网络安全视角下的犯罪

Understanding Cybercrime from the Perspective of Cybersecurity

鲁传颖·上海国际问题研究院

Lu Chuanying Shanghai Institutes For Internal Studies

网络犯罪问题的两种视角

two perspectives dealing with cybercrimes

犯罪视角

crimes

网络安全视角

cybersecurity

1、网络犯罪的基本特性

.

Defining features of cybercrimes

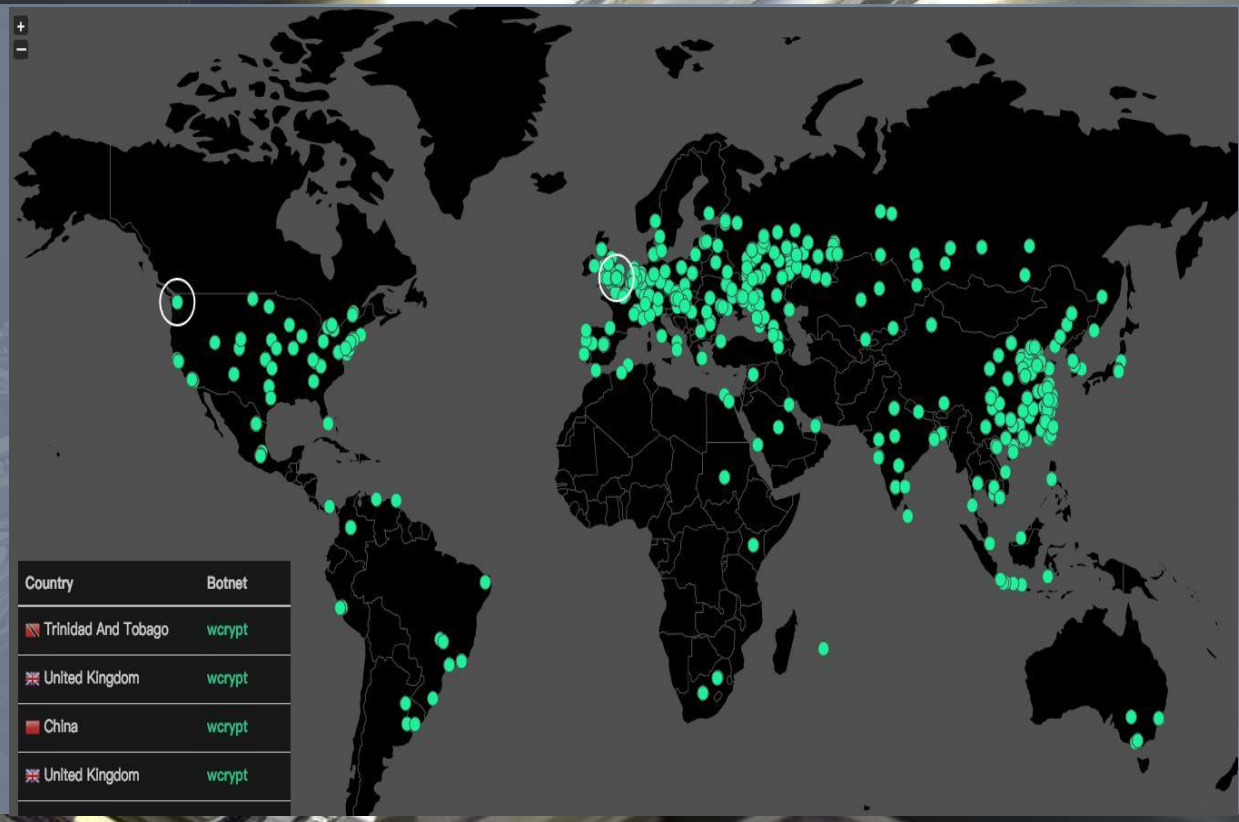
（1）犯罪的溯源难、主体不明确
Attribution is a big challenge

犯罪的溯源难、主体不明确。
可以是个人、犯罪集团、恐怖分子等。

Attribution is a big challenge.
Attackers, who could be individuals, criminal organizations, or terrorists, are hard to identify.

（2）技术的军民两用性 Duel Use of Cybersecurity Technology

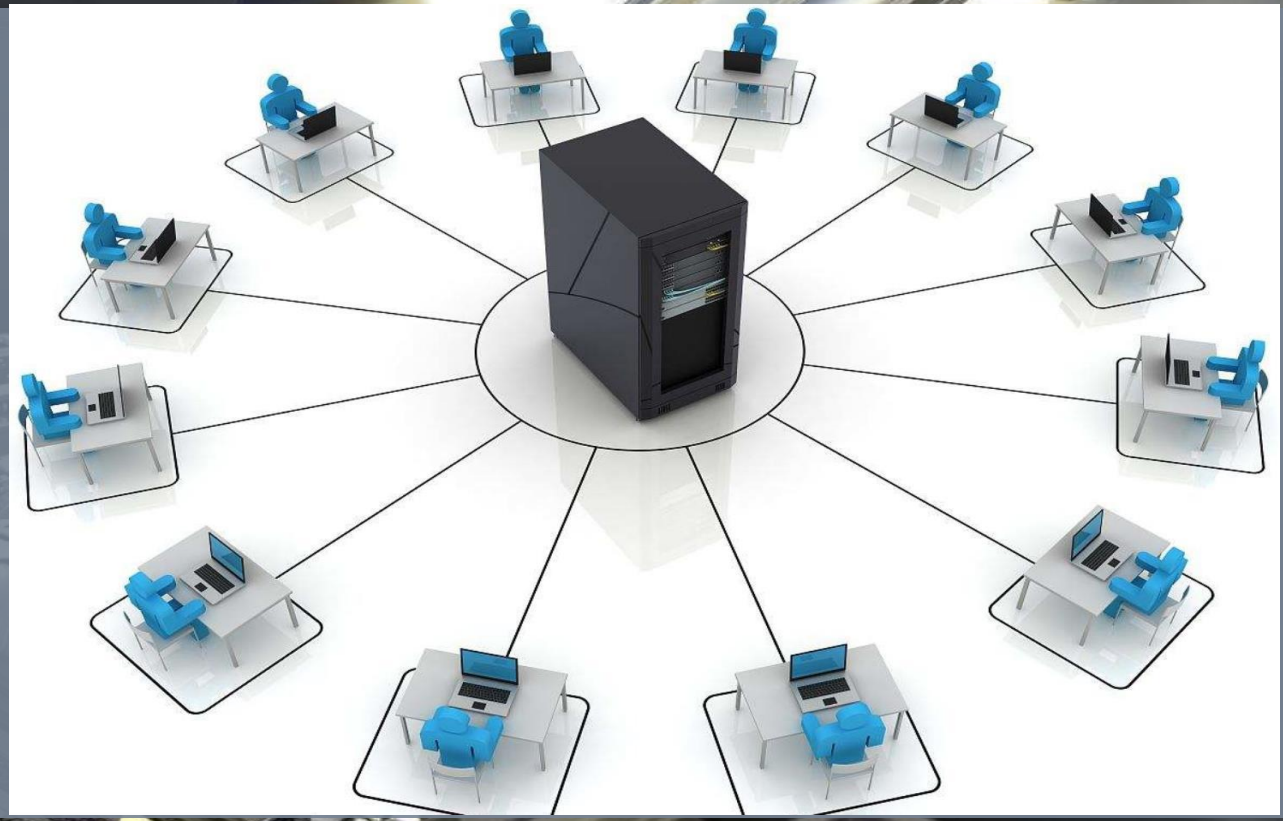
Take Wannacry as an example. Originally developed by NSA under the name “Eternal Blue”, it was later leaked into the dark net. Criminals used this tool and developed a ransomware called Wannacry.



（3）目标更加复杂 The objectives are even more complicated

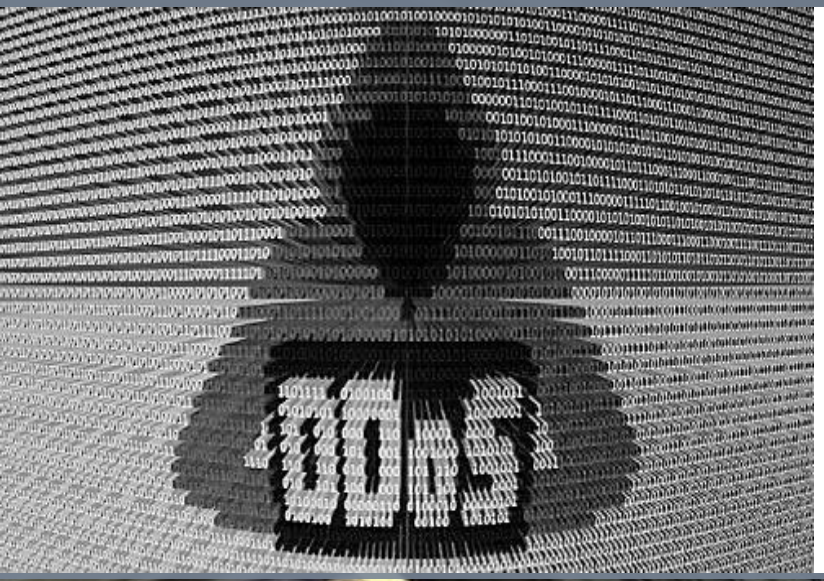
不仅仅是以经济为目标，开始把军事和政治和社会列入攻击目标。

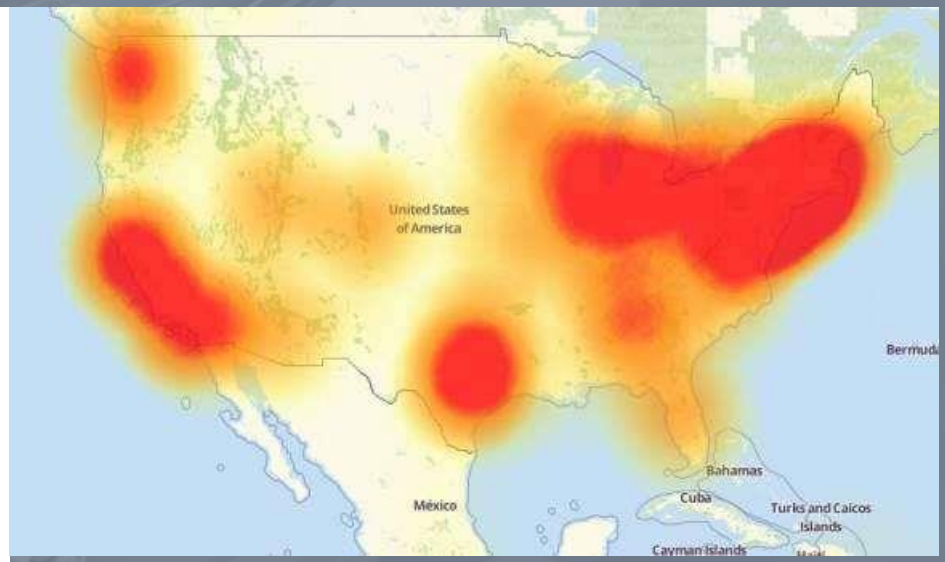
Cybercrimes are mostly committed, first and foremost, with economic targets in mind, but may, over time, turn to military, political and social targets for various reasons.



(4)网络犯罪的普遍性（低门槛、低成本）
The universality of cybercrime due to the low threshold and low cost

For example, Mirai, Japanese manga MIRAI NIKKI, was first designed as a game plug to attack MineCraft server and led to network breakdown in eastern U.S., which is widely known as the DYN event. Later, in order to acquit, the Mirai code was uploaded to the Internet and used for secondary attacks.





（5）网络犯罪的创新性
The innovative nature of cybercrime

Take Binance as an example. It is one kind of the bitcoin. The hackers control a large number of Binance accounts, and use the currency in the account to conduct bitcoin transactions in a very short time so as to manipulate the bitcoin price. Although hackers cannot cash it out, they obtained enormous benefits on the futures market by selling them in advance. Cracking down on this kind of cybercrime goes beyond the current law enforcement capabilities of the state.

2、网络安全国际治理中的打击网络犯罪问题

Combating cybercrime in the international cybersecurity governance

网络安全国际治理的进程和全景
Stakeholders in the international governance of cybersecurity

UN

IEG, UNGGE, WSIS, ITU

Technical and law enforcement agencies

CERT, Interpol

Regional Organizations

The European Commission, the SCO, the Arab League

Private Sector

Microsoft Digital Geneva, Munich Security Forum Trust Charter

3、国内执法与其他网络安全议题之间的关系

Relations between domestic law enforcement and other cybersecurity issues

（1）议题视角
What is at stake

关键基础设施保护、个人信息保护、军事情报。

critical infrastructure protection,
personal information protection,
military / intelligence.

（2）机构视角
Institutional design and operation

以美国为例-FBI\DHS\NSA都存在打击网络犯罪的职能，如何划分智能边界以及统筹协调。

Take the U.S. as an example. Different departments including FBI, DHS and NSA have the function of combating cybercrime. It is essential to define their functions and make coordination.

（3）非国家行为体视角
Engaging non-state actors

私营部门和公众在打击网络犯罪和隐私保护之间缺乏共识。

There is a lack of consensus between the public and private sectors on the fight against cybercrimes and privacy protection.

4、发现

Findings

（1）打击网络犯罪的国际网络安全困境
International cybersecurity dilemma in combating cybercrime

既要全面整体的看待打击网络犯罪问题与网络安全国际治理的关系，又要设立一定的防火墙避免政治化和其他议题的影响；

.

It is necessary to take a holistic view of the relationship between the fight against cybercrime and the international governance of cybersecurity. It is also necessary to set up a firewall to avoid politicization and the impacts of other issues.

（2）打击网络犯罪的国内网络安全困境
Domestic cybersecurity dilemma in combating cybercrime

需要厘清各个部门之间的关系，加强统筹协调，区分国家安全、网络犯罪、国防的议题，避免相互干扰；

It is essential to clearly define responsibilities between various departments, strengthen coordination, and distinguish issues of national security, cybercrime, and national defense from mutual interference.

（3）认知的挑战
Perception needs to be improved

对于政策制定者和决策者而言，如何全面的理解网络犯罪与网络安全问题、国际治理和国内治理之间的关系等复杂的关系，需要有长期、持续的关注和国际、国内经验的总结。

Policy makers and decision makers must pay sustained attention and review international and domestic experiences in order to fully understand the complex relations between cybercrime and cybersecurity, and the interplay between international and domestic governance.

5、建议

Suggestions

（1）在提高对网络犯罪问题的理解基础之上，积极推进建立全球应对网络犯罪的综合性国际法和机制.

国际性讨论的本身对于提升国际社会对于网络犯罪的意识和认识具有重要的意义；

The process of discussion itself played a critical role for international society to raise the awareness and perception of cybercrime and cybersecurity.

（2）专家组应当加强与联合国其他机制之间的互动，如UNGGE、WSIS，加强各个议题之间的协调.

The IEG and its secretariat should interact with other institutions on cyber issues, such as UNGGE and WSIS, to ensure better coordination on different issues.

（3）加大对其他区域性机制的统筹协调，如欧委会、上合、非盟、美洲国家组织。

The IEG and its secretariat should coordinate with other regional organizations on cybercrime issues, like COE, SCO, AU and OSA.

（4）国内层面
Domestic

国内层面，需要建立统筹协调机构，如白宫网络事务协调员或中国国家互联网信息办公室，有助于决策者更加全面理解和指导网络安全和网络犯罪问题。

Domestically, there needs to be a coordination body to supervise cybersecurity issues, such as the Whitehouse cybersecurity coordinator and the Cyberspace Administration of China, which helps decision makers better understand and tackle cybersecurity and cybercrime issues.