Nine Areas of Disputes in the Debate on International Cyber Norms
网络空间国际规则谈判的九个分歧点

Nine Areas of Disputes in the Debate on International Cyber Norms

一、四个难以分割的主题

1. Four Interrelated Dimensions

从广义上讲，网络空间国际规则谈判至少包括以下四方面内容。第一方面是网络空间的谈判，主要涉及军事和情报部门。重点关注国际法如何适用于网络空间，第一届至第五届联合国信息安全政府专家组（UN GGE）是典型的谈判论坛。第二方面是网络犯罪治理的全球对话，主要涉及公安和司法部门。关键文本包括美国主导的《布达佩斯网络犯罪公约》，也有俄罗斯递交的《反俄罗斯网络犯罪公约》。双方对互联网名称与数字地址分配机构（ICANN）等技术社群的司法管辖权存在争议，有一些国家甚至试图重新分配互联网名称、数字、参数体系。第四方面是各国在跨境数据流动上的争夺和实践，各国近年来都采取了一系列加强网络空间国家管辖权的行动，体现在一系列重要立法和战略文件中，如中国的《网络安全法》和欧洲的《通用数据保护条例》。

Broadly speaking, the debate on international cyber norms covers at least four interrelated dimensions. The first dimension is the negotiation about the legitimacy and rules of cyber weapons, mainly involving military and intelligence entities and focusing on the applicability of international laws to the cyberspace. The first to the fifth United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) were typical negotiation forums in this regard. The second dimension is the global dialogue on cybercrime governance. It mainly involves public security authorities and justice systems and key texts include the Budapest Convention on Cybercrime, which the European Union (EU) strongly advocates, and the Draft UN
Belongs to the fourth dimension, but the two instruments are to some extent responses to actions of U.S. military and intelligence agencies as exposed in Snowden Leaks, which falls into the first dimension.

具体来说，本报告主要叙述了网络空间国际规则谈判的起源、分歧及走向，梳理了9个领域的分歧点：（1）沿用旧法与制定新法；（2）网络安全漏洞治理；（3）动网和动武关系；（4）网络空间与新战场；（5）网络间谍活动；（6）互联网基础法律；（7）金融机构和金融数据；（8）社交媒体和政治稳定；（9）网络威胁论与网络空间命运共同体。这主要是推动领先国家和落后国家的谈判，强者不想限制自己的网络军事实力和野心，这是谈判无法禁止武器、防止军备竞赛的主要原因。同时，由于互联网自身的特性，尤其是“高处不胜寒”，反而认为自己极端脆弱，担心无人机被劫持，担心网络指挥系统被攻击，担心数据被篡改，担心知识产权被盗用，这些认识显然是夸大了，但也有一些道理。因此，网络空间国际规则谈判中诞生了许多看起来荒唐但实际上理性的规则语言。

Specifically, this report presents the origins of, disputes in, and trends of the debate on international cyber norms. There are nine areas of disputes: (1) applying existing laws vs. working on a new treaty; (2) governance of cybersecurity vulnerabilities; (3) relationship between a cyberattack and a physical attack; (4) legitimacy of the cyberspace as a new battlefield; (5) cyber espionage activities; (6) Internet infrastructure; (7) financial institutions and data; (8) social media and political stability; and (9) cyber deterrence conception and cyberspace with a shared future. These disputes reflect the gap between more powerful nations and less powerful ones. Powers are unwilling to accept restrictions to their cyber military capabilities and cyber ambitions. This is the major reason for the failure to ban cyber weapons and prevent a cyber arms race. Meanwhile, due to the technical features and the asymmetry of the Internet, powerful nations tend not to feel their own power and, on the contrary, believe themselves to be vulnerable. They are worried about the possibility that their drones might be hijacked, their command and control systems might be attacked, their financial data might be manipulated, and their intellectual property might be stolen. These worries may be exaggerated to a large extent, but there is still some truth in them. Therefore, the debate on international cyber norms
produced a lot of paradoxes, complexities, and ridicules, which are actually quite justifiable.

In the context of international law, the debate on international cyber norms has been lively, with new mechanisms and initiatives emerging. A wide range of places such as Tallinn, the Hague, Geneva, Wuzhen, Washington DC, Moscow, Tel Aviv, New Delhi, Singapore, and London have all marked themselves as producing sites of cyber norms and some norms have gained wider recognition. On the other hand, the debate is gaining in depth and sophistication and it has become more difficult to reach consensuses. Globally, nations and stakeholders stick to highly divided standing points on key issues. Within each nation, disagreements among various departments and actors are no less evident than in the global arena. The norms-making landscape will continue to be fragmented for the time being while the various parties searching for new possibilities to move forward. Besides literature review and on-site observations, we also conducted in-depth face-to-face interviews with 15 people, including government officials, think tank members, and professors from the EU, the United States, and the Russian Federation. These are how we produced the nine areas of disputes and presented some emerging international norms.

II. Nine Areas of Disputes in the Debate on International Cyber Norms

1. Applying Existing Laws vs. Working on a New Treaty

The debate on whether to apply existing international laws to the cyberspace or work to produce an international cybersecurity treaty has been prominent. The United States and some EU members who have accumulated advantages in the traditional international legal system favor the former option and aim for non-binding cyber norms, believing that integration and interpretation of existing laws will suffice to meet the challenges. The Russian Federation and some other nations are not against the former option but stay skeptical and actually prefer working on a binding new cybersecurity treaty.

2013年，“北约网络合作防御卓越中心”（NATO Cooperative Cyber Defense Center of Excellence）出版了《关于网络战国际法适用的塔林手册》（“塔林1.0”）。2017年出版了《关于网络行动国际法适用的塔林手册2.0》（“塔林2.0”），两部《塔林手册》虽然是用旧法的典型实践，分别对应门槛以上和门槛以下的网络活动。“塔林2.0”和“塔林1.0”在共同之处在于，它们都着眼于网络空间之外已经存在且具有习惯法地位的旧法，并对这些规则应当如何适用于网络空间加以澄清和发展，而不是倡导新法。
网络空间国际规则谈判的九个分歧点

却也同时设定了巨大的局限性，体现了强者的传统思维，难以获得技术社群/代码社群和信息产业的认可，更难尊重代码空间的复杂性。

The two Tallinn manuals represent the traditional approach toward cyber challenges and reflect how law experts view cyber sovereignty. Their working method of applying existing laws and law by analogy, while having some advantages, show a major weakness in that the rigid traditional way of thinking that lies behind it is not easily acceptable to technical communities and the IT industry and shows hardly any respect to the code-based cyberspace.

很多时候，在沿用旧法和制定新法问题上的辩论看起来像是一个伪命题，这样说基于两个理由。第一是双方没有清晰的边界，经常使用同样的论据来反驳对方。沿用旧法的支持者认为新法需要耗费更多的时间，但制定新法的支持者看法正好相反，断削沿用旧法更费时费力。沿用旧法的支持者认为，制定新法会限制技术变革和创新。制定新法的支持者认为，只有制定新法才能尊重技术趋势。此外，双方还都使用网络攻击验证和渊源难度等技术问题去反驳对方。

To a large extent, the debate between applying existing laws and signing a new treaty prove to be misleading. There are at least two reasons for this observation. One is that there are no clear boundary between the two sides. Supporters of the two approaches often cite the same evidence to their squarely opposite points. For example, supporters of existing laws argue that working on a new treaty will take more time while supporters of a new treaty believe that extending the existing laws will be more time-consuming. Supporters of existing laws hold that working on a new treaty will hamper growth and stifle innovation while supporters of a new treaty argue that a new treaty gives more respect to new technical trends. Also, the two sides both cite challenges in checking and attributing cyberattacks as points against the other side.

新旧法支持者辩论的第二个挑战来自于实践，不仅是伊拉克战争，还是利比亚战争，国际法都没有得到充分尊重。在应对网络挑战方面，强权国家也从来都是干涉他国，不尊重自己。一方面，他们利用自己的技术实力，持续入侵他国网络和基础设施，监控世界，惜不收敛，而国际社会对此缺乏法律层面的应对手段。另一方面，甚至在保护自身脆弱性这一问题上，网络强国也经常对国际机制不屑一顾，更不考虑网络技术的复杂性，而是片面强调自己受

网络安全漏洞治理 Governance of Cybersecurity Vulnerabilities

2017年5月中旬，勒索病毒(WannaCry Ransomware)肆虐全球。这个事件涉及两种行为，第一种行为是开发行为，政府开发、储存软件漏洞。建立网络武器库，是正常履行国家安全和网络安全职责，还是不负责任、滥用网络空间？第二种行为是泄密行为，网络武器类库本身说明了什么问题？如何评估这个事件？这是不是一个非常严重的问题？泄露开发者、散布者、运营者/用户等谁的罪责最大？

In mid-May 2017, the WannaCry Ransomware plagued the world. There are at least two actions behind this event: exploitation and proliferation. Is exploitation of vulnerabilities a fulfillment of the government duty of ensuring national security and cybersecurity or an irresponsible misuse of the cyberspace? What does the proliferation reflect? How should it be understood? How serious is this problem? Who should be blamed the most, the developers, proliferators, operators, or end users?

许多国家认为要从源头和扩散两个角度来看问题，认为根源在于政府开发、储存漏洞，并且未能做到防止扩散和泄露。也有一些国家认为，安全部门开发、储存漏洞是履行政府职能，是正常不过的行为。不这样做，反而是政府的渎职,
网络空间国际规则谈判的九个分歧点

认为问题在于那些扩散漏洞的人是应该承担责任，并且责任运营商、用户的安全意识淡薄。

Some nations believe that the primary cause for the WannaCry Ransomware attack is the exploitation and stockpile of vulnerabilities by governments and the failure to prevent proliferation. Other nations hold that it is quite normal for security agencies of each nation to exploit vulnerabilities and that it would be a misconduct if these agencies fail to do so. Thus, these nations tend to hold the proliferators most liable and blame the operators and users for their lack of awareness of cyber risks.

联合国信息安全专家组2015年共识报告第13条第(i)款写道：“各国应该采取合理的步骤，保障供应链的完整，维护用户对ICT产品安全的信心。各国有其防止恶意信息与通信技术（ICT）工具的扩散，避免使用有害功能。”第13条第(j)款“各国应该鼓励负责任地汇报信息与通信技术漏洞，分享漏洞修复手段有关的信息，限制并努力消除对信息与通信技术和借助信息技术的网络基础设施的潜在威胁。”“这些条款为思考网络安全漏洞建设立法提供了起点。”

Article 13 (i) of the 2015 consensus report of UN GGE states that “States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products” and “States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.” Article 13 (j) notes that “States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.” The two may serve as a starting point for us to think about global governance of cybersecurity vulnerabilities.

2017年2月14日，勒索病毒攻击事件尚未发生，但就像预料到这类事件会马上发生一样，微软公司总裁兼首席法务官史密斯（Brad Smith）在信息安全大会（RSA）大会上提出《数字日内瓦协定》倡议，微软公司认为：“网络空间无处不在，海、空存在差异，最大差异是网络空间归私有部门所有，由私有部门经营，不管是海底电缆、数据中心，还是服务器、笔记本电脑、智能手机，均属私人财产。世界各国政府不能对私有部门开展网络攻击，不能擅自民用基础设施，不能强制要求在ICT产品上植入后门，不能擅自积累漏洞。”

On February 14, 2017, two months before the outbreak of the WannaCry Ransomware attack, Brad Smith, President of Microsoft Corporation, called for the Digital Geneva Convention. Microsoft claims that the cyber domain fundamentally differs from the ground, sea and air in terms that the targets from submarine cables to data centers, servers, laptops and smartphones are private property owned by civilians. Governments shall not target the private sector or critical infrastructure with cyberattacks, shall not require any back door on IT products, and shall report vulnerabilities to vendors, not stockpile, sell or exploit them.

大国之间的信任仍然是漏洞问题上建立体制的主要障碍。一些国家行为主体继续沿用冷战思维，敌我视角来思考网络安全漏洞问题。在一个本来不分国界、相互依赖的技术问题上，各国明明有机会构建和谐共处的命运共同体关系，但是一些强硬派人士，试图在没有边界或边界模糊的问题上强行设置意识形态边界，在勒索病毒攻击等事件中，有国家明明是漏洞制造者、植入者，却利用新闻传播领域的优势，已将自己定义为好人、受害者，将别国定义为坏人、施害者。

Lack of trust among powerful nations is a major barrier to the global governance of vulnerabilities. Some state actors have kept to the Cold War mentality and drawing ideological lines when facing the issue of cybersecurity vulnerabilities, which is a technical issue featuring no natural boundary, only interdependence. Thus, the world is losing out on an opportunity to build a community with a shared future. Worst of all, in the WannaCry Ransomware attack, those who actually exploited and stockpiled vulnerabilities made use of their advantages in the media and and defined themselves as good guys and victims while condemning others as bad guys and perpetrators.

3.“动网”与“动武” Relationship between a Cyber Attack and a Physical Attack

The United Nations Charter第51条表示：“联合国任何会员国受武力攻击时，在安全理事会采取必要办法，以维持国际和平及安全以前，本宪章不得认为禁止行使单独或集体自卫之自然权利。会员国因行使此项自卫权而采取之办法，应立即向安全理事会报告。此项办法于任何方面不得影响该会员国按照本宪章随时采取其认为必要行动之权责，以维持或恢复国际和平及安全。”

Article 51 of the Charter of the United Nations writes: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an
This is allegedly the first time that the United States and major powers like Germany, France, Italy, Canada, and Japan shared the same stance in regard to cybersecurity. It stipulates how Article 51 (on self-defense) of the Charter of the United Nations can be applied to the cyberspace. Many believe this to be a misinterpretation that equates cyberattack with armed attack. Article 51 of the Charter of the United Nations actually allows self-defense only when an armed attack occurs, not a cyberattack.

2016年9月17日-18日，不结盟运动第17届首脑峰会在委内瑞拉举行，会议通过了长达206页的成果文件，文件第811.6条表示：“一些国家表示要使用传统武器回应网络攻击，不结盟运动国家对此深感忧虑，不结盟运动国家认为，应对此新威胁的最佳途径是各国携手合作，避免网络空间成为军事行动的角斗场”。国家创新与发展战略研究会副会长郑飞力将军这样描述各国在这个方面的立场差异：“一些传统强国往往沿用实体空间思维定势，习惯套用‘动武’即‘动武’的行为准则，追求一种绝对的安全，这不但解不了网络空间面临的问题，而且还带来诸多麻烦”。

Article 811.6 of the 206-page outcome document of the 17th Summit of Heads of State and Government of the Non-Aligned Movement held on September 17 and 18, 2016, in Venezuela writes: “The Heads of State or Government expressed their concern for the potential use of ICT’s in international conflicts, covert and illegal operations, and attacks to third countries by individuals, organizations and states through the use of computer systems of other nations. The Heads of State or Government further expressed their concern on the expressed ability of some Governments to respond to such attacks with conventional weapons, and reiterated that the most effective ways to prevent and address these new threats is through the joint cooperation among all States, and preventing the cyberspace to become a theater of military operations.” General Hao Yeli, Deputy Director of Chia Institute for Innovation & Development Strategy, described the division between nations on this issue in the following way: “some traditional powers tend to keep to some stereotypes of the physical world, apply the principle that a cyberattack equals an armed attack, and pursues absolute security. This is of no help to solving the problems of the cyberspace and may even bring more trouble.”

armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.”

2016年5月27日，七国集团日本峰会发布《七国集团网络空间原则和行动》（G7 Principles and Actions on Cyber），第二部分第5条表示：“在一些情况下，网络空间允许动用武力或发动武力攻击”。因此，七国集团认为，可以激活《联合国宪章》第51条关于自卫权的论述，使用传统武力进行反击。这条规则的完整论述为：在一些情况下，网络空间等同于动用武力或发动武力攻击，符合《联合国宪章》和国际惯例的含义。对于通过网络空间发动的武力攻击，各国可以依照《联合国宪章》第51条和《武装冲突法》等国际法的规定，行使固有的个体或集体自卫权。

Paragraph 5 of Part II in G7 Principles and Actions on Cyber announced by the Group of 7 Summit in Japan on May 27, 2016 states that “under some circumstances, cyber activities could amount to the use of force or an armed attack.” Therefore, Article 51 of the Charter of the United Nations could be activated to respond to a cyberattack with traditional armed forces. The full paragraph writes: “We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the UN Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace.”

这是美国副总统、法、英、日等国代表在七大会议中提出的网络空间原则和行动。该条款是七国集团对《联合国宪章》第51条（自卫权）如何适用于网络空间的解读。许人认为，这种解读扭曲了该条款的原始含义，将“网络攻击”和“武力攻击”等同起来。《联合国宪章》第51条关于自卫权的真义是在遭到武力攻击（an armed attack）方能行使自卫权，而非遭到网络攻击。
网络空间国际规则谈判的九个分歧点

2017年6月中旬，第五届联合国信息安全政府专家组最后一次会议在纽约召开。美国及其军事盟友将七国集团的高官势暇原则引入报告草案。古巴谈判代表罗德里格斯（Miguel Rodriguez）表示，这段话试图将网络空间转变为军事行动的新战场。侵害受害者名义，企图通过经济制裁、军事行动等手段，回应网络攻击，借此合法化诉诸单边武力的行为。因此，古巴认为这种措辞不可接受。古巴的立场获得很多新兴和不发达国家的共鸣。这种分歧导致谈判陷入僵局。古巴和乌拉圭等国发起多边性行为，促使古巴认为修订草案不切实际，达成共识报告。

The contradiction of opinions about the relationship between a cyberattack and a physical attack divided the last meeting of the fifth UN GGE held in New York in mid- to late June 2017. The United States would like the Group of 7 wording be included in the draft final report while other nations expressed worries about the wording. Representative of Cuba Miguel Rodriguez said that such an understanding could convert cyberspace into a theater of military operations and legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by states claiming to be victims of illicit uses of ICTs. Many emerging and developing nations echoed this opinion. Disputes like this on cyber activities above the threshold and around countermoves below the threshold led to a failure to reach consensus at the meeting.

4. 网络空间新战场所Legitimacy of the Cyberspace as a New Battlefield

网络空间“是不是”已经成为一个新战场？网络空间“要不要”成为新战场？这两个问题如何分清？前者的后果让步，还是后者向后者妥协？制定网络空间新战场所行为规范，是否在制定网络空间作战规则？在制定网络空间新战场的合法性？在制定网络空间新战场的合法性和在推动网络空间军事化？

Has the cyberspace already become a new battlefield? Should it be one? How should we face these questions? Answer to which of them shall prevail in the event of a conflict? Does making a cyberspace code of conduct equal making rules for cyber warfare? Are we legitimizing the cyberspace as a new battlefield? Are we pushing towards a cyber battlefield?

各国专家对现实的看法基本一致，都大致承认网络空间已经成为一个新战场。毕竟，已经有近40个国家和地区组建了网络部队，但是各国在网络空间应该
网络空间国际规则谈判的九个分歧点

cyberspace. This is fully in line with their attitude towards the governance of cybersecurity vulnerabilities. Most emerging and developing nations, and civil society groups, on the contrary, believe the reality to be unacceptable and advocate a step back from it to de-militarize and de-weaponize the cyberspace. In their opinion, the world should not yet give up on efforts in this regard and we make rules exactly because we want the cyberspace to no longer be a battlefield. To them, international debate on cyberspace norms should challenge the reality rather than accept it as it is.

2017年3月1日，中国外交部和国家互联网信息办公室联合发布《网络空间国际合作战略》，明确表示：“网络空间加强军备，强化威慑的倾向不利于国际安全与战略互信。中国致力于推动各方切实遵守和平解决争端、不使用或威胁使用武力等国际关系基本准则，防止网络空间成为新的战场。”

The International Strategy of Cooperation on Cyberspace jointly issued by China’s Ministry of Foreign Affairs and Cyberspace Administration on March 1, 2017, states: “The tendency of militarization and deterrence buildup in the cyberspace is not conducive to international security and strategic mutual trust. China encourages all parties to commit to peaceful settlement of disputes, non-use or threat of force and other basic norms in international relations so that the cyberspace will not become a new battlefield.”

网络空间武器化和军事化是在西方国家的领导下进行的，本身就是一种不负责任的国家行为。网络空间应该提倡一种新逻辑、新思维，避免走向武器化、军事化，防止出现新的军备竞赛，这应该是联合国信息安全政府专家组辩论的出发点，如果背离了这个出发点，转而制定作战规则，那就是“缘木求鱼”，违背初衷，反而赋予了网络空间作为新战场的合法性，间接推动网络空间军事化。

The weaponization and militarization of the cyberspace, led by the West, is an irresponsible state action. Advocating a new logic and a new way of thinking and preventing a cyber arms race shall be the mission of UN GGE. Acting against such an assumption brings the risk of legitimizing internationally the status of the cyberspace as a military zone.

5.网络间谍活动 Cyber Espionage Activities

国家行为主体可不可以窃取私营企业的知识产权信息？中国和美国达成共识，并表示：可以，但不能用于增强本企业竞争力。继中美之后，这条国际
Commission, founded in February 2017 at the Munich Security Conference, consists of over 40 prominent cyber personalities from nearly 20 nations.

The first norm that the Commission initiated is non-interference with the public core of the Internet. The Commission explained this norm at the Global Conference on Cyberspace held in New Delhi on November 21, 2017. State and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2018年5月19日至20日，网络空间稳定委员会在斯洛伐克召开会议，发布新文件，对互联网公共核心做了详细阐释，认为它由四大类组成：(1) 包路由选择和转发（packet routing and forwarding）；(2) 命名和编号系统（naming and numbering systems）；(3) 安全和身份机制（The cryptographic mechanisms of security and identity）；(4) 物理传输介质（physical transmission media）。

The Commission elaborated on the definition of the public core in a new document it issued at a meeting held in Bratislava on May 19 and 20, 2018. It contains four categories: (1) packet routing and forwarding, (2) naming and numbering systems, (3) cryptographic mechanisms of security and identity, and (4) physical transmission media.

The Internet's role and the importance of information security, however, are often overlooked or underestimated. The Internet has become a crucial tool for governments and businesses, and its role in global politics cannot be ignored. The Internet has also become a vital tool for international cooperation and dialogue, and its role in global politics cannot be ignored.

A moral perspective, penetration of submarine cables, cyber espionage, R&D of killer robots, and stockpiling vulnerabilities should all be banned. However, the real
网络空间国际规则谈判的九个分歧点

世界是远从什么在做。在现实中，这些行动并不仅是禁止的，而是也存在广泛的社会化、甚至机构化的，明确地要求各种国家在加入该文件之前要进行修改。这似乎是与可被理解的需要有关的，例如对人权的挑战以及极端主义和部分的不正当理由，如这种形式的优势在军事和情报领域。

如果将互联网公共核心比如为公民住宅，那么对于是否可以进入这个空间，本来是需要弄清楚是否获得法院的搜查令即可。只要没有搜查令，任何进入这个空间的行为都应该属于非法行为。然而，这种规则表示，同样是进入访客的行为，如果毁掉住宅的大门，是不可以的，只要不毁掉住宅的大门，就可以进入访客。

如果比较的裸体线的互联网作为私有住宅，我们仍需要看到如果法院发出搜索令是否适合我们来决定其是否合法考虑。

另一方面，某些强权国家在某种意义上讲，委员会提出的这些规则对维卫之行，行整容之术，似乎高高举起了搜索公共核心的大旗，其实际是实现了不具物理破坏性的渗透行为。与此相比，《欧洲隐私保护协议》反而构成了对更有效、更透明的法律文本，隐私保护协议直接禁止没有合法理由的彪形无差别监控行为，比捍卫公共核心规则更能够维护全球互联网用户的利益。

Under such circumstances, the norm proposed by the Commission must be examined with more scrutiny for norms can indeed be deceptive. It indulges aggressive actions in the cyberspace in the name of protection, giving de facto permission to penetration that does not cause tangible damage. In comparison, the EU-U.S. Privacy Shield may be a better instrument in that it bans unjustified mass surveillance activities and better protects the interests of global internet users.

当然，从另一方面来看，或许只有委员会所规定的这种横棱两可的语态，才能使得各国尤其是美国军方、情报部门的默许，给对方宣布获胜的机会。在复杂的规则环境中胜出，对于美国、俄罗斯、英国等网络强国的军事和安全部门来

网络空间国际规则谈判的九个分歧点

说，这条规则或因并不坏，但是对于民间团体和科技社群来说，这条规则的诞生和未来生长绝不是好消息。

Surely, in the meantime, such ambiguity as manifested in the norm may be exactly the reason why the norm was acquiesced by the U.S. military and intelligence agencies, afforded all parties involved an opportunity to triumph, and survived the complicated norm-making process. It may be good for the military and intelligence authorities of cyber powers like the U.S., the Russian Federation, and the UK, but it is definitely not a good news for the civil society or the technical community, either for now or in the future when it evolves.

7. 金融机构和数据 Financial Institutions and Data

数字时代，金融犯罪、货币犯罪呈现出明显的跨国特征。不管是对金融行业的网络攻击，还是行业之外的黑客活动，数量和攻击技巧不断提升，并且极有可能牵涉到国家行为，这给金融系统带来了巨大风险，也给许多个利益带来了损失。世界经济论坛“平衡金融稳定、创新与经济成长”项目将网络空间风险定义为“威胁金融稳定的“单一最大风险”。如何保护金融机构和金融数据？在金融领域网络安全建设中研究方面，二十国集团和美国卡内基国际和平基金会均比较活跃。

Financial and currency crimes in the digital age acquires a distinctive transnational feature. Cyberattacks on financial institutions have been increasing in quantity and the sophistication of the techniques used and may possibly involve state actors, posing huge risks to financial systems on the whole and causing damages to individuals. A project of the World Economic Forum—Balancing Financial Stability, Innovation and Growth—identifies cyber risk as perhaps the one single most important risk to the current financial services system. International organizations such as G20 and think tanks like the Carnegie Endowment for International Peace have been active in the research of the protection of financial institutions and financial data.

二十国集团（G20）在这个领域的努力集中于《公开发布网络安全法规、指引与监管措施集锦》这项研究成果上。2017年3月17日-18日，G20财长和央行行长在德国汉堡举行会议并发布联合公报。联合公报第7条表示：“恶意使用信息安全与通信技术（ICT），会破坏金融服务，影响国家和国际金融体系，降低安
网络空间国际规则谈判的九个分歧点

全性和信心，危及金融稳定。我们将致力于提升二十国集团金融服务和金融机构的能力，抵抗包括来自二十国集团之外国家的信息与通信技术（ICT）恶意使用。为了加强跨境合作，我们要求金融稳定委员会（Financial Stability Board，FSB）开展工作。首先盘点二十国集团已经发布的相关法规和监管措施，已有的国际指引，并界定有效实践。

The G20 efforts are crystallized in Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices. Article 7 of the Communique issued by G20 Finance Ministers and Central Bank Governors Meeting held in Baden-Baden, Germany on 17-18 March 2017 notes: “The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the Financial Stability Bureau (FSB), as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, including to identify effective practices.”

2017年10月13日，按照联合公报的要求，金融稳定委员会发布了《公开发布网络安全法规、指导与监管措施集锦》报告，金融稳定委员会调查了中国、美国、俄罗斯、欧盟等25个金融稳定委员会成员国和地区，这些国家和地区在应对金融行业网络安全方面均比较活跃，汇报了共计120项网络安全法规/指导和监管措施。

Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices was released on October 13, 2017, putting together 120 such documents from 25 members including China, the United States, the Russian Federation, and European Union.

卡内基国际和平基金会持续关注金融领域的建章立制，它建议美国和世界各国政府，应该在最大程度上保护金融系统，不管是战时，还是和平时期。卡内基这样阐释关于金融系统稳定的国际规则：各国不能开展或故意支持任何下列活动，故意篡改金融机构的数据和算法的完整性，不管这些数据和算法存储在何地，
On January 9, 2015, members of the Shanghai Cooperation Organization (SCO) proposed an updated version of the International Code of Conduct for Information Security to the United Nations. Compared to its previous version, an important update is Article 2 (3): “Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability.” This indicates that SCO members had started to view the principle of non-interference of domestic affairs from the perspective of a norm and wanted to extend its application to the IT sector and the cyberspace.

2013年和2015年联合国信息安全政府专家组的两个报告已经具体确认了“不干涉内政原则”等国际法基本原则在网络空间的适用性。另外，按照《塔林手册2.0》的解读，某个国家开展跨境宣传活动，虽然在通常情况下不侵犯另一国的主权，但如果一国借此在另一国煽动混乱，则较有可能侵犯主权。这种解读方式较为合理，有助于限制通过信息技术手段干涉他国内政的行为。

The 2013 and 2015 consensus reports of UN GGE both confirm the applicability of the basic international law principle of non-interference in the cyberspace. In addition, Tallinn Manual 2.0 implies the same message when it writes that cross-border publicity activities intended for inciting internal turmoil may constitute an invasion of sovereignty. This is a reasonable interpretation that may help contain interference with internal affairs with ICTs.

哈佛大学法学院教授、胡佛研究所高级研究员戈登史密斯（Jack Goldsmith）是“互不干涉内政”规则的支持者。他表示，美国网络安全政策制定者总喜欢关注别国如何攻击美国，极少反思美国如何攻击别国。他认为，美国应该反思希拉里时代以互联网自由的名义削弱俄罗斯政权的做法，认为美国的这些做法具有挑衅色彩，因此美国应该放弃在俄罗斯宣传美式民主和自由，换取俄罗斯不干涉美国大选。

Jack Goldsmith, professor at Harvard Law School and senior research fellow of the Hoover Institution, is a supporter of the non-interference principle. He once said that those who made the cybersecurity rules of the United States always tended to focus on how other countries attacked the U.S. not how the U.S. attacked others. In his opinion, U.S. authorities should reflect upon their Internet freedom articulations in
the years when Hillary Clinton was Secretary of State, which provocatively undermined the regime of the Russian Federation in the name of cyber freedom. He holds the view that the United States should stop preaching the American-style democracy and freedom in the Russian Federation so that Russia, in return, can stop its interference in the U.S. general election.

Up to this point, the lack of information about cyber sovereignty rules has led to the emergence of the United States-Russia conflict over cyber sovereignty. In 2017, the U.S. State Department and the Russian Foreign Ministry submitted a proposal to the United Nations for a non-interference agreement. However, the United States later reversed its stance, leading to the failure of the bilateral negotiations.

The SCO proposed the relevant norms exactly at the time of the cyber dispute between the United States and the Russian Federation, which led to a resolution of this dispute. However, when Russian Deputy Foreign Minister Sergei Ryabkov proposed on July 18, 2017 in Washington a sweeping non-interference agreement at a meeting with the then U.S. Under Secretary Tom Shannon, it was turned down for less than ideal timing. The norm-building process thus suffered a setback bilaterally between the Russian Federation and the United States.

Whether cyber security is a legitimate issue for the United Nations Security Council to address is a matter of debate. The U.S. and Russia have different views on the role of the United Nations in cyber security matters.

The social media disputes between the Russian Federation and the United States refocused the attention of the United Nations on internet security. Information security or cybersecurity has long been the focus of the debate. Russia and China show interests in content and information regulations, while the U.S. and Europe often circumvent this real challenge in the name of freedom of expression.

9. Cyber Deterrence and Cyber Community with a Shared Future

Some countries talk a lot about cyber deterrence, emphasizing the division between allies and enemies and clinging onto the cold war mentality. This has its origin in the deep-rooted traditional way of thinking. Other countries advocate a cyber community with a shared future to promote peaceful coexistence of nations and civilizations in the cyberspace. This also stems out with traditional beliefs.

2017 February 27, the U.S. Defense Science Board (DSB) published a report on cyber security, listing China and Russia as major threats. The report pointed out that China and Russia are the key countries that pose the greatest threat to the United States.

The cyber deterrence conception is evident in the report of the U.S. Defense Science Board (DSB) Task Force on Cyber Deterrence issued on February 27, 2017, in which major powers China and Russia, lesser powers Iran and North Korea, and the ISIs are listed as cyber threats to the United States.

Despite the differences in views on cyber security, the United States and China share a common goal of promoting a cyber community with a shared future. The United States has no use for cyber attacks and seeks to establish a normal relationship with China.
drawn on political and ideological basis. Such a discourse is favored and promoted by old and new military industry players and cybersecurity authorities in the United States, pushing the cyberspace towards a time of warfare and fast growing risks.

This kind of anti-Western ideology is the core of the cyber war discourse. Its main characteristics are: the previous generation of political warfare, which primarily involved the military and the economy, and the new generation of social warfare, in which the political warfare component is emphasized. The cyber war discourse reflects the Western worldview of a mixture of the Cold War rhetoric of the 1960s-1980s, and the so-called cold war of civilizations, a theory proposed in the 1990s.

China, on the contrary, has gained in recent years a clearer understanding of the cyberspace and formed a set of its own ideas. It has also established more economic and political confidence. Since President Xi Jinping took office in 2013, China gradually formed its understanding of global governance. On December 16, 2015, Xi proposed at the Second World Internet Conference a cyber community with a shared future. He said that cyberspace is the common space of activities for mankind. The future of cyberspace should be in the hands of all countries. Countries should step up communications, broaden consensus and deepen cooperation to jointly build a cyber community with a shared future. This initiative can be understood in three aspects.

First, in the area of digital economy, China leads the way towards globalization and supports free trade. On January 17, 2017, President Xi explicitly expressed support for economic globalization in his speech at the World Economic Forum, saying that we should seize the opportunities of the new industrial revolution and the digital economy. Then, on May 14, 2017, at the Belt and Road Forum for International Cooperation, Xi elaborated on China’s ideas for globalization from a historical perspective.
Both history and reality show that pride and prejudice are two biggest obstacles to exchanges and mutual learning among civilizations."

China believes the cyberspace is a place where the most extensive communication occurs between civilizations, cultures, and nations and it should not see a repetition of the failures the world had in the physical world or be weaponized based on an absolute division between allies and enemies. Instead, a worldview of reconciliation should prevail in the cyberspace so that different civilizations, cultures, and nations can respect one another and coexist in peace in the cyber world. All in all, a cyber community with a shared future goes beyond the traditional confrontations between powers of the world, welcomes all parties with their own interests and pursuits, and serves as the overarching guideline of China when dealing with issues regarding the cyberspace.