破坏计算机信息系统罪
利用网络开展恶意竞争

黑色产业链

[网络犯罪分类]

非法侵入计算机信息系统罪

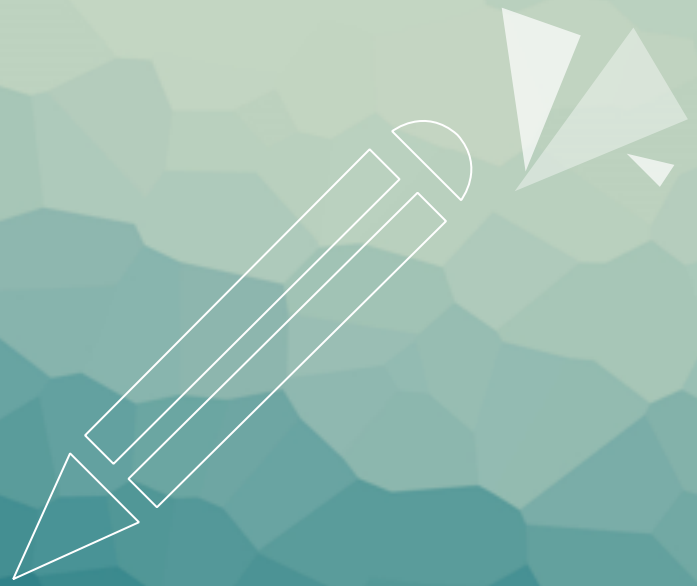
破坏计算机信息系统罪

利用计算机网络实施的犯罪

网络犯罪克星

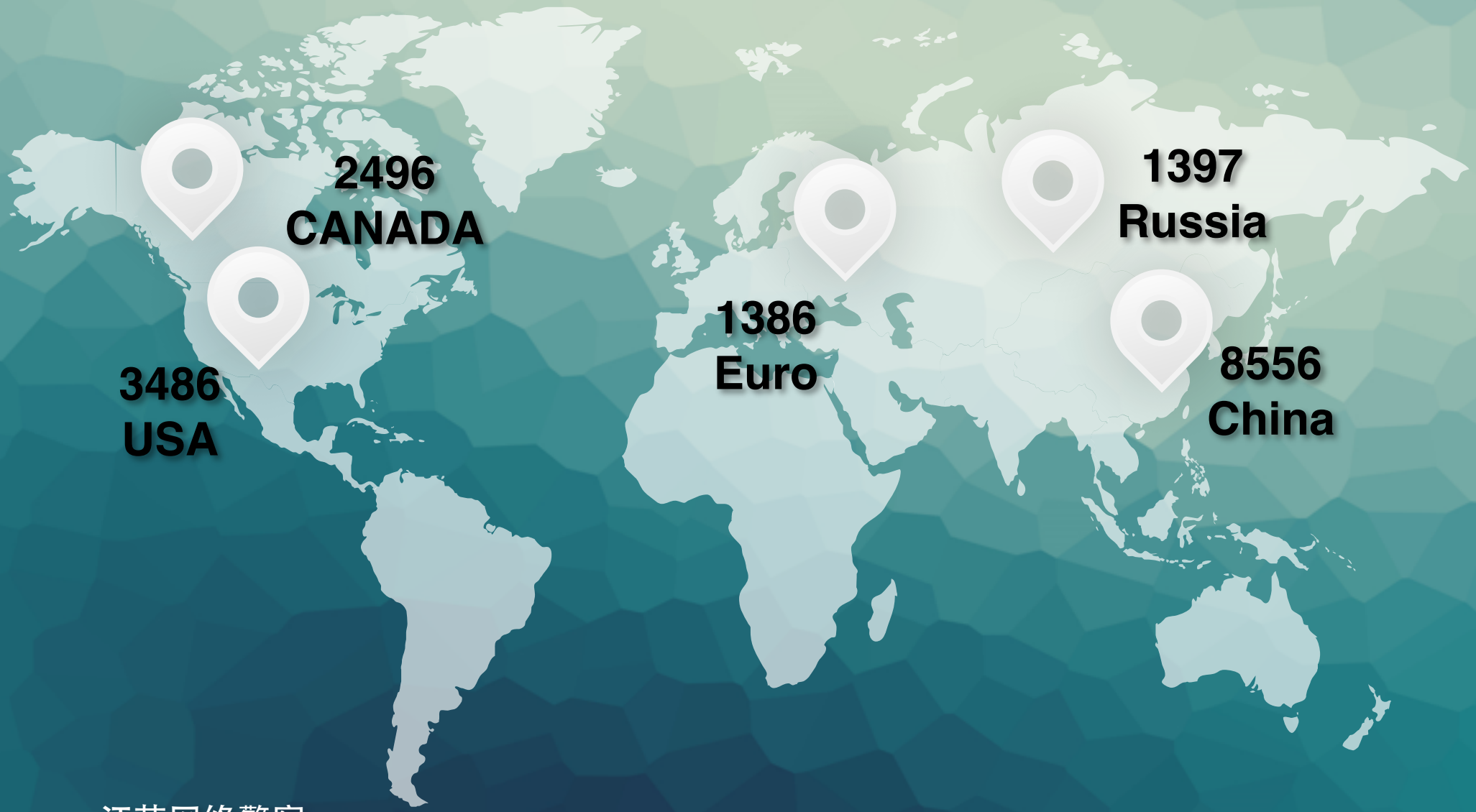
网上犯罪是一种高技术型犯罪，与其他犯罪相比，具有隐蔽性、复杂性、呈国际化趋势等特点，网络警察应以对越境数据流实行“严格控制下的合理利用”为己任。

在网络上，人与人之间很难判断身份、距离，所以网络成为很多诈骗、敲诈勒索、传播淫秽物品、出售假冒伪劣产品等犯罪嫌疑人从事违法犯罪活动的场所。但是因为有网络警察，所以网络就不会成为违法犯罪的沃土。因为哪里有违法犯罪的存在，哪里就有法律的利剑高悬。



从案件看Ddos攻击发展

全球DDos攻击分布

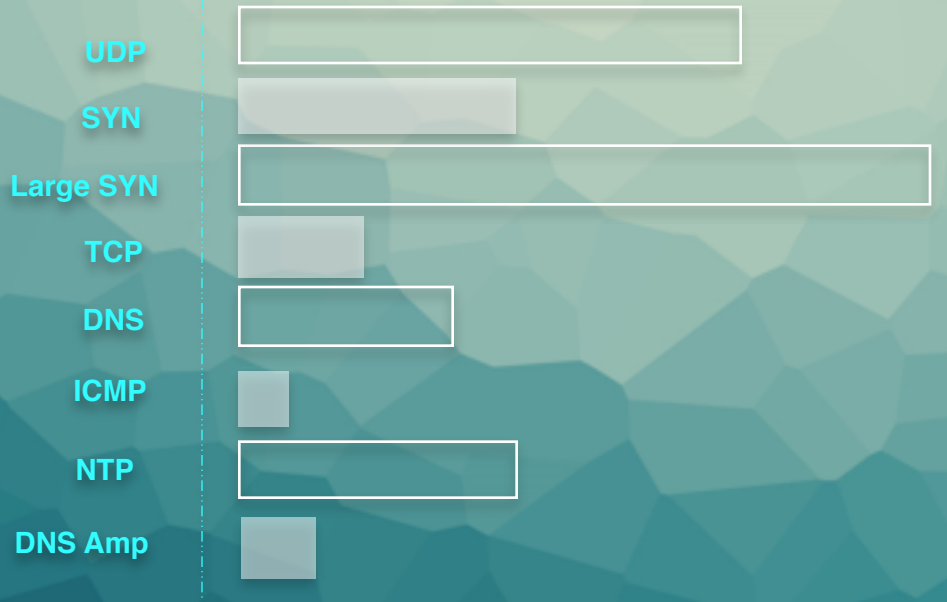


DDos攻击类型

网络层D攻击类型分布（比例）

56.7%
50.7%
22.0%
21.2%
12.3%
10.4%
9.5%
7.9%

网络层D攻击类型分布（峰值）



61.1Gbps
28.2bps
73.9Gbps
17.6Gbps
35.5Gbps
6.0Gbps
39.7Gbps
18.8Gbps

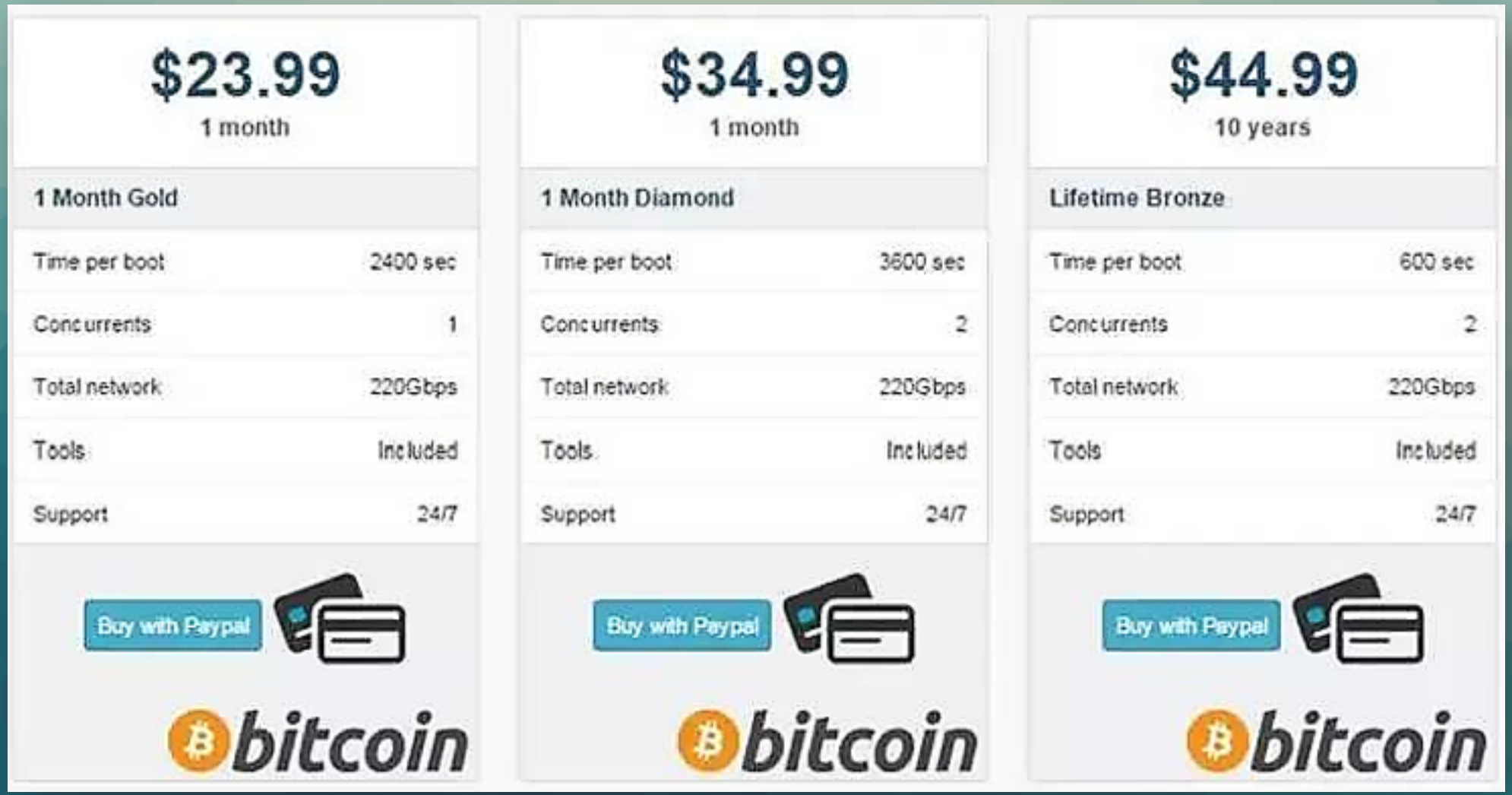
主要的攻击类型

NTP-FLOOD

SYN-FLOOD

UDP-FLOOD

僵尸网络


$23.99
1 month
1 Month Gold
Time per boot 2400 sec
Concurrents 1
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin
$34.99
1 month
1 Month Diamond
Time per boot 3600 sec
Concurrents 2
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin
$44.99
10 years
Lifetime Bronze
Time per boot 600 sec
Concurrents 2
Total network 220Gbps
Tools Included
Support 24/7
Buy with Paypal
bitcoin

受攻击目标排名

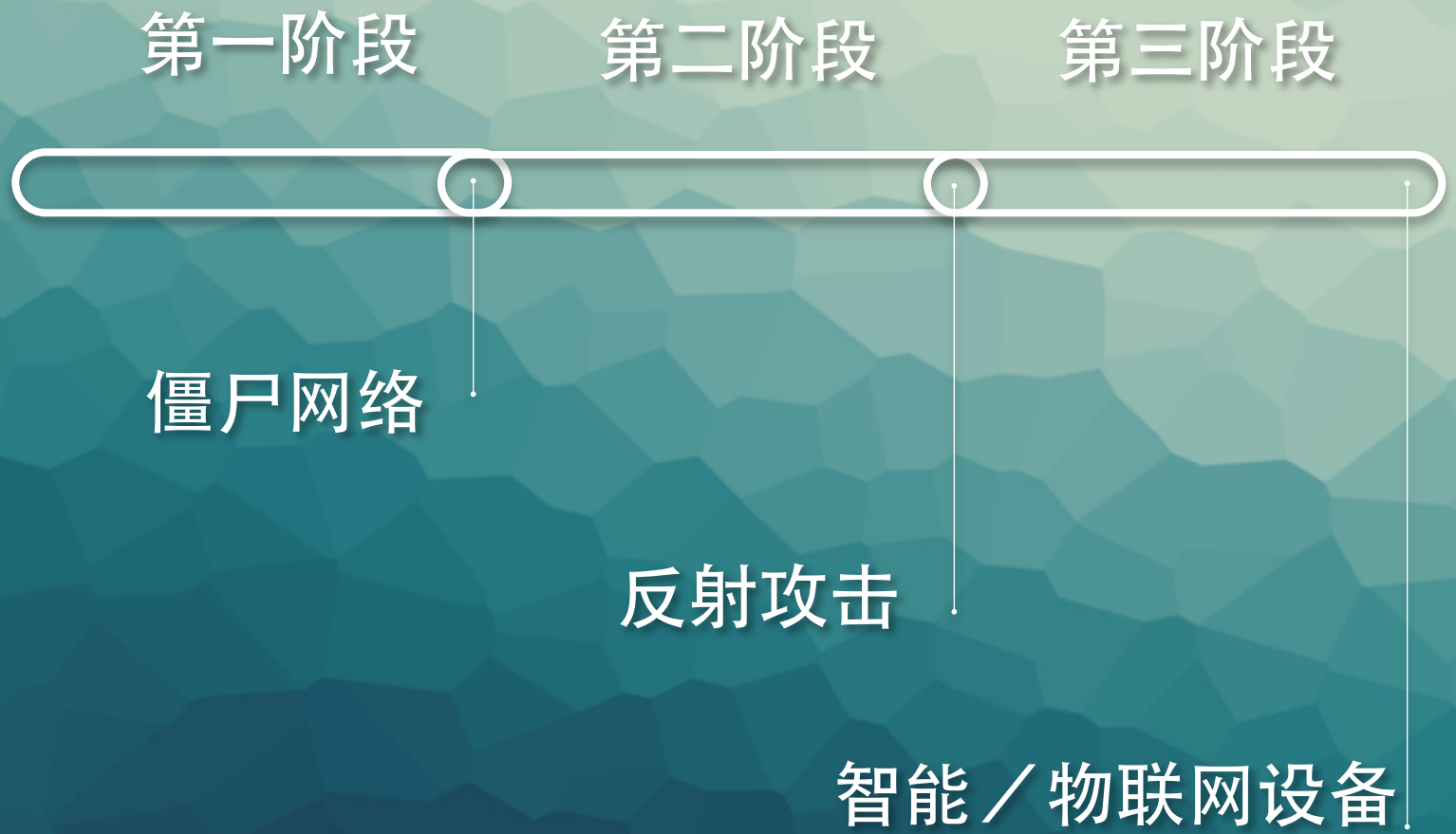
50%
在线游戏

70%
商业公司

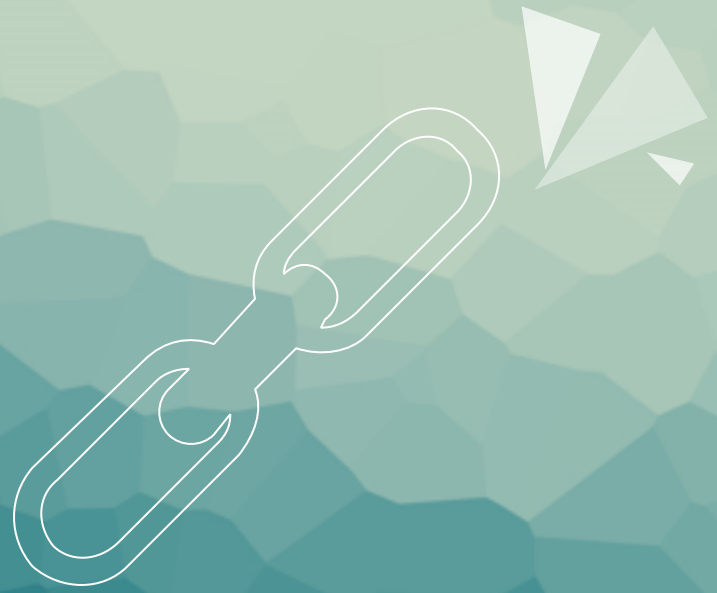
80%
政府机构

国内受害现状

D攻击发展趋势



D攻击发展趋势



针对Ddos攻击的自我防范

D攻击基础防御

网络设备可能是其整个业务运营过程中的瓶颈

网络地址转换（NAT）虽然可以很好地解决因IP地址不足而存在的资源分配的问题

目前网络环境中，针对应用层的DDoS攻击越来越多

配备较大的网络带宽

升级服务器的硬件设备

购置高性能的网络设备

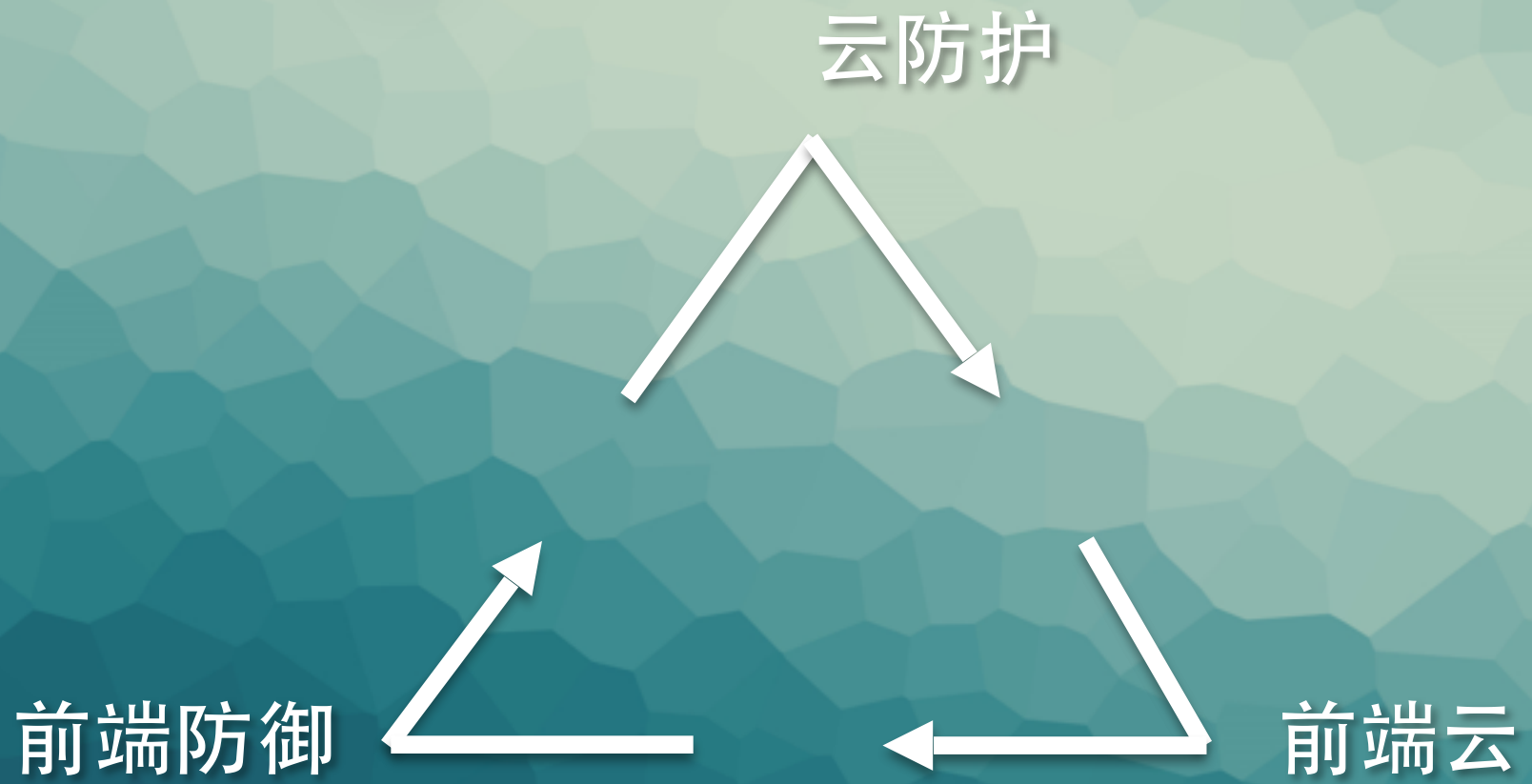
避免使用网络地址转换

动态Web应用改为静态页面

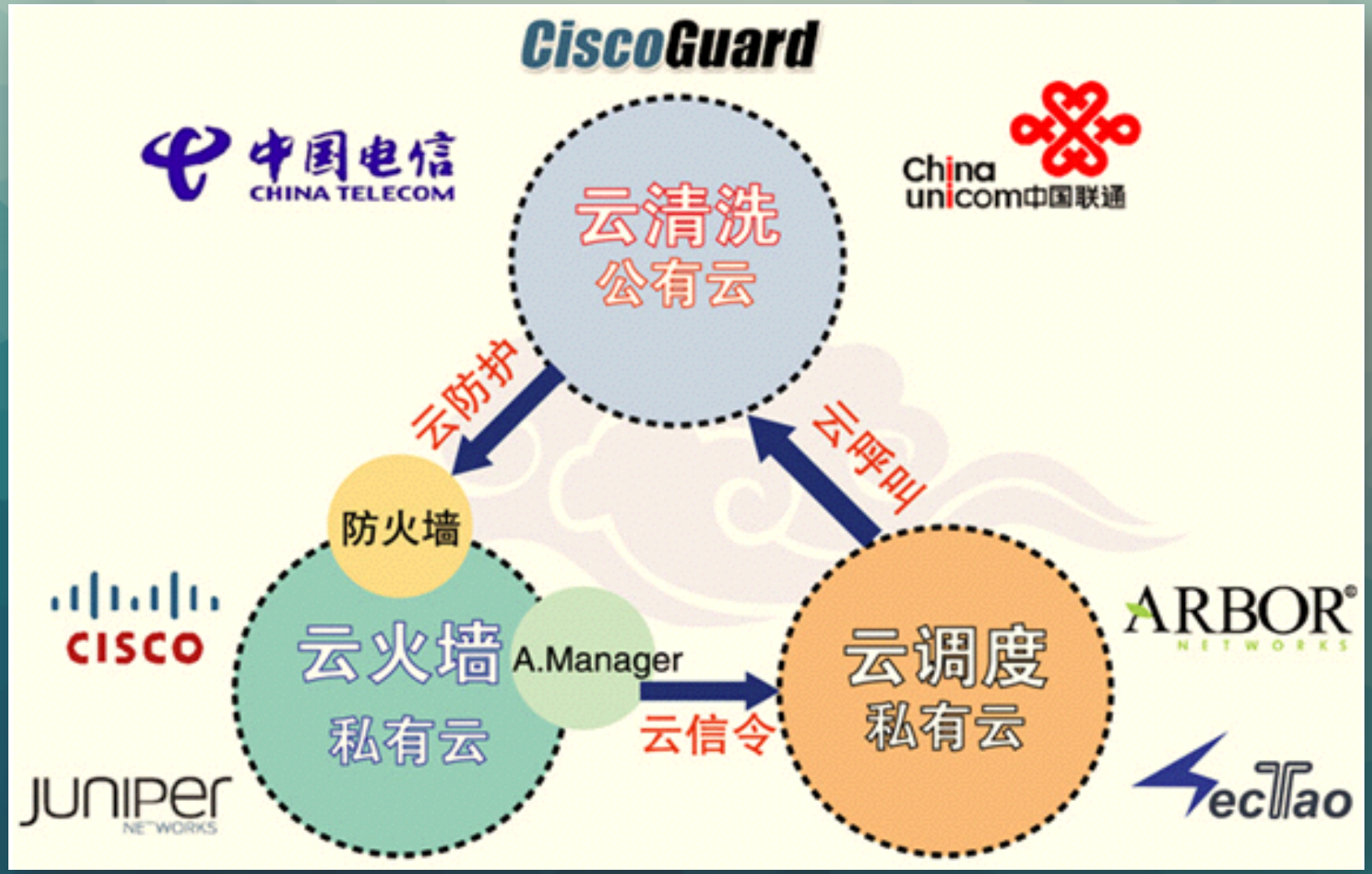
因为网络带宽的大小直接关系到网络运行的快慢以及能够抵御DDoS攻击的大小

DDoS攻击的目的就是浪费掉服务器的资源

主要防御模式



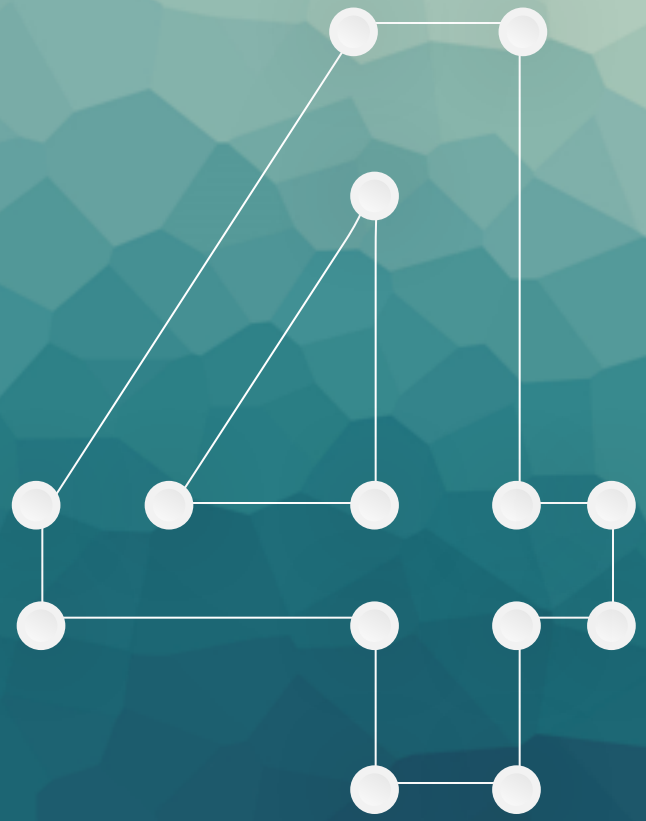
江苏电信“云清洗”


CiscoGuard
中国电信
CHINA TELECOM
China unicom中国联通
云清洗
公有云
云防护
云呼叫
防火墙
CISCO
云火墙
私有云
A.Manager
云信令
云调度
私有云
ARBOR
NETWORKS
JUNIPER
NETWORKS
ecTao

D攻击防范瓶颈

1.过多的硬件设备
2.过高的宽带消费
3.消耗过多的人力资源

中小企业无力承担



如何应对D攻击

D攻击违法性

刑法286条

刑法286条第1款：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

遭遇D攻击的应对

5000￥+
造成损失

1W用户1h+
瘫痪网络

20台+
非法控制

遭遇D攻击的应对

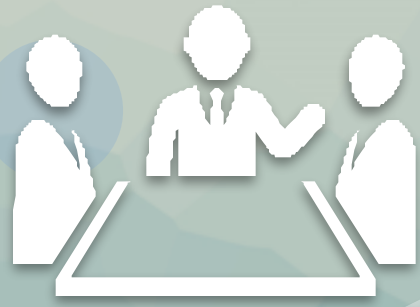
管辖权

对网络安全人员的建议

对中小企业的建议

对涉网单位的建议

对普通网民的建议



网警呼吁共同防御D攻击

刑事打击联盟

江苏网警&腾讯安全中心

2015

THANK YOU FOR WATCHING