音调不定的号角：全球网络空间博弈解析与中国的战略选择

沈逸 副教授

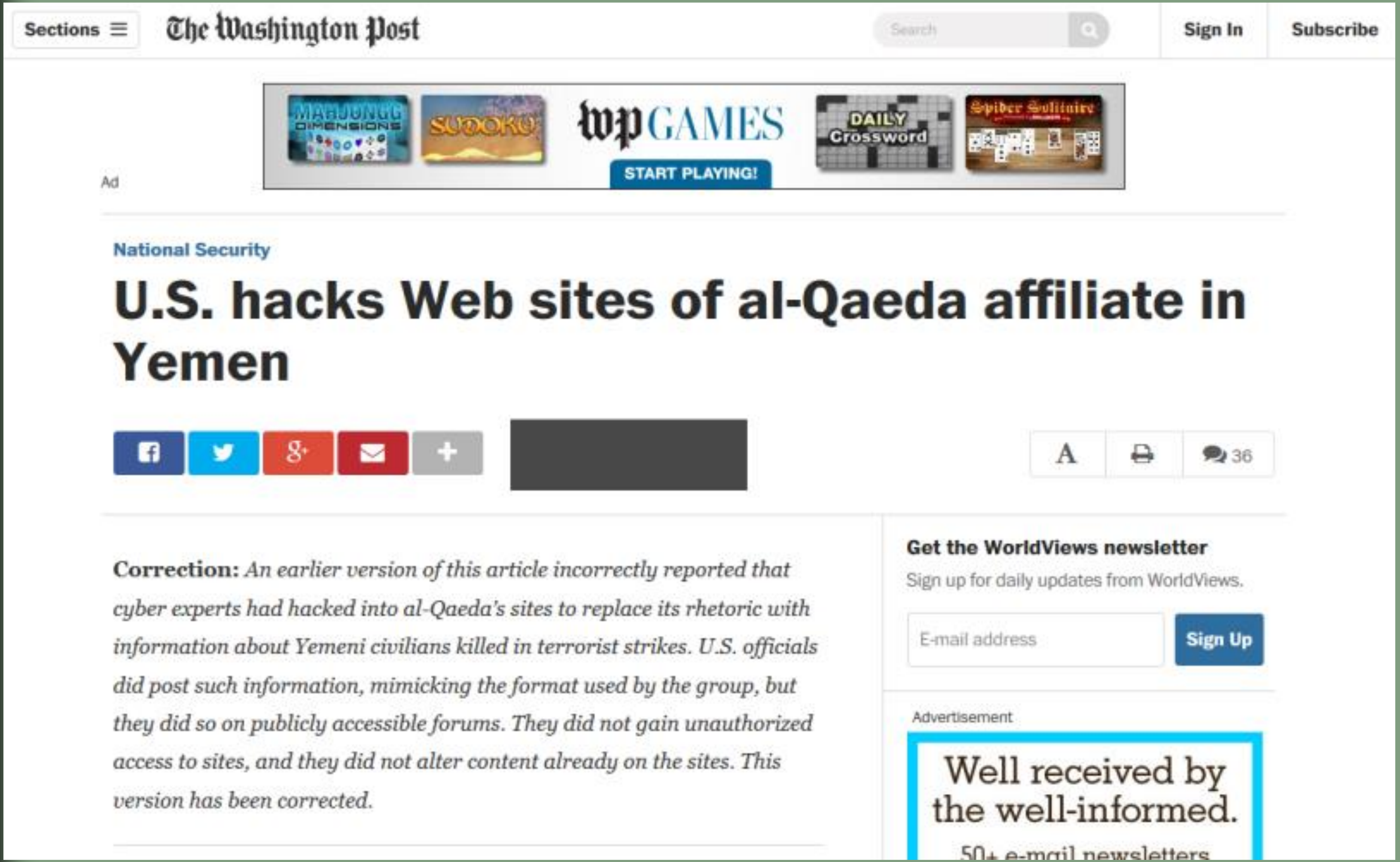
复旦大学网络安全研究中心（筹）

复旦大学国际关系与公共事务学院

2015年1月20日

案例1： APT1报告

案例2：围绕内容传播的博弈



National Security

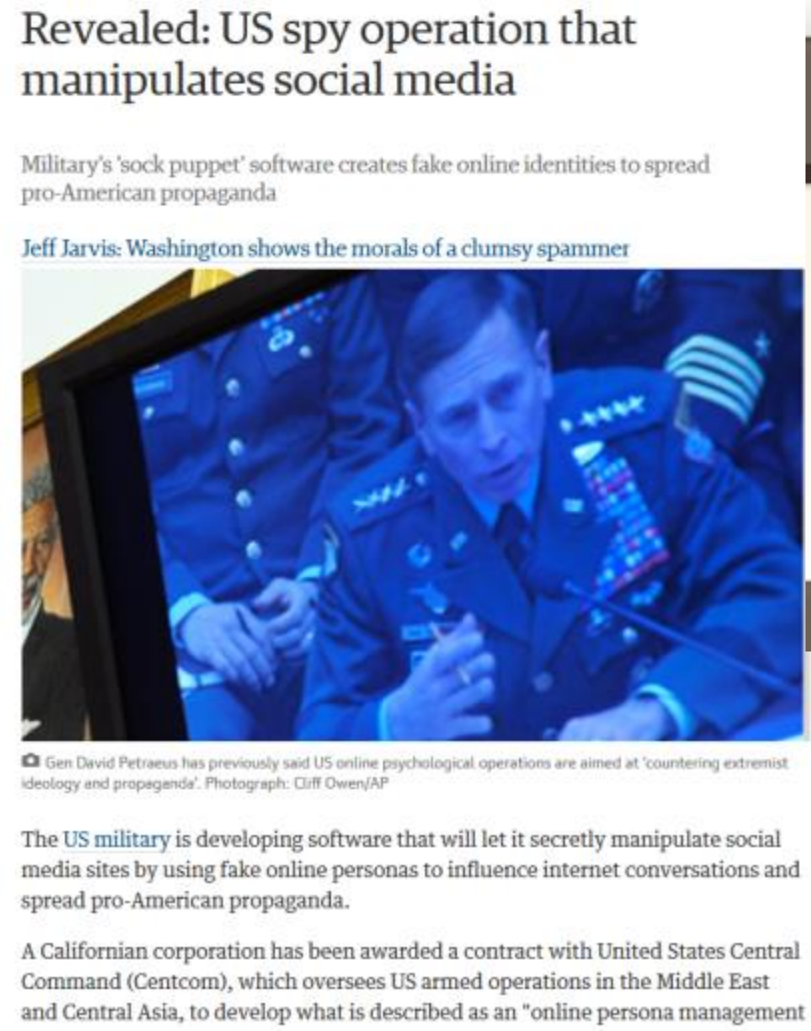
U.S. hacks Web sites of al-Qaeda affiliate in Yemen

Correction: *An earlier version of this article incorrectly reported that cyber experts had hacked into al-Qaeda's sites to replace its rhetoric with information about Yemeni civilians killed in terrorist strikes. U.S. officials did post such information, mimicking the format used by the group, but they did so on publicly accessible forums. They did not gain unauthorized access to sites, and they did not alter content already on the sites. This version has been corrected.*

Get the WorldViews newsletter

Sign up for daily updates from WorldViews.

- Clinton said the campaign was conducted by the Center for Strategic Counterterrorism Communications, based at the State Department, with expertise drawn from the military and the intelligence community.
- The State Department’s activities are the latest in online counterterrorism efforts to stem the spread of radical Islamist ideology that stretch back at least a decade.
- The U.S. Central Command has a digital engagement team that monitors blogs and forums, targeting those that are moderate in tone and engaging with users, said Maj. David Nevers, former chief of the team.



Revealed: US spy operation that manipulates social media

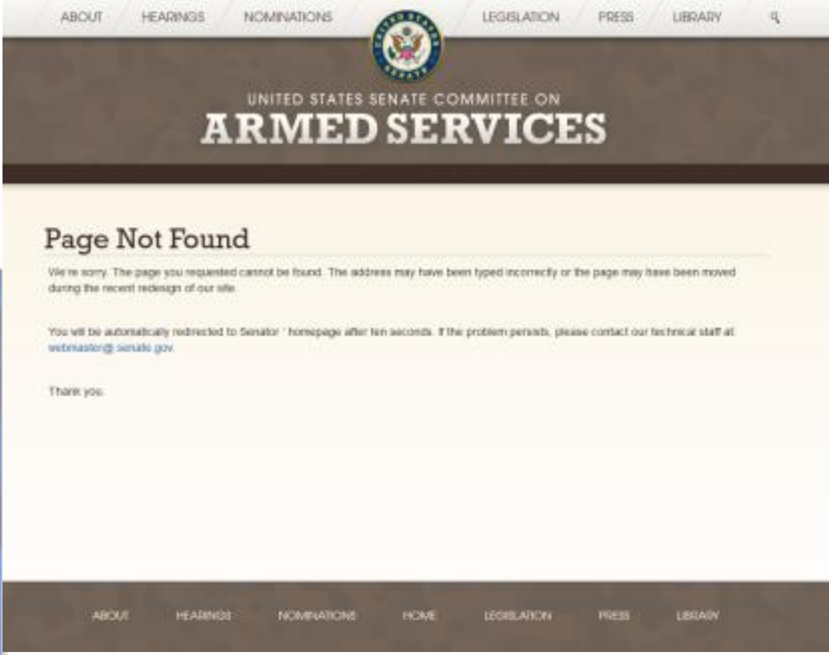
Military's 'sock puppet' software creates fake online identities to spread pro-American propaganda

Jeff Jarvis: Washington shows the morals of a clumsy spammer

Gen David Petraeus has previously said US online psychological operations are aimed at 'countering extremist ideology and propaganda'. Photograph: Cliff Owen/AP

The US military is developing software that will let it secretly manipulate social media sites by using fake online personas to influence internet conversations and spread pro-American propaganda.

A Californian corporation has been awarded a contract with United States Central Command (Centcom), which oversees US armed operations in the Middle East and Central Asia, to develop what is described as an "online persona management

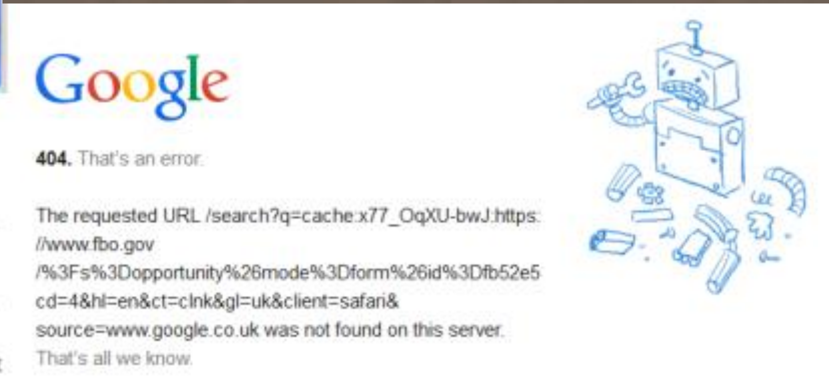


Page Not Found

We're sorry. The page you requested cannot be found. The address may have been typed incorrectly or the page may have been moved during the recent redesign of our site.

You will be automatically redirected to Senator ' homepage after ten seconds. If the problem persists, please contact our technical staff at webmaster@ senate.gov.

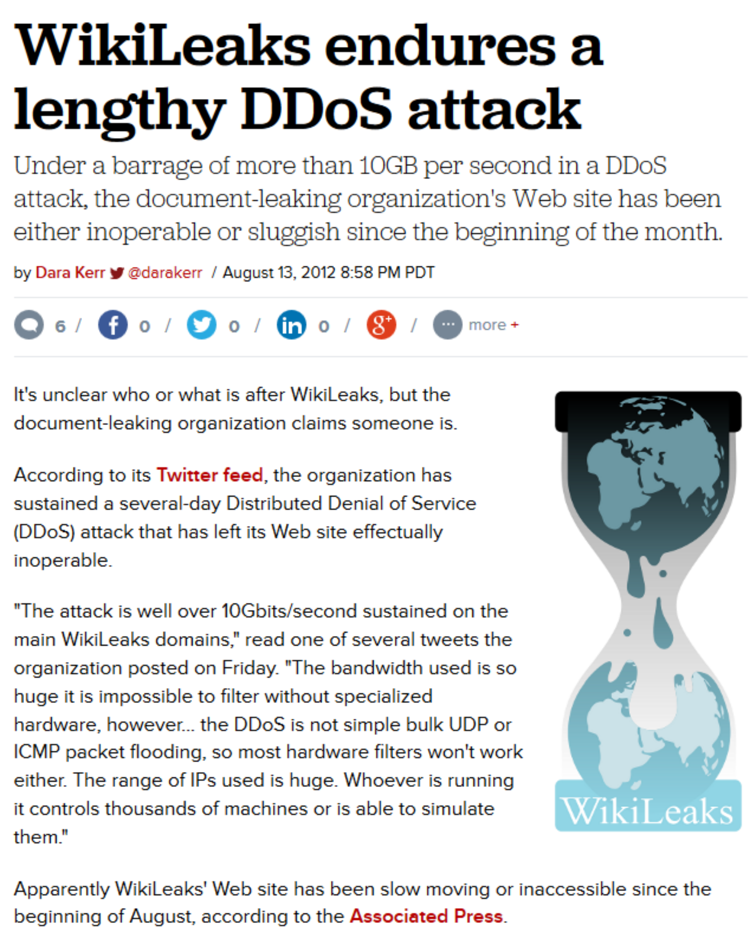
Thank you.



404. That's an error.

The requested URL /search?q=cache:x77_OqXU-bwJ:https://www.fbo.gov/%3Fs%3Dopportunity%26mode%3Dform%26id%3Dfb52e5cd=4&hl=en&ct=clnk&gl=uk&client=safari&source=www.google.co.uk was not found on this server. That's all we know.

案例3：复杂行为体之间的博弈



WikiLeaks endures a lengthy DDoS attack

Under a barrage of more than 10GB per second in a DDoS attack, the document-leaking organization's Web site has been either inoperable or sluggish since the beginning of the month.

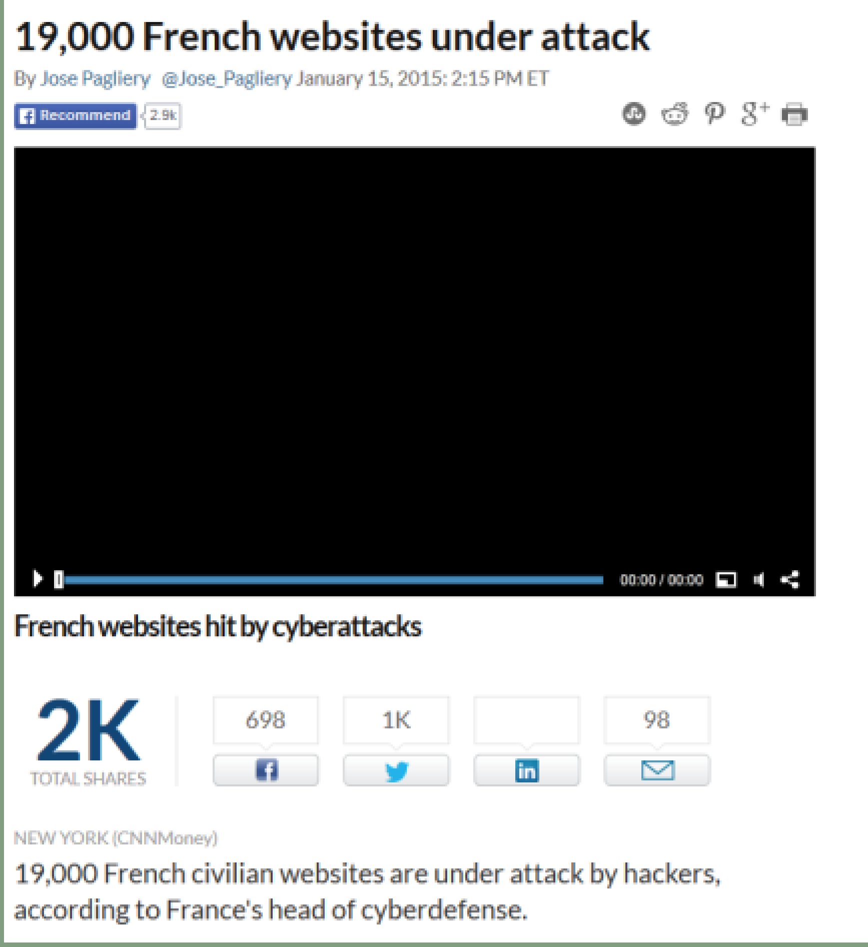
by Dara Kerr @darakerr / August 13, 2012 8:58 PM PDT

It's unclear who or what is after WikiLeaks, but the document-leaking organization claims someone is.

According to its Twitter feed, the organization has sustained a several-day Distributed Denial of Service (DDoS) attack that has left its Web site effectually inoperable.

"The attack is well over 10Gbits/second sustained on the main WikiLeaks domains," read one of several tweets the organization posted on Friday. "The bandwidth used is so huge it is impossible to filter without specialized hardware, however... the DDoS is not simple bulk UDP or ICMP packet flooding, so most hardware filters won't work either. The range of IPs used is huge. Whoever is running it controls thousands of machines or is able to simulate them."

Apparently WikiLeaks' Web site has been slow moving or inaccessible since the beginning of August, according to the Associated Press.



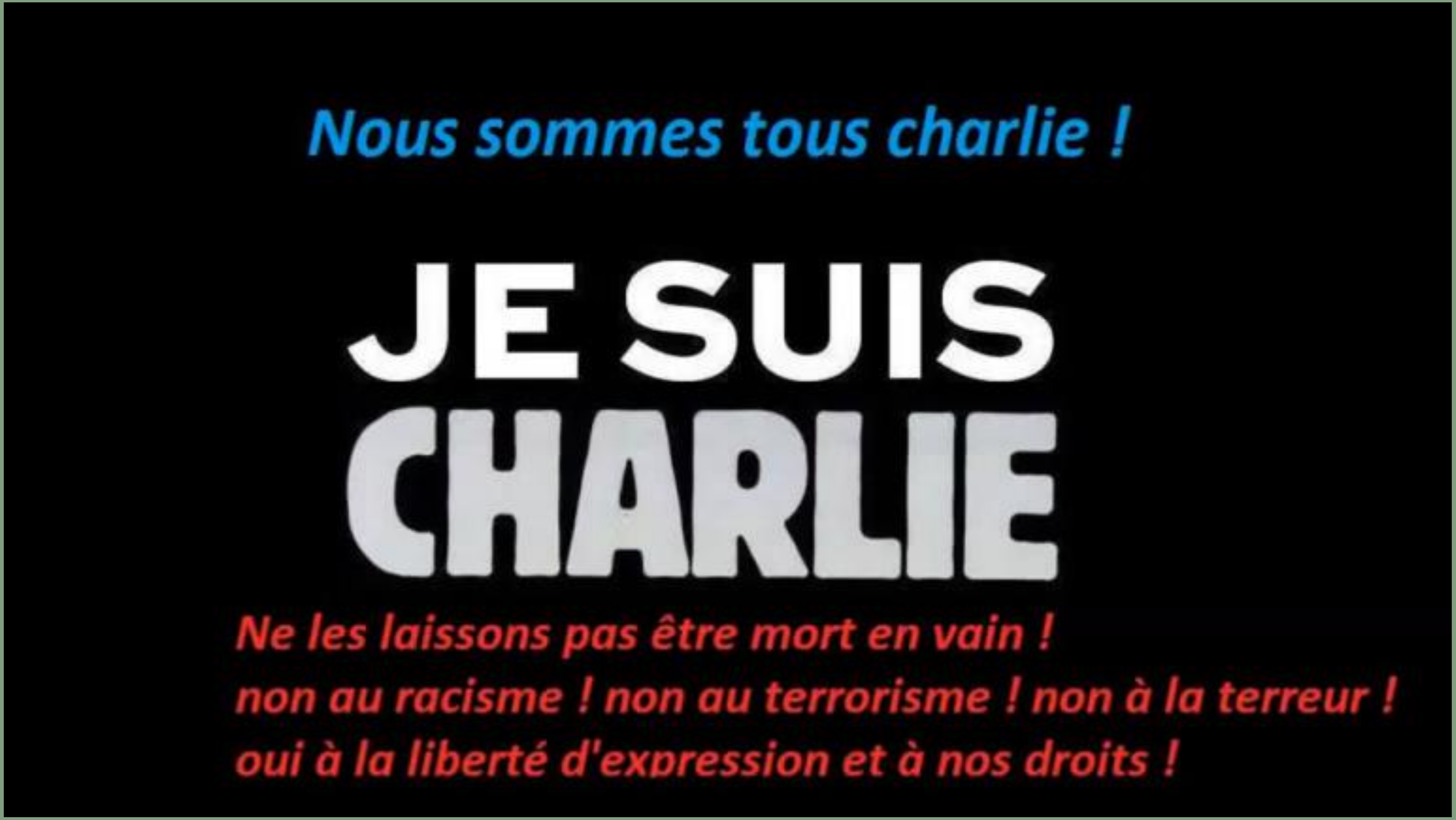
19,000 French websites under attack

By Jose Pagliery @Jose_Pagliery January 15, 2015: 2:15 PM ET

French websites hit by cyberattacks

NEW YORK (CNNMoney)

19,000 French civilian websites are under attack by hackers, according to France's head of cyberdefense.

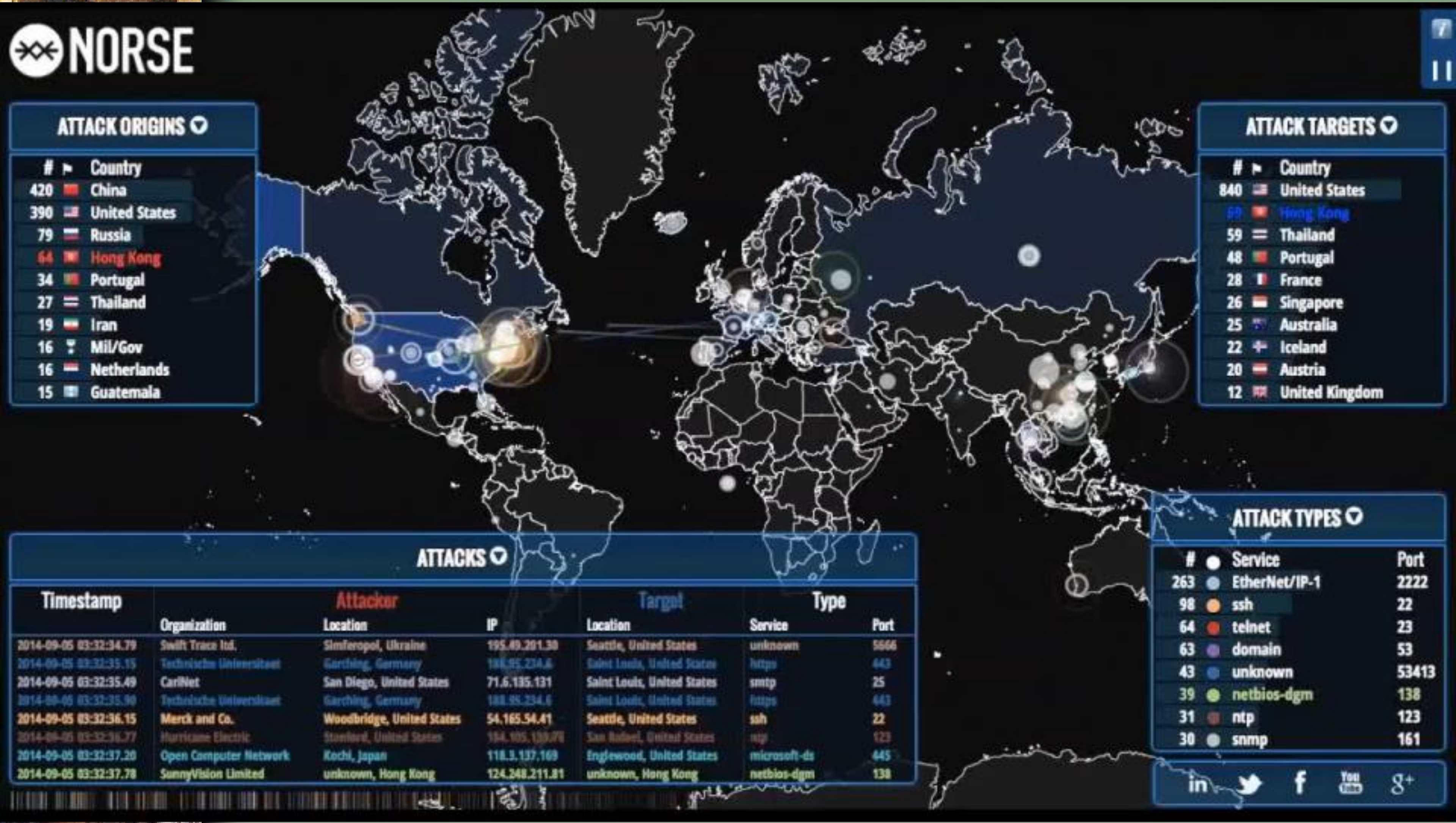


Nous sommes tous charlie !

JE SUIS
CHARLIE

Ne les laissons pas être mort en vain !
non au racisme ! non au terrorisme ! non à la terreur !
oui à la liberté d'expression et à nos droits !

案例4：网络战



ATTACK ORIGINS

#	Country
420	China
390	United States
79	Russia
64	Hong Kong
34	Portugal
27	Thailand
19	Iran
16	Mil/Gov
16	Netherlands
15	Guatemala

ATTACK TARGETS

#	Country
840	United States
69	Hong Kong
59	Thailand
48	Portugal
28	France
26	Singapore
25	Australia
22	Iceland
20	Austria
12	United Kingdom

ATTACK TYPES

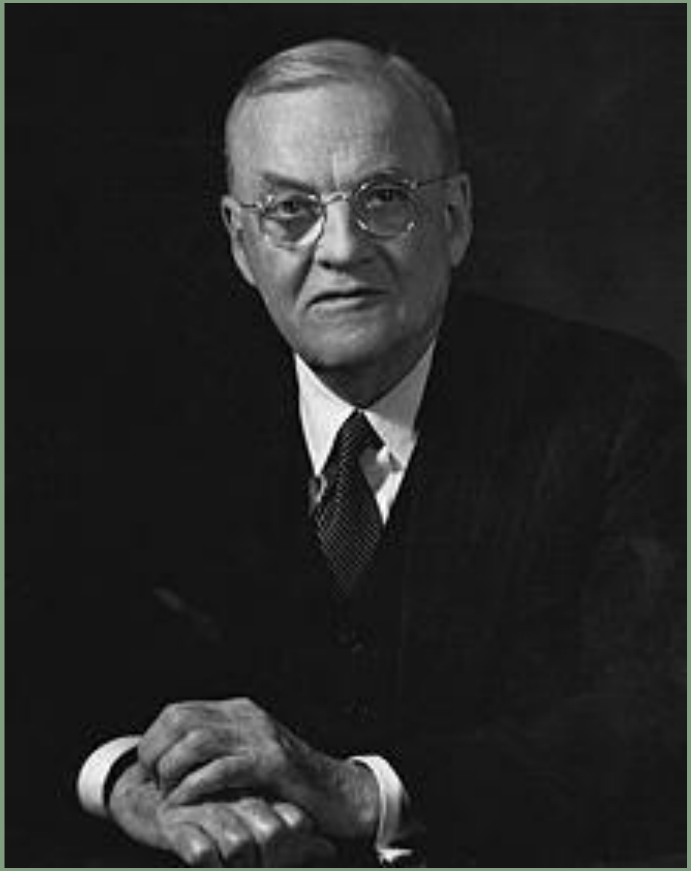
#	Service	Port
263	EtherNet/IP-1	2222
98	ssh	22
64	telnet	23
63	domain	53
43	unknown	53413
39	netbios-dgm	138
31	ntp	123
30	snmp	161

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-09-05 03:32:34.79	Swift Trace ltd.	Simferopol, Ukraine	195.49.201.30	Seattle, United States	unknown	5666
2014-09-05 03:32:35.15	Technische Universitaet	Garching, Germany	188.95.234.6	Saint Louis, United States	https	443
2014-09-05 03:32:35.49	CariNet	San Diego, United States	71.6.135.131	Saint Louis, United States	smtp	25
2014-09-05 03:32:35.90	Technische Universitaet	Garching, Germany	188.95.234.6	Saint Louis, United States	https	443
2014-09-05 03:32:36.15	Merck and Co.	Woodbridge, United States	54.165.54.41	Seattle, United States	ssh	22
2014-09-05 03:32:36.77	Hurricane Electric	Stanford, United States	184.105.139.70	San Rafael, United States	ntp	123
2014-09-05 03:32:37.20	Open Computer Network	Kochi, Japan	118.3.137.169	Englewood, United States	microsoft-ds	445
2014-09-05 03:32:37.78	SunnyVision Limited	unknown, Hong Kong	124.248.211.81	unknown, Hong Kong	netbios-dgm	138

核战略演进与网络安全

- “大规模报复”，杜勒斯，1954年1月12日
  - U.S. would respond to military provocation ″at places and with means of our own choosing.″
  - 在（美国）选择的地点，以（美国）选择的手段，进行大规模报复



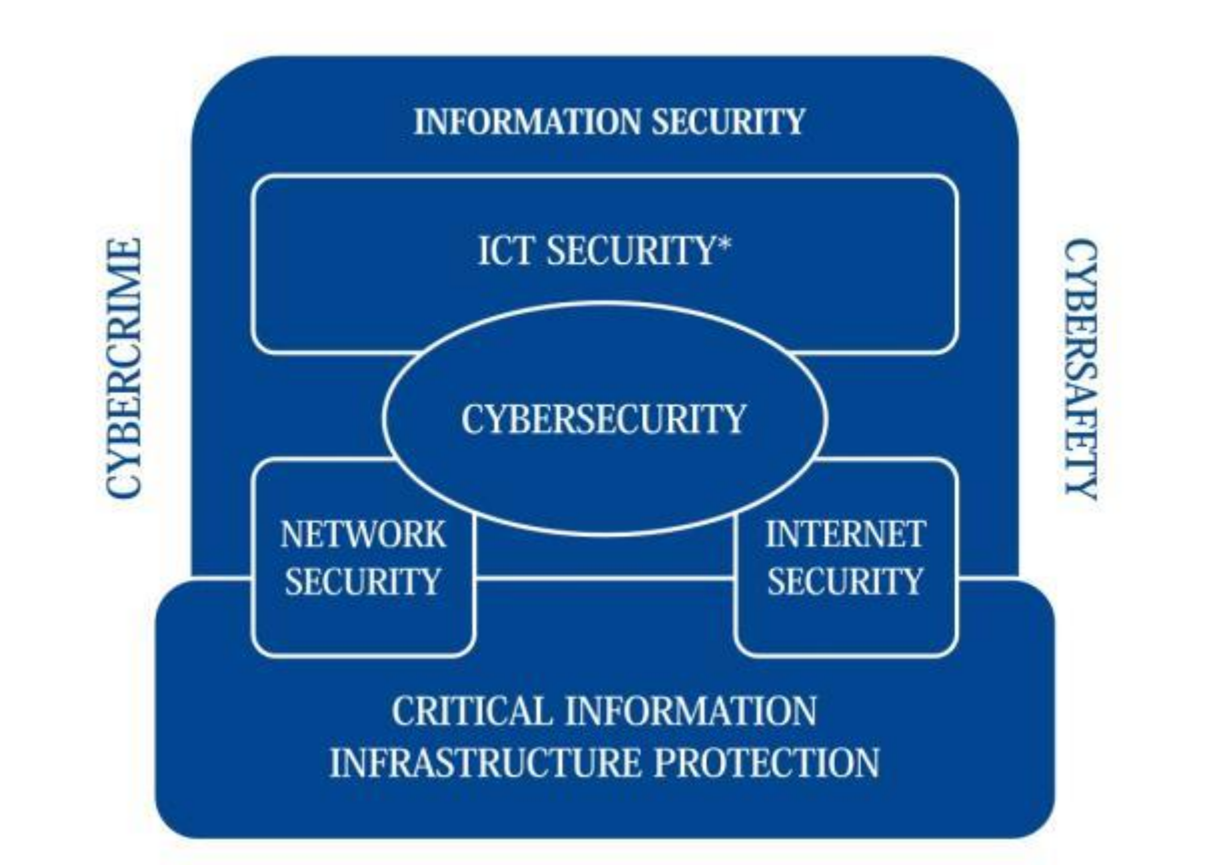
大规模报复战略的困境

- 大规模报复战略成立的基础
  - 压倒性的优势
  - 不成比例的攻防能力
- 大规模报复战略的困境
  - 变迁的力量对比
  - 新的力量均衡
  - “承诺”的可信度与行动自由

灵活反应战略

- 大规模报复战略让美国陷入困境
  - 要么在常规战争中被击败
  - 要么动用核武器（与对手同归于尽）
- 建立全频谱的反应能力，从常规武器到战术核武器到战略核武器，形成一种综合能力体系

全球网络安全博弈态势


INFORMATION SECURITY
CYBERCRIME
ICT SECURITY*
CYBERSAFETY
CYBERSECURITY
NETWORK SECURITY
INTERNET SECURITY
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

国际标准化组织定义网络安全

- 信息安全（Information Security）指强调根据相关用户的需要，保障信息的保密性，完整性和可用性；

- 网络安全（Network Security）指如何在技术层面，对那些实际运行的网络，确保分布在网络上的组织内部，组织与组织之间，以及组织与个人之间的信息安全；

- 互联网安全（Internet Security）关注在互联网（也就是使用TCP/IP协议连接起来的网络）如何保障可靠性和可用性；

- 关键基础设施保护（Critical Information Infrastructure Protection）保障那些提供或者关键基础设施运营者的网络系统的安全，关键基础设施运营商包括能源、通讯、饮用水系统等，关键基础设施保护确保这些系统和网络在面临各种类型的风险时能得到足够保护，有足够的弹性或者说防御能力；

- 网络安全（Cyber Security）又被称为网络空间的安全（Cyberspace Security）被定义为保障在网络空间上存储的信息的保密性、完整性和可用性，而网络空间存储信息的真实性、可核实性、不可抵赖性以及可靠性也可以纳入网络安全（Cyber Security）的框架内。

传统的定义与变化的现实

网络恐怖主义

- 内容传播与“独狼”袭击的威胁

黑客活动分子

- 跨境分布的能力与市场机制的结合

多目的的跨国活动网络

- 复合网络行动及其后果的失控

变化的现实提出新的要求

攻击-防御能力的拓展

- 向内容的延伸

主权的投射与管辖的边界

- 关键资源与边界

全网范围的共同指导原则

- 网络自由的实践与限度

网络空间博弈要求“灵活反应”

- 对网络安全的传统定义，促成网络安全战略更加接近“大规模报复”战略，新的多样化的威胁的兴起，暴露出此类安全战略的局限
- 构建“灵活反应”成为主要行为体面临的共同诉求

总体趋势

多主体的复杂互动

- 国家与非国家的自主性互动

多要素的动态重构

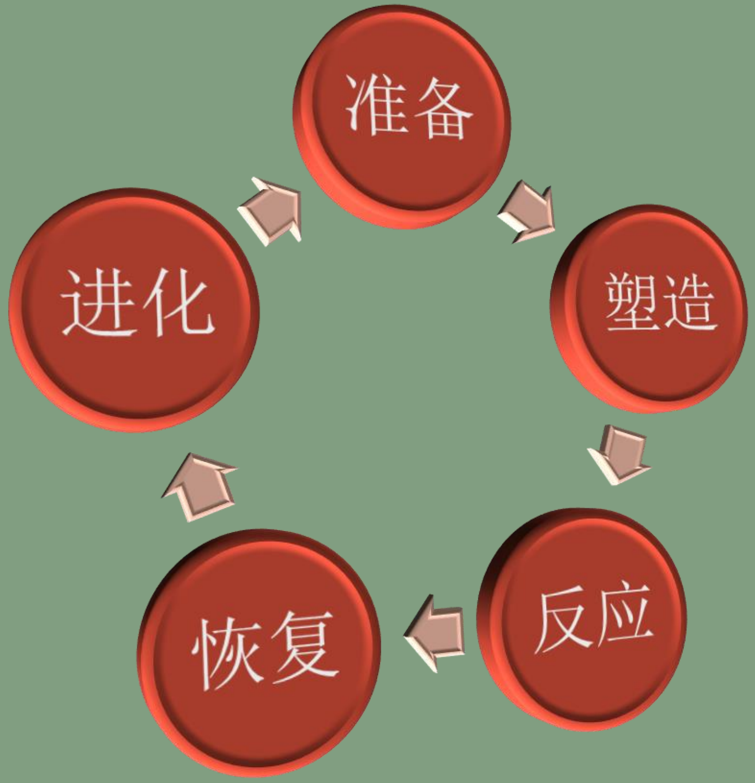
- 能力、意图、资源、行为的变化组合

体系与链的耦合

- 国际网络安全体系与国家网络安全能力链初现维形

网络安全能力链维形

- 形塑适合自身需求的网络安全能力链是当前全球网络空间安全博弈的本质与核心
- 网络安全能力链的基本功能性模块包括准备、塑造、反应、恢复、进化
- 全球网络空间的战略稳定取决于主要行为体之间网络安全能力链能否形成动态均衡



准备

塑造

反应

恢复

进化

中国的战略选择

网络安全战略流程再造

观念、机构与行为模式创新

以能力为导向的资源重新分配

谢谢！