网络安全与网络秩序

第十七辑

中文社会科学索引（CSSCI）来源集刊

复旦国际关系评论

上海人民出版社

网络安全与网络秩序

复旦国际关系评论

中文社会科学索引（CSSCI）来源集刊

第十七辑

上海人民出版社

图书在版编目(CIP)数据

网络安全与网络秩序/沈逸主编.—上海:上海人民出版社,2015
(复旦国际关系评论;第17辑)
ISBN 978-7-208-13436-2

Ⅰ.①网… Ⅱ.①沈… Ⅲ.①计算机网络-安全管理-研究-世界 Ⅳ.①D815.5 ②TP393.08

中国版本图书馆CIP数据核字(2015)第280806号

责任编辑 汪 娜 赵荔红
封面装帧 王小阳

·复旦国际关系评论 第十七辑·
网络安全与网络秩序
沈 逸 主编
世纪出版集团
上海人民出版社出版
(200001 上海福建中路193号 www.ewen.co)
世纪出版集团发行中心发行 常熟市新骅印刷有限公司印刷
开本635×965 1/16 印张11.75 插页2 字数175,000
2015年12月第1版 2015年12月第1次印刷
ISBN 978-7-208-13436-2/D·2768
定价48.00元

复旦国际关系评论
FUDAN INTERNATIONAL STUDIES REVIEW
Vol.17 / 2015

《复旦国际关系评论》第十七辑/2015年
FUDAN INTERNATIONAL STUDIES REVIEW Vol.17/2015
主办单位：复旦大学国际关系与公共事务学院

主编：沈　逸

目 录

Perspectives of International Information Security
国际信息安全问题展望

Institute of Information Security Issues,
Moscow State University
莫斯科国立大学信息安全问题研究所

A.A.Kulpin, P.A.Karasev
安德雷·科尔　高敬文　译*

Threats emanating from Information space require development of international cooperation on a multitude of levels—global, regional and bilateral. The novel concept of International Information Security, introduced by the Russian Federation in Principles of State Policy of the Russian Federation in the field of international information security for the period until 2020, is defined as a state of the global information space which excludes the possibility of violations of the rights of the individual, society and the rights of the state in the information sphere, as well as destructive and unlawful influence on the elements of national critical information infrastructure. This concept will enable the global community to fully embrace all the benefits of the digital age and at the same time to shield itself from threats emanating from global information space.

(应对)信息领域的威胁扩散需要多层次的国际合作——全球性合

* 莫斯科国立大学信息安全问题研究所国际中心主任;高敬文,复旦大学金砖国家研究中心首席信息技术顾问。

作、区域性合作以及双边合作。国际信息安全这一新概念，出自《截至2020年俄罗斯联邦政府国际信息安全领域的国家政策规范》，定义为“一种全球性的信息领域状态，既排除了在信息领域侵犯个人、社会以及国家权益的可能性，也排除了对国家关键信息基础建设元素的破坏性和非法的影响。”这一概念的提出展现了一种可能性，即全球民众在充分享受数字化时代种种便利的同时，又能保护自己远离全球信息领域的风险。

From the standpoint of academia, the priority topics for development of International Information Security are:

从学术角度来看，国际信息安全发展的首要议题如下：

1. Frameworks for Adaptation of International Law to Conflicts in Cyberspace;

2. Improving the Information Security of Critical Infrastructures;

3. Legal and Technical aspects of ensuring Stability, Reliability and Security of the Internet;

4. Challenges of countering the threat of the use of social media for interference in the internal affairs of sovereign states(extremism, radicalization etc.);

5. National Priorities and Business Approaches in the sphere of International Information Security System Development.

1. 调整国际法框架，使之适用于网络领域的矛盾冲突；

2. 改善关键性基础建设的信息安全措施；

3. 从法律和技术层面确保互联网的稳定性、可靠性和安全性；

4. 应对利用社交媒体干涉主权国家内部事务（如极端主义、激进分子等）带来的挑战；

5. 国际信息安全系统开发领域的国家重点和商务渠道。

Considering the topic of **Frameworks for Adaptation of International Law to Conflicts in Cyberspace** there are certain issues, which have to be addressed by joint efforts of governments and academia. The most pressing concern is defining the Principal directions of International Humanitarian Law adaptation to cyberspace. Secondly, we have to overcome the Challenges of international-legal legitimization of International

Humanitarian Law developments with regard to cyberspace. Finally, there is a need in Frameworks of cyberconflicts data objectification and attribution of subjects of cyberattacks. Finding a solution to these issues will make a way to peaceful resolution of cyberconflicts within legal frameworks of International humanitarian Law.

关于第一项议题，**调整国际法框架使之适用于网络领域的矛盾冲突**，有以下几个问题需要政府和学术界的共同努力。首先，最迫切的问题就是确定国际人道主义法在网络领域修订的基本方向。其次，我们需要克服国际人道主义法网络领域修订版的国际法合法化问题带来的挑战。最后，需要对网络冲突数据客体化以及网络攻击对象归属问题建立基本框架。寻求以上问题的答案将在国际人道主义法的合法架构中开辟出一条和平解决网络冲突的道路。

One of the important topics of International Information Security is **Improving of the Information Security of Critical Infrastructures.** Among the crucial challenges in this field are: creation of an international system of Critical Infrastructure(CI) Information Security; development of an international certification system for information systems used in CI; and International and national regulations and standards of CI Information Security. Equally important is international sharing of national best practices of development of Critical Infrastructure(CI) Information Security, international Data sharing on CI cyber incidents and development of cooperation between CERTs with regard to confidence building measures.

国际信息安全的一项重要议题就是**改善关键性基础建设的信息安全措施**。这方面主要的挑战是：创建关键性基础建设(CI)信息安全国际体系；建设 CI 使用的信息系统的国际认证体系；以及制定国际和国内 CI 信息安全标准。还有一个同等重要的问题就是在全球范围分享 CI 信息安全方面的国内最佳实践经验，CI 网络事件数据以及计算机紧急情况响应小组之间合作时建立信任措施方面的经验。

In the modern connected world global communication networks are in the foundation of economic prosperity, scientific advancement and cultural exchange. This raises the importance and level of discussion of **Legal**

and Technical aspects of ensuring Stability, Reliability and Security of the Internet. Among them of particular importance is development of Technical standards and specifications to ensure safety, integrity and reliability of Internet Infrastructure and review and development of International regional and multilateral legal documents relevant to safety, integrity and reliability and legal aspects of technical standardization. Some of these aspects were a subject of discussion in bilateral project of ISI MSU and ICANN *Legal and Technical Aspects of Stability, Security and Resiliency of the Infrastructure of the Global Internet*. Some results have been announced at ICANN meeting 53 in Buenos Aires(Argentina), June 21—25, 2015.

在现代社会,全球互联网络是经济繁荣、科技发展和文化交流的基础。这使得**从法律和技术层面确保互联网的稳定性、可靠性和安全性**这一问题的重要性进一步提升。其中尤为重要的是制定技术标准和规范以确保互联网基础架构和安全性、完整性和可靠性,重估相关技术文档的安全性、完整性和可靠性、合法性,并制定国际、区域及双边法律文档。以上部分内容已经是一个叫作"法律和技术层面看全球互联网基础架构稳定性、安全性和可靠性"的 ISI MSU(莫斯科国立大学信息安全问题研究所)和 ICANN(互联网名称与数字地址分配机构)双边项目的讨论议题,部分结果发表在 2015 年 6 月 21—25 日的布宜诺斯艾利斯(阿根廷)ICANN 53 号会议记录。

The use of ICANN greatly impacts our everyday life, as more and more aspects of human life become dependent on it. This raises the challenge of how to preserve the best opportunities offered by information space and neutralize the adverse and destructive trends of its application—including **the use of social media for interference in the internal affairs of sovereign states(extremism, radicalization etc.).** In particular, we, as academia, must study the benefits and implications of Social media as a new phenomenon of public life and provide analysis and prognosis of use of Social media for destructive purposes. After thorough research certain International and national mechanisms of countering the threat of interference

in the internal affairs of sovereign states can be developed and implemented.

随着人类生活越来越多的方面依赖于 ICTs(信息与传播技术),其应用对我们日常生活的影响越来越深远。这就提出了一项挑战:怎样抓住信息化带来的最佳机遇,与此同时消除其应用带来的不利因素和破坏性的影响——比如**利用社交媒体干涉主权国家内部事务(如极端主义、激进分子等)**。特别地,我们作为学术界人士,必须将社交媒体当作公共生活中的新现象来研究它的优势和影响力,并提供社交媒体用于破坏性目的时的分析和预测结果。经过彻底的研究,才能建设并贯彻执行某些用于反对利用社交媒体干涉主权国家内部事务的国际国内机制。

Considering National Priorities and Business approaches in the sphere of International Information Security System Development it is important to understand the many venues of international cooperation in development of International Information Security. First and foremost, it is bilateral cooperation and agreements. In 2013 first such document has been drafted and signed between Russia and the USA: *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building*. In 2015 a much more broad *Intergovernmental agreement between Russia and China on cooperation in the field of ensuring international information Security* has been signed. The purpose of this Agreement is to offer legal and organizational bases for cooperation between Russia and China on International Information Security.

考虑到国际信息安全系统开发领域的国家重点和商务渠道,理解许多国际信息安全发展方面的国际合作场景是很重要的。首先,最重要的就是,这是一种双边合作协议。2013 年,美俄起草并签署了第一份这样的协议:《美俄总统关于在新领域开展互信建设合作的联合声明》。2015 年,中俄签署了一份内容更广泛的协议:《中俄关于确保国际信息安全领域合作的政府间协议》。这份协议的目的是为中俄在国际信息安全领域的合作提供法律和组织基础。

Equally important is multilateral cooperation on both global and regional level. Representative fora and organizations such as Shanghai Co-

operation Organization and BRICS greatly help the convergence of views of different countries. In 2009, the Agreement has been made among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security. The more recent Dushanbe Declaration of SCO(2014) clearly represents active development and progress in the sphere of International Information Security, as it says that States-members will promote joint efforts to build a peaceful, secure, fair and open information space, based on the principles of respect for state sovereignty and non-interference in the internal affairs of other countries.

全球和区域层面的多层次合作同样重要。如上海合作组织(SCO)和金砖国家(BRICS)这样有代表性的论坛和组织在收集汇总不同国家观点方面起到了很大的作用。2009 年,上海合作组织成员国政府就确保国际信息安全领域的合作达成共识。最新的上海合作组织杜尚别声明(2014)中明确展示了在国际信息安全领域的积极发展和进步,声称其成员国将基于尊重国家主权和不干预他国内政的原则,合作建立一个和平、安全、公正、公开的信息空间。

At a global level the most important international venue for discussions of issues associated with information security has always been the UN, and these issues have been on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly. Since then there have been annual resolutions on Developments in the field of information and telecommunications in the context of international security and reports by the Secretary-General to the General Assembly with the views of UN Member States on the issue. More importantly, there have been four Groups of Governmental Experts(GGE) with the mandate to examine the existing and potential threats from the cyberspace and find possible ways to address them. The first successful GGE report(of the second GGE) was issued in 2010(A/65/201). The third GGE continued the work of its predecessor and the report of the 2012/13 Group of Governmental Experts was presented to the 68th session of the General Assembly in September 2013(A/68/98). The

new GGE, with 20 experts, held its first meeting in New York in July 2014, and elected Brazil as the Chair. The Group would report to the General Assembly in 2015.

全球层面讨论信息安全相关议题的最重要的国际场合一直是联合国,这类议题从1998年俄罗斯在联合国大会第一委员会上首次提出决议草案后就列入了联合国议事日程。从那以后就有了年度决议《国际安全角度看信息和电信领域发展》,并由秘书长在大会上就联合国成员国在此问题上的意见作报告。最重要的是,大会选举出四个政府专家组(GGE)审核信息空间已有的和将来可能出现的威胁,并找出可能定位它们的方式。首次成功的政府专家组报告(第二届 GGE)发布于2010年(A/65/201)。第三届GGE延续了前任的工作,并于2013年9月(A/68/98)在第68届大会上提交了2012—2013年度政府专家组报告。新一届的政府专家组有20位专家,2014年7月在纽约举办了第一届会议,并选举出巴西作为会议主席。专家组将于2015年再次向联合国大会提交报告。

The work at the UN goes beyond GGE, as member-states regularly submit their proposals on the issue to the United Nations General Assembly. On 12 September 2011, four members of the SCO presented a Draft International Code of Conduct for Information Security. The code of conduct gave rise to extensive international attention and discussion after it was distributed as a document of the General Assembly (A/66/359). Recently, on January 9, 2015 the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan submitted a revised code of conduct(A/69/723), taking into full consideration the comments and suggestions from all parties.

联合国的工作不仅仅是政府专家组报告,成员国还需要在联合国大会上定期提交议题相关的建议,2011年9月12日,四个上海合作组织的成员国提交了一份国际信息安全行为准则草案。这份行为规范草案加入了大会文档(A/66/359),随后引起了广泛的国际关注和讨论。最近,2015年1月9日,在充分考虑各方的意见和建议后,中国、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦和乌兹别克斯坦常驻联合国代表提交了行为准则修订版(A/723/69)。

Another important tool for discussion of issues of International Information Security is *Track 1.5*(venues with participation of government officials and independent experts). One of the fine examples of *Track 1.5* is an annual International Forum State, Civil Society and Business Partnership on International Information Security held in April in Garmisch-Partenkirchen(Germany). The main goal of the Forum is to exchange experiences of representatives of Russian and foreign state, academic and business institutions, members of International Information Security Research Consortium(IISRC) on the current issues of International Information Security. IISRC meets twice a year and serves as a site for multiple projects. As of now IISRC has achieved wide representation with 22 organizations from 15 countries. Among priorities and research projects of the Consortium are:

讨论国际信息安全议题的另一重要工具是 1.5 轨道(Track 1.5)(由政府官员和独立专家构成)。Track 1.5 的一个不错的例子就是每年 4 月在加米施-帕滕基(德国)举办的国际论坛《国际信息安全相关的国家、民间社团和企业合作伙伴》。这一论坛的主要目标是让俄国和外国代表、学术和商业机构、国际信息安全研究协会(IISRC)成员之间交流国际信息安全相关问题的经验。国际信息安全研究协会每年开两次会并为许多项目提供服务。迄今为止国际信息安全研究协会已经得到来自 15 个国家的 22 个组织的广泛支持,协会的重点关注和研究项目如下:

1. Escalatory Models: Development of shared models of escalation in cyber conflict, including definitions of hostility levels;

2. Civilian Infrastructures: International legal status of civilian cyber infrastructures in the context of peace or war;

3. Cyber Definitions: Definitions of information warfare and cyber defense topics;

4. Cyber Law: International legal frameworks to increase stability of intergovernmental relations and promote orderly international economic processes;

5. Codes of Conduct: Development of shared norms for behavior in

cyber space for individuals, countries and non-state actors;

6. Cyber Terrorism: International agreements to counter non-state actors seeking to launch cyber attacks on countries or provoke conflicts among countries using cyber means;

7. Cyber Crime: Legal and technical coordination against cyber crime;

8. Technical Cooperation: International mutual assistance across public and private spheres to improve cyber situational awareness, enhance protection of critical infrastructures and respond to significant cyber failures or attacks;

9. Protection of the Commons: Framework to separate technical architectures and operation of cyber space from economic and political issues and provide separate mechanisms on the technical plane or the political economic level for resolving differences or marshalling international cooperation;

10. Industrial Espionage: International legal framework for industrial espionage whether sponsored by states or whether its fruits are purchased on criminal black markets by states.

1. 升级模型：开发应对网络冲突升级版的共享模型，包括敌方等级的定义；

2. 民用基础设施：在和平或战争背景下民用基础设施网络的国际法律地位；

3. 网络定义：信息战和网络防御课题的定义；

4. 网络法：用于增加政府间关系的稳定性，促进有序的国际经济进程的国际法律架构；

5. 行为规范：制定个人、国家和非国家团体在网络空间中的统一行为规范；

6. 网络恐怖主义：全球达成共识反对非国家团体寻找机会对国家发动网络袭击，或用网络手段激起国家间的冲突；

7. 网络犯罪：为防止网络犯罪而进行的法律和技术协作；

8. 技术合作：公共和私人领域的全球互助合作，以增进对网络势态的敏感，加强关键性基础设施的保护，应对显著的网络故障和攻击；

9. 保护公共空间：建立框架将技术架构和网络空间运作与经济政治议题分离，并为技术层面或政治经济层面解决分歧开展国际合作提供独立的机制；

10. 工业间谍：针对工业间谍建立的国际法律架构，不论间谍行为是否由国家资助，也不论其目标是否在黑市上流通。

One of the examples of fruitful collaboration in IISRC is a Russia-U.S. Bilateral projects on Cybersecurity: Critical Terminology Foundations (2011) and Critical Terminology Foundations 2.0(2013). The goal of these projects has been to discuss and come up with consistent terms (twenty in each project) that define cyber and information security and thus provide a solid foundation for development of common understanding of the issues at hand and at the same time to aid in negotiation process.

国际信息安全研究协会合作项目硕果累累，其中一个例子就是美俄网络安全双边项目：核心术语基础(2011)和核心术语基础 2.0(2013)。这些项目的目标是讨论并确定出一套定义网络和信息安全的统一术语(每个项目二十个)，这样才能为手头议题达成统一理解提供一个坚实的基础，在项目协商过程中起到辅助作用。

All members of the international community recognize the existence and significance of Information Security Issues. Information security issues are in the focus of attention of political leaders of major world powers. The goal of all stakeholders, including governments, academia and business community is to design and deploy a system of knowledge, skills and standards of the global information security culture—a system of International Information Security.

国际社会的所有成员(已经)正视信息安全议题的切实存在及其重要性。这些议题已经成为世界主要大国领导人关注的焦点。所有利益相关方——包括政府、学术界以及企业界的目标是：设计和部署一个关于全球信息安全文化的知识、技能和标准的机制——国际信息安全机制。

信息安全与国际关系

王世伟*

【内容提要】 信息安全作为非传统安全的重要领域和当代面临的全球性重大挑战，正在对当代国际关系产生重要影响，信息安全已成为经济全球化的重要考量、世界多极化的重要博弈和国际关系民主化的重要议题。

【Abstract】 Information security is an important area of non-traditional security and a major challenge toward the global society. Information security is becoming an important factor in economic globalization, world multi polarization, the democratization of international relations and the rule of law, which has become an important consideration of economic globalization, an important game of world multi polarization, and an important issue in the democratization of international relations.

* 王世伟，上海社会科学院信息研究所研究员。