Research

Governance for Combating Cyber-attacks on Society

Masayuki Miyazaki
Senior Researcher, Technology Strategy Group, 3rd Research Department

Reports have indicated that the electoral outcomes of the U.S. and France presidential elections that were held last year and this year respectively were affected by the spread of disinformation, or fake news, on the Internet. “Cyber-attacks targeting society,” which spread false information through the Internet or other forms of media to mislead the judgment of people and public consensus as well as the actions of the public, have lately become a serious issue. In response to such attacks, many countries have begun to examine corresponding measures and new regulations as well as social systems are underway.

1. Growing Cyber-attacks on Society

In recent years, there has been a more widespread trend in the manipulation of public consensus through disinformation (fake news) by major terrorist organizations and the like to influence the politics and society of other countries and regions in order to steer public opinions in the direction that is deemed desirable by the attacker. During the U.S. presidential election in 2016, the spread of fake news using falsified emails of the Democratic Party undermined the trust of the people toward democracy with a decline in the support for Hillary Clinton, who was the presidential candidate for the Party.

Table 1 shows a comparison between the characteristics of conventional cyber-attacks on systems and those on society. While the main attackers are major professional organizations in both cases, they differ in the targets of the attacks as well as the damage that has been inflicted.

In particular, cyber-attacks on society can be characterized as being easy to perpetrate but difficult to safeguard against. There are a huge number of attacks through the spread of fake news on the Internet as these can be done easily at a low cost. Not only so, defense against the propagation of fake news is difficult with the instantaneous and extensive spread of information from one person to another via digital media.

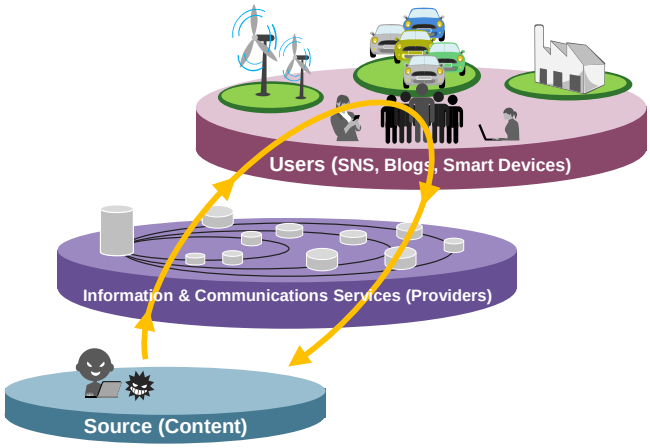
Table 1: Comparison of Cyber-attacks on Systems and Society

	Attack on Systems	Attack on Society
Attacker	Large organizations (nation, terrorist, etc.)	
Target	System malfunction or crash; illegal leak of information and data	Misjudgment, manipulation of public opinions, misleading the public
Propagation	From system to system	From person to person
Degree of Sophistication	High level of attack and defense	Easy and low cost to attack, difficult to defend
Damage	Economic losses	Political and economic chaos

Prepared by Hitachi Research Institute

2. Technical Issues Concerning Social Attacks and Countermeasures

Cyber-attacks on society that are propagated via information and communications networks are illustrated in Fig. 1. There is a tendency for malicious sources of information (content providers) to send out huge quantities of fake news from a large number of locations. Fake news that has been sent out is spread among individuals (users) within a short period of time via information and communications service providers. Users are then misled into taking actions based on their misjudgment due to the fake news, which in turn causes the repeated spread of disinformation among the users, thus resulting in social chaos.



Prepared by Hitachi Research Institute

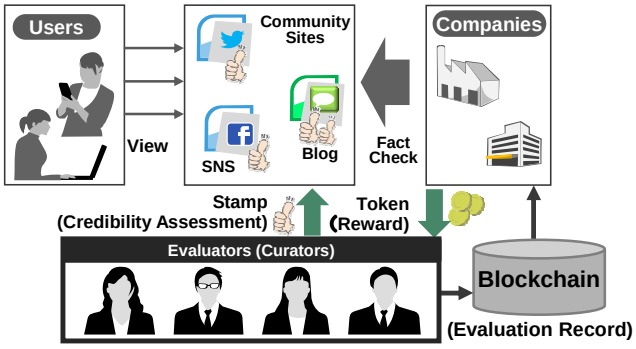
Fig. 1: Flow of Information during Cyber-attacks on Society

To combat such attacks on society, it is crucial to defend it from fake news and suppress chaos in public opinions. This necessitates construction of a system that restricts the propagation of information with a multi-tiered approach, such as by (1) identifying the source of the fake news and preventing its occurrence; (2) detecting and suppressing the spread of fake news on information and communications networks; (3) preventing misjudgment and spread of disinformation by the users. The objectives of and measures to address the respective issues are described below:

(1) Source of fake news: attackers send out information to major SNS operators by making use of or going through a large number of small providers so that they would not be tracked down. It is therefore important to trace back to the source while identifying such a characteristic by which the attacker employs a large number of providers and changes them frequently. While it is difficult to trace the origin as attacks are perpetrated from a wide range of locations by the attacker, who is also the source, it is possible to pin down the source if the provider is able to track the log for changes in the IP address of the server that is used for sending out the malicious information.

(2) Information and communications networks (service providers): unlike cyber-attacks on systems, those that target society do not result in the abnormal operation or failure of IT systems and the like, thus making it difficult for victims to recognize the attack in most cases. For this reason, it is necessary to forecast the possible distribution of fake news by monitoring the traffic volume on information and communications networks. A system that does not rely on the detection of system abnormalities and allows for the early determination of attacks is needed, such as one that detects and suppresses the circulation of fake news by utilizing the exchange points on networks to check for sudden changes in the traffic volume.

(3) Users: users with no malicious intent tend to spread fake news from one person to another without questioning the credibility of the information. SNS providers such as Facebook are in the process of introducing a “fact check” function on information that is posted on their web page. This is done by having a third-party organization verify information that is deemed dubious, but the amount of information that can be handled by such a manual task is limited. Meanwhile, Userfeeds, a Poland-based company, is currently considering a system that enables the credibility of information to be verified mutually among the users by creating a broad base of users known as “curators” whose role is to assess information (see Fig. 2). In other words, in addition to fact checks by the providers, it is also important to develop means that allow the credibility of information to be verified easily in order to effectively curb the extensive spread of fake news.



Prepared by Hitachi Research Institute

Fig. 2: Efforts by Userfeeds to Prevent Misjudgment and Spread of Fake News

3. Social Movements Aiming to Resolve the Issues

Measures from the social system’s perspective are also needed in relation to cyber-attacks on society, and many countries have already begun to introduce the necessary regulations or develop new systems.

3.1 Balancing between Strict Regulations and Freedom of Expression

In April 2017, the German government reached a cabinet decision to introduce a mandatory regulation to counter the spread of fake news, which requires SNS providers in the country to delete any fake news within 24 hours. However, enforcement of the regulation is still under review as some issues have been pointed out, such as the limitation it imposes on the freedom of expression and its accuracy in determining whether the information in question is authentic. Besides the criteria for judgment, other issues in relation to the balance between regulations and the freedom of expression include who to appoint as the regulating body.

For example, while this is implemented based on government regulations in Germany, the private sector is required to impose self-restrictions in the U.S. Other issues that have been raised include the need for a well-defined scope for regulating fake news. While the government in Japan has yet to review the necessary measures, the private sector has begun to engage actively in movements such as the Fact Check Initiative with discussions carried out on how fact checking can be done.

3.2 Widespread Sharing of Incidental Information between Public and Private Sectors

A system for sharing incidental information between the public and private sectors is necessary as part of the measures to battle cyber-attacks. In Japan, although CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) by ISAC (Information Sharing and Analysis Center) and NISC (National Center of Incident Readiness and Strategy for Cybersecurity) are responsible for countering cyber-attacks on important infrastructures in the respective infrastructure industries within the country, they are only available to social infrastructure business operators. Meanwhile, cyber-attacks on society are mostly dealt with by information service providers. In order to enhance the capability for handling the growing number of cyber-attacks on society, there needs to be a system that allows not only sharing of information between the operators of important infrastructures and the government, but also one that takes into consideration cooperation with information service providers.

4. Issues for Future Research

While a wide variety of measures to combat cyber-attacks on society are currently under consideration, many issues remain to be addressed. In order to prevent political, economic or social chaos caused by fake news, it is of primary importance to establish cyber governance with the development of new technologies and systems.

Hitachi Research Institute will strive to contribute to the achievement of cyber governance by continuing to promote the following studies.

(1) The role of the social system to regulate fake news and share information with the trends of other countries taken into consideration
(2) The measures to adopt in Japan and how the private sector can make contributions through their business