Li, Tian; Fei, Fang; Yanqing, Hong

**Conference Paper**

# Governing Social Media Platforms As Critical Information Infrastructures

22nd Biennial Conference of the International Telecommunications Society (ITS): "Beyond the Boundaries: Challenges for Business, Policy and Society", Seoul, Korea, 24th-27th June, 2018

**Provided in Cooperation with:**

International Telecommunications Society (ITS)

# Governing Social Media Platforms As Critical Information Infrastructures

Tian Li, School of New Media, Peking University
Fang Fei, School of New Media, Peking University
Hong Yanqing, School of New Media, Peking University

## 1. Introduction

On July 11th, 2017, when the Cyberspace Administration of China (CAC), the executive office of the Central Leading Group of Cyberspace Affairs[1], issued the draft *Regulation on the Protection of the Security of Critical Information Infrastructure* (hereafter as *the Regulation* ) under the mandate of the *Cybersecurity Law* of China[2] for public comment, there were immediate outcries among the western commentators.

One of the major issues that particularly raised eyebrows was the unclear scope of the Critical Information Infrastructure (CII) in *the Regulation.* Article 18 of *the Regulation* defines the CII as *"*network facilities and information which are operated and managed by the Entities (danwei) listed below, which once having suffered destruction, loss of functionality or leakage of data, could severely endanger national security, the national economy and the people's livelihood and the public interest*"*.[3] And "Information networks such as telecommunications networks, television broadcast networks and the Internet, and Entities (danwei) which provide cloud computing, big data and other large-scale public information network services" is explicitly included to be as such entities.[4]

This vague wording implicates major social media platforms (hereafter as dominant SMPs) that operates in China, such as Weibo[5], which by definition is not a "news organization", but nonetheless could be classified as "large-scale

---

[1] President XI Jinping assumes the head of this central leading group, which was established in the early 2014. http://www.cac.gov.cn/2014-02/27/c_133148354.htm

[2] Article 31 of the *Cybersecurity Law*: "The state shall, based on the rules for graded protection of cybersecurity, focus on protecting the critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs and the critical information infrastructure that will result in serious damage to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage. The specific scope of critical information infrastructure and security protection measures shall be developed by the State Council. The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system."

[3] the draft Regulation on the Protection of the Security of Critical Information Infrastructure, http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

[4] The other four categories that are explicitly mentioned in the *draft Regulation* are: 1) Governmental agencies and Entities (danwei) which are in industry sectors and fields such as energy, finance, transportation, water conservancy, hygiene and medical care, education, social insurance, environmental protection, and public utilities; 2) R&D and manufacturing Entities (danwei) which are in industry sectors and fields such as science and technology for national defense, large equipment manufacturing, chemicals, and food and drug; 3) News organizations (danwei), such as broadcasting stations, television stations and news agencies; and 4) Other critical organizations (danwei).

[5] The Chinese equivalent of Twitter. By the end of September this year, the number of monthly active users (MAU) and daily active users (DAU) on Weibo reached 376 million and 165 million respectively. In terms of financials, their total revenue reached nearly 2.13 billion RMB, with annual growth of 80%. See the its financial report for Q3 2017. https://chozan.co/2017/11/16/wechat-data-weibo-data-q3-2017/

public information network services". Thus, having already been subject to heavy regulation in terms of (user-generated) content[6], the SMPs in China with user-base exceeding a certain number to be qualified as large-scale, would be additionally regulated as CII, which entails enhanced security obligations, such as implementation of a series of mandated management and technical measures (Article 23), establishing inside the organization of specialized network security management departments and persons who bear responsibility for network security management (Article 24), launching network security inspection and emergency response drills (Article 25), and so on. In addition, once being classified as CII, the SMPs would have to store the personal information and the so-called important data within China by default[7]. And the operation and maintenance of the SMPs should be carried out within the territory of China as well.[8] Therefore, SMPs operating in China and bearing the label of CII would have to place their servers and store data within the country under the CII regime, an requirement which would effectively exclude the presence in China of foreign SMPs that predominantly rely on the model of one unified platform for the users across the world.

One would thus take the *Cybersecurity Law* and *the Regulation* as further evidence of Chinese Government's hardened control on the freedom of expression of Chinese people. This impression seems to be again corroborated by the recent investigations announced by CAC which targeted on Tencent, Baidu and Sina Weibo for their potential violation of the *Cybersecurity Law*, particularly their failures to control users who have posted inappropriate content related to violence, terror, pornography, fake news, etc.[9]

All of these could be easily interpreted as the inclusion of SMPs as CII is the new cover for China to tighten its grip on day-to-day communications and information transmission for its citizens. Under this interpretation, citing cybersecurity concerns faced by SMPs and demanding corresponding security measures are all just to serve the true purpose of content control, all of which are actually renewed attempts of the Chinese Government to justify its strict limitation on the freedom of expression.

However, does this interpretation or theory account for everything?

For the traditional regulatory framework for SMPs, emphasis has been put on the implications of the rises of SMPs on the distribution of political power within a polity. Take an interesting debate that recently happened in the US as example. Some have argued that SMPs are *proprietary domain*, where owners of such

---

[6] A point which will be elaborated later.

[7] Article 29 Personal information and important data which an operator collects or generates in the course of its operations within the territory of the People's Republic of China should be stored within that territory. When there is a veritable need to provide it overseas for reasons of business necessity, they should conduct an assessment in accordance with the Measures for the Security Assessment of Personal Information and Important Data Leaving the Country. Where law or administrative regulations provide otherwise, such provisions shall prevail.

[8] Article 34 The operation and maintenance of critical information infrastructure should be carried out within the territory of China. When there is a veritable need to carry out remote overseas maintenance for reasons of business necessity, they should report it in advance to the national industry regulatory or supervisory departments and to the public security department of the State Council.

[9] http://www.cac.gov.cn/2017-08/11/c_1121467425.htm

proprietary domain, like Facebook, have primary authority to regulate what can or cannot be said and done. Whereas some have regarded SMPs are *public forum*, like parks, streets and town halls where speech and debates happen. Hence "public officials may not 'block' their constituents on social media".[10] This debate mostly concerns about the nature of SMPs in the domestic political system and decision-making. It has not yet been settled, and the continence of it still holds valuable meanings.

In the meanwhile, a new reality has emerged. With incoming waves of fake news or disinformation campaigns or information warfare from enemy countries on the eve of major political elections in the western countries, and increasingly influence from the domestic and foreign terrorist groups to radicalize and recruit young people online across the world, SMPs have gained more and more traction in the national security related debates worldwide. A different governing framework for the dominant SMPs may be warranted in the context of increasing securitization of information, or the emerging information warfare among states.

With this in mind, this essay seeks to address, could the dominant SMPs be governed as the critical information infrastructures (hereafter CII)? A directly related question is, are current and proposed regulations on SMPs both inside and outside China exhibiting strong correlations to, or simply converging on, the regulatory approaches that are traditionally adopted in the domain of the CII protection? If the answers to both questions are yes, then we are most likely to witness a dramatic regulation regime changes regarding SMPs in the near future. Furthermore, the governing framework of SMPs as political apparatus in a polity will entangle with this new governing framework that sees SMPs as security apparatus for national security and stability, and causes great new uncertainties for the [cross-border] operation of the dominant SMPs.

## 2. Current regulatory regime for SMPs in China

### 2.1 Content layer

The first order of the CAC is about internet news information services. On May 2, 2017, the CAC issued the long-awaited *Provisions for the Administration of Internet News Information Services* (hereafter as the *Provisions*)[11], replacing *the 2005 Provisions for the Administration of Internet News Information Services*[12] issued by State Council Information Office and Ministry of Information Industry. *The Provisions* effectively established the regulatory framework for all the internet news information services in China. Here are its major requirements.

---

[10] Kieren McCarthy, Blocking peeps on social media? That's a paddlin' for governors, senators, house reps. US officials' online spaces – a public forum or private haven? 10 Aug 2017, https://www.theregister.co.uk/2017/08/10/governors_senators_and_house_reps_suedwarned_over_social_media_blocking/ See also Thomas Wheatley, Why social media is not a public forum, Washington Post, August 4 2017, https://www.washingtonpost.com/blogs/all-opinions-are-local/wp/2017/08/04/why-social-media-is-not-a-public-forum/?utm_term=.d92ad137ed49

[11] http://www.cac.gov.cn/2017-05/02/c_1120902760.htm

[12] http://www.gov.cn/flfg/2005-09/29/content_73270.htm

First. “news information includes the reports and comments on political, economic, military, diplomatic and other social and public affairs, and the reports and comments on relevant social emergencies.”[13] So SMPs are necessarily involved in the provision of news information according to the *Provisions.*

Second, Article 5 of the *Provisions* requires that “to provide Internet news information services through Internet websites, apps, forums, blogs, microblogs, public accounts, instant communication tools, Internet broadcast and other forms to the public, a permit for Internet news information services shall be obtained, and activities of providing Internet news information services without a permit or beyond the scope permitted shall be prohibited.”[14] Therefore, to be a SMPs where users can have meaningful discussion on matters beyond their personal lives would need a permit from the State.

Third, the *Provisions* divides entities that are providing internet news information services into three categories:

> I. services of collecting, editing, producing and releasing Internet news information: the services to collect, edit, produce and release news information.
> II. Services of reposting news information means the services to select, edit and release the news information that has already been published by other entities.
> III. Services of providing a platform to disseminate news information means services to provide users with a platform for them to disseminate news information.[15]

And Article 4 further requires that “whoever is approved to provide services of collecting, editing and releasing Internet news information may provide services of reposting Internet news information at the same time. If any entity that is approved to provide services of providing a platform to disseminate Internet news information plans to provide the services of collecting, editing, releasing and reposting news information at the same time, it shall obtain the permit for collecting, editing, releasing and reposting Internet news information in accordance with the law.”[16] Essentially, the *Provisions* requires SMPs in China would have to obtain permit for services of reposting news information (category II) and services of providing a platform to disseminate news information (category III).

Permit for category I is set with very hign bar. Article 6 of *Provisions* requires that the an applicant for category I permit shall be a news entity (including an entity in which it holds controlling shares) or an entity under the charge of the news publicity department.[17] This particular requirement effectively prohibits private sector to apply for this permit. In this way, the State maintains its monopoly on the news production, where private sectors could engage in

---

[13] Article 2. http://www.cac.gov.cn/2017-05/02/c_1120902760.htm
[14] Ibid.
[15] Article 5, http://www.cac.gov.cn/2017-05/02/c_1120902760.htm
[16] Article 4, http://www.cac.gov.cn/2017-05/02/c_1120902760.htm
[17] Article 6, http://www.cac.gov.cn/2017-05/02/c_1120902760.htm

reposting and disseminating news stories with users' comments. This is further strengthened by Article 7 of the Provisions.[18]

Fourth, the qualifications for permits that are relevant for SMPs.

**a. Organizational Qualifications**

The SMP should be a legal person legally formed within the territory of the People's Republic of China. No organization may form an entity providing Internet news information services in the form of a Chinese-foreign equity joint venture, Chinese-foreign cooperative joint venture or foreign-funded enterprise.

During the application, the SMP have to provide the following materials[19]:

(1) The equity structure chart, including the names of shareholders, shareholding ratio, form of capital contribution, time of capital contribution, and other information. If a shareholder is a non-natural-person subject, the natural person, public institution and wholly state-owned company must be traced level by level, and an explanation on the actual controller shall also be given. The entity's official seal and signature of the legal representative shall be affixed to the equity structure chart.
(2) Certification materials on shareholders. If the shareholder is a natural person, his or her identity certification materials must be provided. If the shareholder is a non-natural-person subject, materials on its name, organizational form and legal representative, among others, must be provided.

(3) The company's bylaws, including the company's bylaws and resolutions on previous amendments.
(4) A letter of commitment on no foreign investment. The applicant shall issue a written commitment that no shareholder listed in the equity structure chart has foreign investment.
(5) Opinions issued by a professional agency. A written certificate issued by a law firm or an accounting firm to prove the truthfulness, accuracy and integrity of the aforesaid equity materials, including a capital verification report, legal opinion and other materials.

**b. Qualifications for editorial team**

The SMP is required to have a chief editor, who should be a Chinese citizen. For permit application, the SMP needs to provide certificate proving that its principal person in charge or chief editor is a Chinese citizen, including a photocopy of the identity card of its principal person in charge or chief editor, among others.

The SMP should also have full-time news editors, content reviewers and technical

---

[18] Article 7: " No organization may form any Sino-foreign equity joint venture, Sino-foreign cooperative joint venture or foreign-funded enterprise to provide Internet news information services. An Internet news information service entity that cooperates with any domestic or foreign Sino-foreign equity joint venture, Sino-foreign cooperative joint venture and foreign-funded enterprise on businesses involving Internet news information services shall report to the Cyberspace Administration of China for safety assessment."
[19] Detailed Rules for the Licensed Management of Internet News Information Services, Article 5 and 6, http://www.cac.gov.cn/2017-05/22/c_1121015789.htm

support specialists suitable for its services. In application, the State would examine: qualifications of its full-time news editors, content reviewers and technical support specialists, including the basic information on relevant staff members, their press cards uniformly issued by the State Administration of Press, Publication, Radio, Film and Television, practicing certificate of the news entity, relevant training and assessment certificates and other materials. The number of relevant staff members shall be suitable for the services which the applicant provides.[20]

### c. Internal management rules

The SMP should have internal management rules for Internet news information services, including the rules for the chief editor of the website, and the rules for the education, training and examination of employees, among others.

### d. Technical measures for content control

The followings are required from applicant: information security management rules and technical support measures, including the rules for information release and examination, rules for the patrol inspection of public information, rules for emergency response, and rules for protecting users' personal information, among others, and the relevant technical support measures.[21]

### e. Security assessment

Finally, A report on the security assessment of Internet news information services is needed. It is a safety assessment report issued by the relevant department or relevant qualified institution for the applicant's information security management rules and technical support measures.[22] Apparently, this assessment would take into account all the elements mentioned above. But what framework would this assessment would make reference to is not that clear. Another regulation issued by the CAC may shed some lights on this aspect.

On Dec. 1, 2017, the CAC issued the Provisions on the Administration of the Safety Assessment of New Technologies and Applications for Internet News Information Services.[23] Although this assessment aims at the so-called new technologies and new application, the requirements in this particular rule are very relevant for the security assessment mandated in application of permit.

For this rule, the “safety assessment of new technologies and applications for Internet news information services” (hereinafter referred to as the “safety assessment of new technologies and applications”) means the activities of determining the assessment grade, according to the nature of news media and public opinion, or capability of social mobilization of new technologies and

---

[20] For additional requirements for personnel, see Measures for the Administration of Content Management Practitioners in Internet News Information Service Providers, http://www.cac.gov.cn/2017-10/30/c_1121877917.htm

[21] Detailed Rules for the Licensed Management of Internet News Information Services, http://www.cac.gov.cn/2017-05/22/c_1121015789.htm

[22] Ibid.

[23] http://www.cac.gov.cn/2017-10/30/c_1121878049.htm

applications, as well as the safety risks of information content arising therefrom, and conducting an examination and assessment of the information safety management system and technical support measures thereof.[24]

In either self-assessment or regulatory assessment, the SMP should firstly describe:

(1) Service programs (including service items, service method, business form and service scope).
(2) The major functions of products (services), major business processes and the composition of the system (with a brief introduction to the types, brands, versions and deployment locations of major software and hardware systems, among others).
(3) The supporting information safety management rules and technical support measures for the products (services).

Then SMP should assess the extent to which the service programs' scale of users, functional attributes, modes of technical realization or allocation of basic resources could lead to a major change in the nature of news media or public opinion or capability of social mobilization.[25]

The bottom line is that SMPs shall establish and improve the information safety management system and have ***safe and controllable technical support measures***, which would enable SMPs from distributing or disseminating any information content prohibited by any law or administrative regulation.[26]

### 2.2 Technical Layer

If *the Regulation* were to enact in current form, the SMPs with users exceeding certain threshold would be enrolled in state-mandated CII protection regime. Below provides a snapshot of what CII protection regime would look like:

Firstly, the SMPs have to take on a series of security obligation for their systems and data (irrespective of content).[27]

Additionally, according to *the Regulation*, the State would establish implement the requirements of the General Secretary XI on the establishment of a "24-hour all-round cybersecurity situational awarness system". Articles 36 and 37 of Chapter 6 of *the Regulation*, "Monitoring, Early Warning, Emergency Handling, and Assessment", respectively, require national cybersecurity and informatization departments and national industry supervisory and regulatory bodies to establish a national level, and industry and sectoral level monitoring and early warning systems, and carry out the cybersecurity information collection, analysis and investigation and notification work in a timely manner.

In addition, Article 38 also requires the national cybersecurity and informatization

---

[24] Ibid.
[25] Article 7, http://www.cac.gov.cn/2017-10/30/c_1121878049.htm
[26] Article 3, http://www.cac.gov.cn/2017-10/30/c_1121878049.htm
[27] See the Introduction of this article.

departments to coordinate the establishment of a cybersecurity information sharing mechanism between the government, enterprises, and research institutions. *The Regulation* through the establishment of a cross-public and private sector, rich layered, interconnected cybersecurity information sharing network, will ultimately achieve the comprehensive use of all aspects of data resources, and enable better awareness of the effectiveness of the cybersecurity risk situation.

Article 40 of *the Regulation* requires the national industrial supervisory and regulatory authorities to regularly organize random inspections of industry, sectoral, and critical information infrastructure security risks and how operators are fulfilling their security obligations. Unlike the previous "compliance tick" security inspection and checks, the inspection envisioned by the Regulations has been essentially different. Now industry regulatory or supervisory departments in their daily work not only grasp the cybersecurity risk situation of the industry and sector, but also through the monitoring and early warning system established by national cybersecurity and informatization departments, grasp the national cybersecurity risks. Therefore with this risk understandings and knowledge, during security checks and testing, it will be possible to effectively guide and urge the operators to find the problem in time and put forward security measures commensurate with the current risk situation. Therefore, through the regular random inspections by the supervisory and regulatory departments, the perception of risk can become inputs to decision-makings in security protection, and changes in the external situation can be matched by the new security requirements, and then implemented.

Article 39 of the Regulations provides that national cybersecurity and informatization departments guide the relevant departments to organize cross-industry, cross-regional cybersecurity emergency drills, while industry supervisories or regulators regularly organize exercises to enhance industry and sector’s cybersecurity response and disaster recovery capabilities. In the same way, with a comprehensive grasp of the momentary changes in the risk of the situation based on the development of emergency drills, no doubt it will, to greatest extent, avoid a "racking your brain" situation, making the exercises have a direct relevance and timeliness to the realities.

Combining these three aspects above, *the Regulation* will establish a three-dimensional, cross-network security situational awareness system for critical information infrastructure nationwide, and through government departments spot checks, tests, exercises and other actions, real-time risk perception and analysis will be translated into dynamic, targeted security requirements.

### 2.3 Summary

From the analysis above, it is apparent that dominant SMPs in China are under heavy regulation, all the way from the physical infrastructures, to algorithm and data, to service model, to the editorial and technical measures to discover and stop the transmission of illegal contents, and finally to the owner-ships of the SMPs. Practically speaking, every basic elements in SMPs are subject to

state-mandated requirement.

Would this all necessary if SMPs would only play a role in the distribution of political power within a polity? The next section this article would argue that the regulatory regime for SMPs in China are largely rooted in the National Security perspective.

## 3. Policy Rationales behind China's Regulatory Approach to SMPs

The internet services is a double-edged sword. While bringing conveniences to people, social media platforms also helps in generating many potential hazards--from trivial issues as disseminating false information, to serious problems as being maliciously employed by terrorist groups--hence exerting a damaging impact on national security.

The negative influences exerted upon national security by social media platforms are of the following three aspects: the divergence of social consensus; the reveal of the invisible society and the transfer of communication power.

### 3.1 The divergence of social consensus

National security includes many connotations, such as the citizen's security, homeland security,political security, etc. Among these, ideological security is a crucial composition of political security, therefore a necessary part of national security. The Infringement upon one nation's mainstream ideology will necessarily result in the chaos of the national political belief, political values, and ethical standards, as well as societal risks, hence the ultimate damage upon national security. The threat exerted upon national security by SMPs lies in the hence precarious role of the mainstream ideology, and the potential risk of social consensus being diverged.

The relatively low requirement in content filtering mechanism of social media inevitably results in the vast amounts of information existing on the SMPs. Due to the high efficiency feature of communication, the sharing feature, the congregating feature, as well as the integrative feature of the social network communication, it is quite easy for the negative information be passed on along the networks as in the process of interpersonal communication and group communication, or even in mass communication, hence exert certain influences upon people's values, beliefs--the result being a divergence from their original personal ideology.

The collaborative information filtering of the social media also contributes to the individual's ideology divergence from the mainstream ideology. According to the collaborative information filtering algorithm, the SMPs tend to recommend

contents which users might be interested in or be personally related to. Over time, the range of the information that are passed on to users are strict and limited, hence the deeper divergence of society's mutual understanding. As in the groups' layer, we could see that, the polymerizability of the internet helps to generate a vast amount of virtual groups, these groups have certain exclusivity: in these groups, ideas that are similar to the groups' mainstream ideology are adopted; on the other hand, ideas that are different from the groups' mainstream ideology are rejected. Group polarization phenomenon often occurs. It is difficult for mainstream ideology of one country to reach into these groups, which have quite different ideologies from the mainstream ideology of the country--in this way, gradually social consensus could be divided into various ideology islands. In extreme cases as those groups that have pernicious influences on the society(terrorist groups, reactionary groups) assemble, the impact upon the mainstream ideology in the society and national security will be particularly apparent.

Besides, hostile forces' using social media to infiltrate further aggravated the divergence of social consensus. Take ISIS as an example, in 2015, terrorists from ISIS have opened a large amount of social media accounts, in order to publish terrorist' speech and videos, and to vastly propagate to bewitch young people in the West to join the 'Jihad'--which result in many Westerners attending the Jihad in Syria, and even initiate terrorist activities in their home countries. Meanwhile, in the process of the worldwide power combats, social media have always been employed as the channel for cultural values' output and attack upon the native ideology.

### 3.2 the reveal of the invisible society

In the past where there is no social media or even the internet, the main channel of communication--such as television channels, radio broadcasting companies, newspaper offices are basically controlled by or in close collaboration with the government, hence the direction of information passage is unidirectional, the content of information represents mainly the national interest and ruling class' s will, therefore the extent of exhibiting the whole society being limited. However, the appearance of social media has broaden the channel of communication, made individual participating the society's discussion more convenient, the two parties of the government and citizens using social media to interact becoming more common, and the whole society's participating in online discussion has made the contents accumulated on SMPs rich enough to reflex a quite broad range of, and an intense degree of the society. Naturally, This all-inclusive mirror of the society on the SMPs includes every aspect of the society, which means something as secret and almost invisible in reality, which once posted online, might have a perpetual and huge effect upon the real world. Hillary Clinton's 'Email Gate'..... these are of typical examples. The high efficiency in communication on the SMPs

can make the tension generated from one trivial, individual event inflammatory and even transforming into a storm on the internet, hence exerting an effect upon the real world. A precise example would be the Jasmine Revolution, which originates from a single event of one youth's self-immolation, which started the warfare in North-Africa and the Arabian world.

This ability of social media--to the government of one country--could been seen as a challenge towards their mode and competence of governance; on the other hand, to forces, parties outside the country, it provides a reveal of the society's weakness and points for infiltration to take place. Social media has exposed the invisible society to foreign forces, enabling them chances to take advantage. For foreign hostile forces, they could intentionally stir up some topics, instigate dissatisfaction in the society, causes domestic conflicts, bring damages to social consensus, in the end harm national security. In an era of active and intensified international contacts and combats, such examples of revealing the invisible society on SMPs resulting in other countries' meddling with the internal business are abundant. There are already certain speculations by some mainstream Western media that the 58th U.S Presidential Campaign is in effect manipulated by Russia.[28] In China, behind the Occupy Central with Love and Peace Movement, there are also traces of foreign forces that have intervened.[29]

### 3.3 the transfer of communication power

In the WEB2.0 era, concentration of power have become rather difficult and even impossible: the government's communication power through the channel of traditional media entities is weakened. The power of communication is no longer exclusively owned by the government: transnational corporations, criminal groups, terrorist organizations, even individual citizens--by employing the SMPs, these parties can share the power of communication together with the government. The birth of the internet and new media have challenged and even taken up the mainstream and dominant position of traditional media originally controlled by the government, hence the power to influence the 'gate-keeper' 's voice weakened, and individual citizen's voice amplified, some public events-if not being dealt with care--might bring forth a storm of public opinion online, therefore triggers group actions: the Tunisian Revolution, Arabian Spring--these events are all first started on the SMPs. The magnification of individual's communication power, in the long run, could exert certain influences upon the political power of one government, and cause various social problems, breed many social risks--but this trend is in effect inevitable, and it helps to examine

---

[28] Gordan Corera. Can US Election Hack be Traced to Russia? http://www.bbc.com/news/world-us-canada-38370630 2016/12/22. Access date 2017/12/25.

[29] Simon Denyer. Hong Kong Activists Test China's Red Lines Over Election With Occupy Central Campaign. https://www.washingtonpost.com/world/hong-kong-activists-test-chinas-red-lines-over-election-with-occupy-central-campaign/2013/11/28/07a61478-4ad7-11e3-bf60-c1ca136ae14a_story.html?utm_term=.8b35fd8097f3. 2013/11/28. Access date: 2017/12/25.

and challenge the government's mode and competence of governance. However, the magnification of terrorist organizations', criminal groups' communication power will have a bad influence upon the national security. For instance, the social media strategy applied by ISIS has bewitched many Western people, the consequence being these Western countries still suffering from terrorist attack launched by their own citizens who have been brainwashed.

Furthermore, the transfer of the communication power also manifests as the transfer from the system's empowerment to the technology's empowerment. As a matter of fact, internet sovereignty encompasses the realm of geographical national borders, the companies that provide internet services are mainly based in Western countries, many countries have lost their voices in Cyberspace--and this makes these countries themselves quite passive in the process of internet communication: they are merely the receiver in the process, and are not in control of the communication channels and information contents. The countries are not in effect control of the social media companies, hence they are not in control of the technology, therefore lacking an overall control of the whole communication framework.

Compared with the magnification of individual's communication power, the communication power transfer brought about by technology might generate higher risks. SMPs are prone to become tools employed by foreign threats, while providing conveniences to people with the means of communication, SMPs also provide chances for foreign hostile forces' infiltration and attacks. The government's communication power is being partially eaten up by social media companies: technology's empowerment transcends system's empowerment, the country's political power is challenged--hence national security is at risk.

Now we could see that with the above three layers of social media platforms' negative influences upon one country(the divergence of social consensus, the reveal of the invisible society and the transfer of communication power), it is justified enough to say that SMPs' influences upon one country are so indispensable, that the incapacity or destruction of such systems would have a debilitating impact on nation security and societal functions, hence reasonable to conclude that SMPs could be treated as CII, therefore deserving CII protection.

## 4. Is China that special?

In the conference of Cyber 2017 hosted by the Chatham House in London, one senior UK national security official asked the audience the following:

> The public opinion of UK is mostly formed in SMPs such as Facebook and Twitter, both of which are US companies headquartered in the US. Therefore the British government has little jurisdiction on them. But the ways they compress fake news, combat disinformation campaign, take downs illegal

contents and the results thereof have tremendous impact on UK's national security. So ladies and gentlemen in the room, what should I do?

The question raised by this senior official actually reflects growing concerns of many western countries when they find themselves in the so-called information warfare. In this new narrative, Russia, Iran and China are said to excel in the launching this kind of warfare by employing many tools, one of them being the SMPs.

Take Russia. In the portrait of the media, not only Russia has interfered with the 2016 presidential election of the US, it has launched continuous disinformation campaigns by employing the SMPs to influence the politics, economics and social institutions of countries along its European periphery with Ukraine as the most evident case.[30] It is said that "while many Americans have just awoken to the world of disinformation — sometimes known as 'fake news' — in the recent presidential election, Moscow's efforts date back decades and have become increasingly prominent over the past decade as techniques have been updated for the digital age."[31]

Take Iran. According to the reporting, Supreme Leader of Iran Ali Khamenei has called for Iran to increase its ability to defend against and wage what he called "soft war".[32] "Through a central office, the Islamic Republic coordinates a web of organizations involved in cyberattacks and information campaigns. Goals include the promulgation of Shi'a Islam and narratives about current events that suit Tehran's perspective".[33]

Let us now look at the Emerging regulatory trends for the SMPs in the Developed World.

### 4.1 US

Up till this point, the regulatory trend for the SMPs in the US, if there is any, presents as some limited administrative moves(from the legislative angle this is unformed, but from the government's administrative angle, there are already some concrete moves) in regarding the Election system as CI, specifically: to treat the social media platforms as one element of the states' sixteen critical infrastructures.

According to one article titled 'Should Social Media be Considered Part of Critical Infrastructure?': 'Russia interfered in the U.S. 2016 election, but did not materially affect it. That is the public belief of the U.S. intelligence community. It

---

[30] Bethania Palma, Russia's Neighbor Ukraine Besieged by 'Fake News' and Hacking Years Before United States, Jun 27th, 2017, http://www.snopes.com/2017/06/27/ukraine-fake-news-hacking/

[31] Vera Zakem, How Russia's Disinformation Campaign Could Extend Its Tentacles, January 6, 2017, http://www.npr.org/2017/01/06/508032496/how-russias-disinformation-campaign-could-extend-its-tentacles

[32] Arash Karami, Khamenei warns of 'soft war' between Iran, US, April 20, 2016, http://www.al-monitor.com/pulse/originals/2016/04/khamenei-hezbollah-condemn-oic-statement-saudi.html#ixzz4pXELy95i

[33] Phillip Lohaus, A Vulnerable Castle in Cyberspace: America needs to embrace the 'information warfare' mindset. Aug. 11, 2017, https://www.usnews.com/opinion/world-report/articles/2017-08-11/america-must-make-information-warfare-part-of-its-cybersecurity-plan

is a serious accusation and has prompted calls for additions to the official 16 critical infrastructure categories. One idea is that 'national elections' should be included. A second, less obviously, is that social media should be categorized as a critical industry. The reason for the latter is relatively simple: social media as a communications platform is being widely used by adversary organizations and nations to disseminate their own propaganda. This ranges from ISIS using it as a recruitment platform, to armies of Russian state-sponsored trolls manipulating public opinion via Twitter.[34]

For the government's specific measures in treating the SMPs as critical infrastructure, the following would be an accurate example: during the 58th presidential election, the FBI has monitored social media accounts on Election Day to track Russian efforts to spread damaging false information about candidates, CNN reported Friday. Dozens of agents scanned Twitter and Facebook, where stories promoting conspiracy theories and false claims against Democratic nominee Hillary Clinton had gained traction before the vote.[35]

### 4.2 Germany

In Germany, efforts are focused on regulating social media companies. The regulatory measures mainly manifest as fines only. The country has seen a proliferation of fake news, particularly targeted at the country's refugee population. Lawmakers are considering legislation to force Facebook to remove fake news and incitements to hate crimes from its pages within 24 hours or face significant fines.[36]

A German politician interviewed by Deutsche Welle wants to criminalise the creation of fake news sites, which he said "weaken the media landscape and the very fabric of our state."[37]

### 4.3 Israel

Like the case in Germany, the Israeli government's efforts are focused on regulating social media companies.

Since the collapse of the peace talks in 2014 and Israeli settlement expansion in occupied territory, there have been bloodshed between Israel and Palestine. Reuters has reported that there have been "Palestinians have killed 34 Israelis and two visiting U.S. citizens in a wave of street attacks, mostly stabbings. Israeli forces have shot dead at least 201 Palestinians" in the period from October 2015

---

[34] Kevin Townsend. Should Social Media be Considered Part of Critical Infrastructure?http://www.securityweek.com/should-social-media-be-considered-part-critical-infrastructure. 2017/11/30. Access date: 2017/12/25.

[35] Josh Delk, FBI tracked Election Day social media for fake news from Russia, the HILL, http://thehill.com/policy/technology/345392-fbi-monitored-social-media-on-election-day-watching-for-russian 2017/04/08. Access date: 2017/12/25.

[36] Deutsche Welle, 500,000 euro fines for fake news on Facebook in Germany? http://www.dw.com/en/500000-euro-fines-for-fake-news-on-facebook-in-germany/a-36806244 2016/12/16. Access date: 2017/12/25.

[37] Carla Bleiker, Sensburg: Fake news is 'press warfare', http://www.dw.com/en/sensburg-fake-news-is-press-warfare/a-36753554 2016/12/13. Access date: 2017/12/25.

to July 2016.[38]

In an interview on July 2nd of 2016, Mr. Gilad Erdan, Israel's Minister of Internal Security, has publicly accused Facebook of being "used to perpetuate such bloodshed". Especially, Facebook have been "sabotaging" Israeli police efforts by not cooperating with inquiries about potential suspects in the occupied West Bank and "set(ting) a very high bar for removing inciteful content and posts".[39] With regard to the latter, Minister Erdan revealed that of 74 "especially inciting and extremist posts" Israel had brought to Facebook's attention, only 24 were removed. This has led Israeli government to draft legislation to enable it to order social media sites to remove postings deemed threatening.[40]

In an separate interview, Justice Minister Ayelet Shaked called on social media companies to curb pre-emptive content deemed by Israel to be a security threat. She said, "we want the companies not to approve and to themselves remove posts by terrorist groups and incitement to terrorism without us having to flag each individual post, in just the same manner, for example, that they today do not allow posts and pages with child pornography".[41]

### 4.4 UK

The extent of UK's regulating social media companies is the weakest compared to the three countries above. To this country, social media platforms has become the hotbed for one of its most hated enemies: terrorism.The country has seen a series of terrorist attacks, some of which are proven to have employed social media platforms as tools.

In June this year, according to British Prime Minister Teresa May, social media companies are still providing terrorists with a 'safe place' to operate--and this led to the terrorist attack in London in June. One critical report from the British House of Commons Home Affairs Committee on hate crimes and extremism pointed out: "Social media companies currently face almost no penalties for failing to remove illegal content. There are too many examples of social media companies being made aware of illegal material yet failing to remove it, or to do so in a timely way.' [42]

Beside this, the spreading of fake news on the SMPs is also one of the British government's concerns in regard to regulate SMPs. The Yougov poll was carried out over a two-day period from a sample of 1,684 UK adults weighted to be representative by age, gender, education qualification, social grade, as well as the 2015 election vote, EU referendum vote, government office region and political attention. When those surveyed were shown six individual news stories, three of

---

[38] Ari Rabinovitch, Israeli minister says Facebook a 'monster', hindering security, July 3, 2016, http://www.reuters.com/article/us-northkorea-missiles-idUSKBN1AO011 Access date: 2017/12/25.
[39] Dan Williams, Facebook defends position on content standards after Israeli censure, July 3, 2016, http://www.reuters.com/article/us-israel-facebook-idUSKCN0ZJ0D8 Access date: 2017/12/25.
[40] Ibid.
[41] Ibid.
[42] Khari Johnson. Facebook's AI for targeting terrorists will go beyond Muslim extremists https://venturebeat.com/2017/06/16/facebooks-ai-for-targeting-terrorists-will-go-beyond-muslim-extremists/ 2017/06/16 . Access date: 2017/12/25.

which were true and three of which were fake, only 4% were able to identify them all correctly. Nearly five in ten (49 per cent) of all respondents thought at least one of the fake stories was true.[43]

In this poll, two thirds of the British public (66%) think social media sites such as Facebook or Twitter aren't doing enough to tackle fake news, with half of respondents believing that more fact-checking sites are needed. And over half (55%) of respondents think the government is not doing enough to tackle fake news, suggesting the issue is now on the public's national agenda.[44]

Damian Collins, MP, Chair of The Culture, Media and Sport Committee, said when launching the inquiry into 'fake news' in Feb 2017:

> "Just as major tech companies have accepted they have a social responsibility to combat piracy online and the illegal sharing of content, they also need to help address the spreading of fake news on social media platforms."[45]

Committee chair Damian Collins suggested that any likely solution would focus on social media, saying that major tech companies "need to help address the spreading of fake news on social media platforms" and that "consumers should also be given new tools to help them assess the origin and likely veracity of news stories they read online." He also told Buzzfeed News that Facebook's News Feed would be a key focus of the inquiry, and that it could "absolutely" be the case that they could ask Facebook to attach warnings to potentially inaccurate news stories in the UK.[46]

## 5. Do SMPs fit into the framework of CII protection: preliminary discussion

In 2005, the second resolution on creation of a global culture of cyber-security adopted by the UN General Assembly is 'expanded to include the protection of critical information infrastructures'[47]. This UN resolution is 'cosponsored by a total of 69 countries including China but not Russia'[48]. Compared to the first draft, the final text (the UN General Assembly resolution 58/199 *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* ) includes the following new introduction paragraph: 'each country will determine its own critical information infrastructure'[49].

---

[43] Jessica Goodfellow, Only 4% of people can distinguish fake news from truth, Channel 4 study finds, http://www.thedrum.com/news/2017/02/06/only-4-people-can-distinguish-fake-news-truth-channel-4-study-finds 2017/02/06. Access date: 2017/12/25.

[44] Ibid.

[45] UK Parliament, 'Fake news' inquiry launched, 30 January 2017, https://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news-parliament-2015/fake-news-launch-16-17/ Access date: 2017/12/25.

[46] Jim Waterson and Matthew Champion, Parliament Could Ask Facebook To Add "Fake News" Warnings To British News Stories, https://www.buzzfeed.com/jimwaterson/british-mps-are-targeting-facebook-with-fake-news-inquiry?utm_term=.mrEewpPdJ#.qmm7J16yM 2017/01/30. Access date: 2017/12/25.

[47] Maurer, Tim, 'Cyber Norm Emergence at the United Nations-An Analysis of the UN's Activities Regarding Cyber-security? ' Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

[48] UN General Assembly A/58/481/Add.2

[49] UN General Assembly A/58/199.

Since 1996, the US has had a wide-reaching Critical Infrastructure Protection Program in place. The *U.S Patriot Act of 2001* signed by Bush first distinctly provided a definition of Critical Infrastructure in America: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[50] The National Infrastructure Protection Plan (NIPP)[51] defines the critical infrastructure sectors in the US. Presidential Policy Directive 21 (PPD-21),[52] issued in February, 2013 entitled Critical Infrastructure Security and Resilience mandated an update to the NIPP. This revision of the plan established the following 16 critical infrastructure sectors:

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems.

In Germany, on 10th, Jul. 2015, the German Bundesrat(the country's federal council) approved the new IT *s*ecurity law: *IT-Sicherheitsgesetz.* 'The law will affect institutions listed as "critical infrastructure", such as transportation, health, water utilities, telecommunications providers, as well as finance and insurance firms. It gives companies two years to introduce cyber security measures or face fines of up to € 100,000 ($111,000).[53]

In the UK, the government's official definition of Critical National Infrastructure (CNI) is: "Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social

---

[50] *USA PATRIOT Act.*

[51] *National Infrastructure Protection Plan.* https://www.dhs.gov/national-infrastructure-protection-plan

[52] Office of the Press Secretary, The White House. *Presidential Policy Directive -- Critical Infrastructure Security and Resilience.* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil 2013.02.12. Access date: 2017/12/25.

[53] Germany passes strict cyber-security law to protect 'critical infrastructure' https://www.rt.com/news/273058-german-cyber-security-law/. 2015/7/11. Access date: 2017/12/25.

consequences or to loss of life."[54]

The Commission of the European Committee equates Information and Communication Technologies (ICTs) infrastructure as Critical Information Infrastructure as as 'their disruption or destruction would have a serious impact on vital societal functions'[55].

From these official definitions of CII in the above countries and world organizations, we could see that apart from China which has already offered a clear definition of the precise phrase 'Critical Information Infrastructure'; both the U.S and Germany only offered their definitions of a broader concept: the Critical Infrastructure; UK's 'Critical National Infrastructure' could be regarded as a British counterpart of the 'Critical Infrastructure'.

Despite the different terminology and the slight deviations in connotations adopted outside China--whether they manifest as 'internet networks','mass public information network services''information networks' , 'information technology' , or'computer resources', etc--there is one mutual feature of these definitions of Critical Infrastructure Information (if we could unify all the similar terminologies above as this single noun phrase): they are so vital that the incapacity or destruction of such systems would have a debilitating impact on national security and societal functions.

## 6. Conclusion

Through a comparative study,we have already discussed, that despite the different terminologies and the slight deviations in connotations adopted inside and outside China--whether they manifest as 'internet networks','mass public information network services','information networks' or 'information technology' , etc--there is one mutual feature of these definitions of Critical Infrastructure Information (if we could unify all the similar terminologies above as this single noun phrase): they are so vital that the incapacity or destruction of such systems would have a debilitating impact on national security and societal functions. And with the three layers of SMPs' negative influences upon one country(the divergence of social consensus, the reveal of the invisible society and the transfer of communication power), it is justified enough to say that SMPs could be treated as CII, therefore deserving CII protection.

Also, this comparative study has found that China is the first country (the UN's General Assembly Resolution 55/198 and European Commission's Communication on Critical Information Infrastructure protection are not national but international regulatory documents; the U.S only has regulations on a broader term: Critical Infrastructure; Germany being the same....etc. )which has drafted and brought into effect a national administrative regulation on Critical Information Infrastructure, in which SMPs is included.[56]

---

[54] Critical National Infrastructure. https://www.cpni.gov.uk/critical-national-infrastructure-0.
[55] *Communication on Critical Information Infrastructure protection (CIIP)* https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip
[56] *Critical Information Infrastructure Security Protection Regulations.* http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

Then through a detailed analysis of the recent Chinese regulations of the SMPs since the publication of Cyber-security Law, we could see that though the phrase'resilience and security'-the ultimate goal of traditional CII or CI protections- has not been distinctly lined out in these regulations, in effect, the content of these regulatory documents in China still manifest as directly aiming at achieving the ultimate goal of traditional CII protection.

As we could see from the cases of the U.S., the U.K, Germany and Israel, these four Western democratic nations are exhibiting different degrees of mild trends(legislative or administrative) to regard SMPs as the CII(though their degree is much lower than that of China's--for none of these countries have brought out or even drafted one national administrative or legislative regulation specifically on CII).We see that Israel and Germany are already having legislative considerations in regard to treat SMPs as the CII; whereas the U.S., though it has shown obvious administrative move to regard SMPs as CII, given the fact that it is also the homeland of most of the dominant social media companies, its comprehensive legislative gestures is still yet to come; the U.K's devotion to treat the SMPs as CII, no matter from the legislative or administrative angles, are the weakest among these four countries. On the other hand, in China's case, as the Cyberspace Law comes into force by 1st June this year, China is demonstrating not just a trend, but a strong legislative and the following administrative endeavor to govern the SMPs as CII.

At this point, we could justifiably conclude that the existing and proposed regulations on SMPs both inside and outside China are converging on the regulatory approaches that are traditionally adopted in the domain of the CII protection.

For the interpretations of the SMPs' role, recently there are two different perspectives , one in the field of Media Study, another in the field of Political Science.

For the media study experts, some have regarded SMPs as public forum, like parks, streets and town halls where speech and debates happen. In his 2013's book The Social Media President: Barack Obama and the Politics of Digital Engagement, James Katz examined social media's 'ever-larger role in political rhetoric, campaign strategies, governance appeals and public debate' [57]. To him, the role of social media platform as public engagement clearly has its advantages. Hence "public officials may not 'block' their constituents on social media"[58]. This argument mostly concerns about the role of SMPs in the power distribution in the

---

[57] James E. Katz. *The Social Media President: Barack Obama and the Politics of Digital Engagement*. Palgrave Macmillan. 2013.

[58] Kieren McCarthy, Blocking peeps on social media? That's a paddlin' for governors, senators, house reps. US officials' online spaces – a public forum or private haven? 10 Aug 2017, https://www.theregister.co.uk/2017/08/10/governors_senators_and_house_reps_suedwarned_over_social_media_blocking/ See also Thomas Wheatley, Why social media is not a public forum, Washington Post, August 4 2017, https://www.washingtonpost.com/blogs/all-opinions-are-local/wp/2017/08/04/why-social-media-is-not-a-public-forum/?utm_term=.d92ad137ed49

political system and decision-making. It has not yet been settled, and the continence of it still holds valuable meanings.

In the meanwhile, we could see that, a new reality has emerged. With incoming waves of fake news or disinformation campaigns from enemy countries on the eve of major political elections in the western countries, and increasingly influences from the domestic and foreign terrorist groups to radicalize and recruit young people online across the world, SMPs have gained more and more traction in the national security related debates worldwide. A different governing framework for the dominant SMPs may be warranted in the context of increasing securitization of information, or the emerging information warfare among states.

With this in mind, as we already concluded that the dominant SMPs could be governed as the critical information infrastructures, and that the current and proposed regulations on SMPs both inside and outside China are converging on, the regulatory approaches that are traditionally adopted in the domain of the CII protection, then the governing framework of SMPs as political apparatus in the political system will entangle with this new governing framework that sees SMPs as security apparatus for national security and stability, and causes great new uncertainties for the [cross-border] operation of the dominant SMPs.

Furthermore, we are most likely to witness a dramatic regulation regime changes regarding SMPs in the near future. What kind of sanction mechanism will be adopted in regard to social media companies' failure in conforming to the following regulations in China? At this point, apparently a mere fine of a large amount of money might not be daunting enough for those dominant social media companies as Facebook, Twitter, or even Weibo, etc. 'In March, a German government minister said companies like Facebook could face up to $53 million in fines for failing to do enough to curtail hate speech. British members of Parliament have endorsed similar fines.' [59] Yet in June this year, according to British Prime Minister Teresa May, social media companies are still providing terrorists with a 'safe place' to operate--and this led to the terrorist attack in London in June. One critical report from the British House of Commons Home Affairs Committee on hate crimes and extremism stated:"Social media companies currently face almost no penalties for failing to remove illegal content. There are too many examples of social media companies being made aware of illegal material yet failing to remove it, or to do so in a timely way.' [60] To solve this problem, the statement offered a refreshing envision: "we recommend that the government consult on a system of escalating sanctions to include meaningful fines for social media companies which fail to remove illegal content within a strict time-frame."[61] For the complexity and precision of this future system of 'escalating sanctions', that is of the law-makers and politicians' calculation.

---

[59] Khari Johnson. Facebook's AI for targeting terrorists will go beyond Muslim extremists https://venturebeat.com/2017/06/16/facebooks-ai-for-targeting-terrorists-will-go-beyond-muslim-extremists/ Jun 16. 2017.
[60] Ibid.
[61] Ibid.