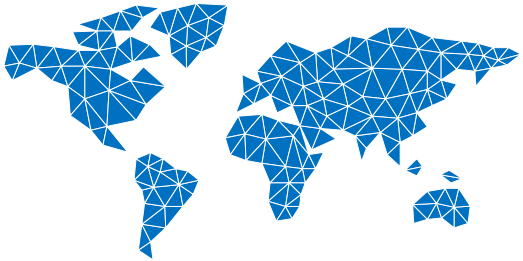


Network Information Security

Rachel Yuan
2019.9

1

没有网络安全就没有国家安全，
没有信息化就没有现代化。

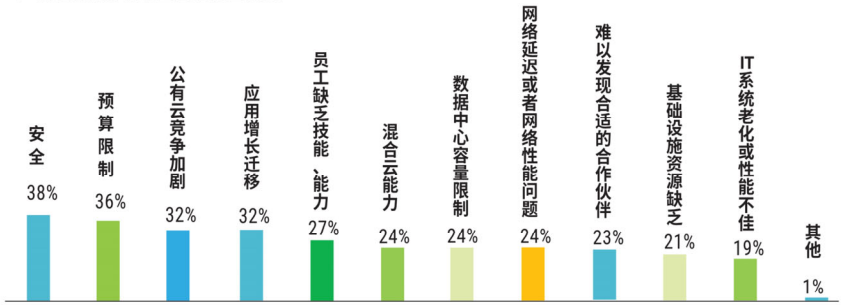
2014年2月27日，习近平在中央网络安全和信息化领导小组第一次会议上发表重要讲话

2

3

安全已经成为全球企业数字化转型的最大挑战

Q：贵组织数字化转型面临哪些挑战?



N（CIO数量）= 500

IDC ANALYZE THE FUTURE

Source：IDC, 2019

5

4

网络空间安全专业

国务院学位委员会 教育部关于增设网络空间安全一级学科的通知

学位[2015]11号

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

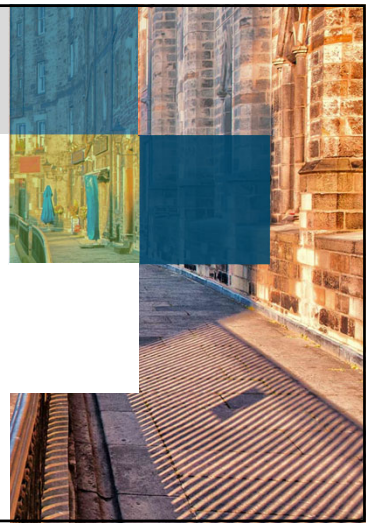
为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

国务院学位委员会 教育部

5

CONTENTS

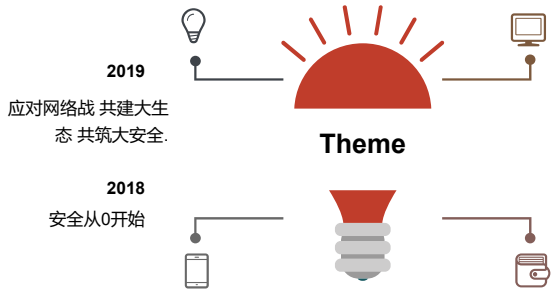
- ISC 2019
- Cyber war (360)
- Why security is hard?
- Course introduction



6

7

ISC (Internet Security Conference)



2019
应对网络战 共建大生态 共筑大安全.

2017
万物皆变，人是安全的尺度

2018
安全从0开始

2016
协同联动共建安全 命运共同体

8

8

网络战


震网事件

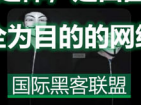

"阿拉伯之春"

乌克兰大停电

什么是网络战

网络战是政策的延伸，是由国家或组织主导发起的，以国家安全为目的的网络攻击行为。


网络军队

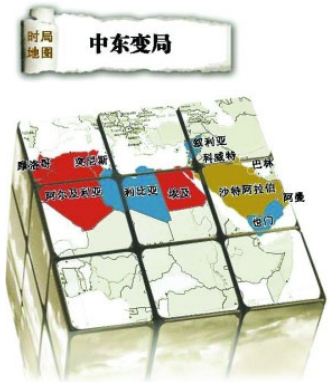

国际黑客联盟


网军投入

网络空间已经逐步发展成为继陆、海、空、天之后的 **第五大战略空间**

9

Arab spring




叙利亚难民营小女孩看见长焦镜头惊恐的举起了双手

10

10

网络战的特点

破坏力、影响力巨大
关乎民生、危及国家安全，会对国际政治产生重大影响

攻击手段多样化
定制化的攻击方案，综合运用社会工程学、供应链缺陷、木马等

隐蔽性高
一般采用0日攻击，未知恶意代码攻击、高级逃逸伪装，很难在前期发现

潜伏时间长
从入侵成功，到产生破坏，可进行长时间潜伏

11

2019事件回顾

APT34组织网络武器库被曝光

12家中国机构 位列被攻击名单,覆盖金融、电信、能源、交通、制造领域

链接地址	域名	地区	行业
https://122.146.71.136/owa/auth/error3.aspx	mail.taifo.com.tw	中国台湾	电信
https://59.124.43.229/owa/auth/error0.aspx	tgpf.org.tw	中国台湾	NPO
https://1.202.179.13/owa/auth/error1.aspx	mail.cecep.cn	中国大陆	能源
https://1.202.179.14/owa/auth/error1.aspx	mail.cecep.cn	中国大陆	能源
https://114.255.190.1/owa/auth/error1.aspx	mail.generali-china.cn	中国大陆	金融
https://180.166.27.217/owa/auth/error3.aspx	exchange.bestv.com.cn	中国大陆	媒体
https://180.169.13.230/owa/auth/error1.aspx	bdo.com.cn	中国大陆	能源
https://210.22.172.26/owa/auth/error1.aspx	lswebext.sdec.com.cn	中国大陆	能源
https://221.5.148.230/owa/auth/outlook.aspx	mail.swsc.com.cn	中国大陆	金融
https://222.178.70.8/owa/auth/outlook.aspx	mail.swsc.com.cn	中国大陆	金融
https://222.66.8.76/owa/auth/error1.aspx	lswebext.sdec.com.cn	中国大陆	能源
https://58.210.216.113/owa/auth/error1.aspx	mail.neway.com.cn	中国大陆	制造
https://60.247.31.237/owa/auth/error3.aspx	crccre.cn	中国大陆	交通
https://60.247.31.237/owa/auth/logoff.aspx	crccre.cn	中国大陆	交通
https://202.175.114.11/owa/auth/error1.aspx	webmail.netcraft.com.mo	中国澳门	电信
https://202.175.31.141/owa/auth/error3.aspx	exchange.must.edu.mo	中国澳门	教育

12

2019事件回顾

针对关键基础设施的潜伏与攻击频繁发生

13

2019事件回顾

6月20日，美网军对伊朗发动准军事行动，通过网络攻击破坏了伊朗的导弹控制系统

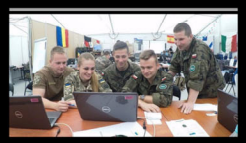
美伊网络安全攻击“你来我往”

7月13日，纽约突发大面积停电，美军方声称遭到了来自伊朗革命卫队信息战部队的打击，后又辟谣。

14

2019事件回顾

北约举行全球最大网络安全演习“锁盾2019”应对网络战

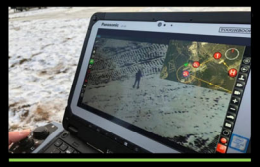


多国参与，协同作战

多达25个国家、1200名专家参与

军事环境，实战演练

复杂的业务和军事系统



红蓝对抗，攻守兼备

4000个虚拟系统，承受2500次攻击

15

网络战正在发生

貌似和平很久，但战争从未远离，只是形式不同

必须用作战的视角看待网络安全

16

对网络战的理解

不宣而战

不分战时平时，渗透潜伏是网络战的一部分

17

对网络战的理解

国家级力量入场

100+国家成立网军，军事级技术，国家级对抗

18

对网络战的理解

关键基础设施成为战场

万物互联时代，虚拟空间和物理空间连通

19

对网络战的理解

没有攻不破的网络

漏洞不可避免，漏洞无处不在

20

EVERY SYSTEM = CYBER THREAT
有系统在的地方，就有网络威胁

21

对网络战的理解

易攻难防

攻防不平衡，资源向攻击方倾斜

22

对网络战的理解

整体战

不分军用民用，不分国家、企业、个人

23

对网络战的理解

超限战

手段多元，无所不用其极

24

对网络战的理解

秘密战

长期谋划，瞬间致瘫

来无影、去无踪，难以溯源

25

对网络战的理解

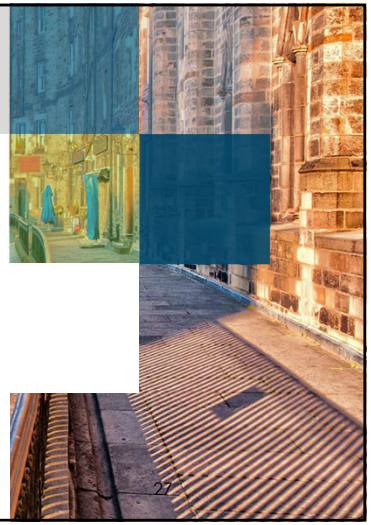
网络战成为战争首选

成本低，效果好，烈度可控

26

Wrap up

- What is cyber war?
- Properties of cyber war
- 0 day attack



27

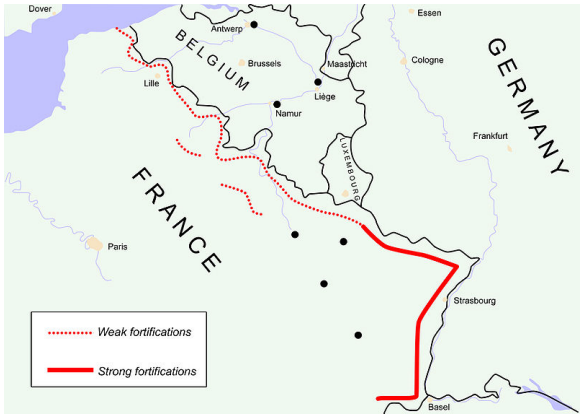
Security is hard, and it is much harder than ever before

请同学们讨论两个问题：

1. 为什么安全是一件困难的事？
2. 为什么目前的安全形势比以往任何时间都要严峻？

28

Why security is hard?



29

Why security is hard?

- Most technology-related efforts are concerned with ensuring that something good happens. Security is all about ensuring that **bad things never happen.**

30

Why security is hard?

- Information management systems are a complex, **"target-rich"** environment comprising: hardware, software, storage media, peripheral devices, data, people.

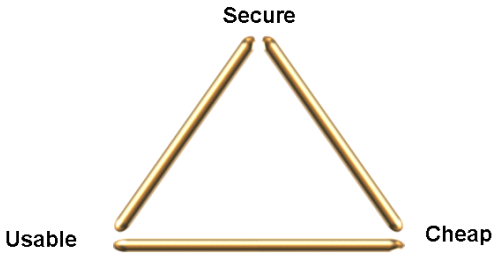
31

Why security is hard?

- **Security is often an afterthought.**

32

Security is a tradeoff



33

Course introduction

- 1. Relationships with other courses
- 2. Learning objectives
- 3. Syllabus introduction
- 4. Evaluation
- 5. References
- 6. Learning methods

34

Learning objectives

- Learn some modern security concepts and technologies.
  - Cryptography
  - Access control
  - Signature
  - …

35

Leaning objectives (cont'd)

- How to apply the above concepts and technologies in network environment?
  - Wifi security: WEP, WPA
  - Web security: SSL
  - Email security: PGP
  - Authentication: PKI, Kerberos
  - Boundary security: Firewall, IDS

36

Learning objectives (cont'd)

- **Raise the awareness of cyber security**
  - What is happening?
  - What is lying underneath?
  - What are the technologies being involved?
  - How to protect myself?

37

Examples

- 俄罗斯**APT28**侵入德国外交及内政部网络长达一年（**3**月**5**日）
- 亲历历史！史上首个核弹级**DDoS**攻击正在荼毒全球（**3**月**1**日）
- 国内两家医院连遭比特币勒索（**3**月**3**日）

38

Learning objectives (cont'd)

- Learning how to learn

39

Course Outline (Draft)

- Part one:
  - Introduction
  - Basic concepts
- Part two:
  - Classical encryption
  - Block cipher & DEC
  - AEC & Operation Mode
- Part Three:
  - number theory
  - Public key crypto & RSA
  - Diff-Hellman key exchange
- Part four:
  - Hash function
  - Digital signature
- Part five:
  - PKI
  - Authentication
- Part six:
  - Access control
- Part seven:
  - IPsec & SSL
  - PGP
- Part eight:
  - Firewall & IDS

40

References

- www.coursera.org
  - Cryptography 1
- en.wikipedia.org or zh.wikipedia.org
- 计算机网络安全的理论与实践 王杰 高等教育出版社
- Cryptography and Network Security (Fifth Edition) William Stallings
- 白帽子讲信息安全 吴翰清 电子工业出版社
- Applied cryptography (应用密码学) Bruce Schneier

41

Evaluation

- In-class performance：5%
- Labs and homework：25%
- Final exam：70%

42

Homework

- 1. Think about why security is hard, and it is much harder than ever before.
- 2. Watch “the fifth space” (第五空间纪录片), jot down the key words you hear while you are watching, such as APT, Stuxnet etc. and check them up in the Internet.
- 3. Get familiar with the network commands ipconfig, ping, tracert, netstat. Complete your lab assignment.

- Next time, we will talk about the three elements of information security and security principles (安全原则).

43