

法律视角下的 全球网络安全态势及对策

Global Cyberspace Security Situation
and Countermeasure from the Legal Perspective

(汉英对照)

许 坚 主编

法律视角下的 全球网络安全态势及对策

Global Cyberspace Security Situation
and Countermeasure from the Legal Perspective

(汉英对照)

许 坚 主编

人民法院出版社

图书在版编目 (CIP) 数据

法律视角下的全球网络安全态势及对策 : 汉英对照 / 许坚

主编. -- 北京 : 人民法院出版社, 2018.1

ISBN 978-7-5109-2052-3

I. ①法… II. ①许… III. ①计算机网络—科学技术

管理法规—研究—汉、英 IV. ① D912.104

中国版本图书馆 CIP 数据核字 (2018) 第 020303 号

法律视角下的全球网络安全态势及对策 (汉英对照)

许坚 主编

责任编辑 : 兰丽专 赵作棟

出版发行 : 人民法院出版社

地 址 : 北京市东城区东交民巷 27 号 (100745)

电 话 : (010) 67550565 (责任编辑) 67550558 (发行部查询)
65223677 (读者服务部)

客服 QQ : 2092078039

网 址 : [http : //www.courtbook.com.cn](http://www.courtbook.com.cn)

E - mail : courtpress@sohu.com

印 刷 : 三河市国英印务有限公司

经 销 : 新华书店

开 本 : 787 × 1092 毫米 1/16

字 数 : 166 千字

印 张 : 15.75

版 次 : 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷

书 号 : ISBN 978-7-5109-2052-3

定 价 : 158.00 元

版权所有 侵权必究

序 言

习近平总书记高度重视互联网安全问题，指出：安全是发展的前提，发展是安全的保障，安全和发展要同步推进，“没有网络安全就没有国家安全，没有信息化就没有现代化。”^① 在中国共产党第十九次全国代表大会上，习近平总书记在报告中多次提到互联网。由此可见，网络安全已上升到同政治安全、经济安全、领土安全并驾齐驱的战略高度，成为国家安全的重要组成部分。全球范围内已逐渐形成一个无边界的网络空间，每个国家都面临着共同的风险和挑战。因此，如何建立基于自愿基础上有效的国际合作以应付日趋严重的信息安全挑战，是亟待加强研究的。

现阶段，我国正在全面推进依法治国，加快建设社会主义法治国家。党的十八大以来，中国共产党加快建设社会主义法治国家，并把全面依法治国提高到“四个全面”战略布局的新高度，开启了加快建设法治中国的新征程。网络的发明和普及，印证了科技发展与法律进步之间的辩证关系。就目前来看，网络的发展已走在法律的前面，相应地，网络也为法治建设开辟了新的渠道和领域，注入了新的动力，也改变了法律规则、原则的一些本质特点。时代赋予互联网治理法治化的历史机遇，法律必然也要因势而谋、应势而动、顺势而为，从我国现实出发，从未来发展着眼，探索出有中国特色的、与国际接轨的全球网络安全应对策略。

^① 摘自2014年2月14日习近平在中央网络安全和信息化领导小组第一次会议上的讲话。载人民网——中国共产党新闻网。<http://cpc.people.com.cn/xuexi/n/2014/1120/c385475-26061137.html>，访问时间：2018年1月18日。

本书就脱胎于农业社会、发展固定于工业社会的传统法学理论以及司法实践如何应对互联网发展的挑战进行了分析，对于具有稳定性、滞后性的法律和发展一日千里的互联网之间如何进行平衡进行了研究，就法学理论和立法司法如何进行时代性更新、回应进行了解答。编写组成员不仅学有专攻，长期以来从事互联网法律研究，而且娴于技术，全书各章节有大量第一手互联网技术资料支撑，因此，本书对技术操作、数据逻辑的描述是精准、权威的。从计划到出版，编写组成员广泛搜集资料，推敲分析精义，采撷最新动态，甚至几易其稿，力求融会贯通，实现言之有据、言之有物、言之有理、言之有度。

全书共五部分。第一部分为日益严峻的全球网络安全形势，第二部分结合具体的 WannaCry 事件进行了分析、反思，第三部分对未来网络安全热点及趋势进行了预测，第四部分提出了维护网络安全的国际行为准则，第五部分讲述维护网络空间安全的中国行动。这一编排体例结构清晰、一目了然，使得整个研究围绕中心有针对性地进行集中论述。较之以往类似主题的研究，本书紧跟我国法治发展趋势，在兼顾系统性、完整性、通俗性的同时，强调针对性、应用性和前沿性，贡献独特、意义重大。

相信《法律视角下的全球网络安全态势及对策》的出版能为我国学界和实务界提供有价值的素材，为构建和平、安全、开放、合作的网络空间提供有益借鉴，为建立多边、民主、透明的全球互联网治理体系提供有效支持，为完善网络空间安全治理对话协商机制提供技术支撑，为制定更加公正合理的全球网络空间治理规则提供法律基础。故，欣然为之序。



2018年1月18日于北京

目录

CONTENTS

背景

第一部分

日益严峻的全球网络安全形势

一、网络威胁影响国家政治军事安全 / 7

(一) 敏感信息泄漏影响政治安全 / 7

(二) 网络攻击影响国家军事安全 / 7

(三) 网络攻击规模将会不断加剧 / 8

二、网络的强依赖性导致灾难性后果 / 9

(一) 对工业系统的攻击波及面广 / 9

(二) 对金融系统的攻击日益严重 / 10

(三) 核设施遭打击后果难以预测 / 11

(四) 网络攻击造成社会运转瘫痪 / 12

三、网络攻击全方位威胁商业的发展 / 13

(一) 大型关键企业是主要攻击点 / 13

(二) 网络攻击窃取金融商业机密 / 15

(三) 企业邮箱存在严重安全风险 / 16

四、网络安全关涉每一个体切身利益 / 19

(一) 超半数网民通讯信息被泄漏 / 19

(二) 网络诈骗侵害个体财产权益 / 21

(三) 网络入侵危及个体生命安全 / 22

五、企业网络安全防护存在严重不足 / 24

(一) 恐暴露问题而存在侥幸心理 / 25

(二) 重自身损失而忽略社会责任 / 25

(三) 动态防御应急缺乏相应意识 / 26

第二部分

WannaCry 事件分析及其反思

一、WannaCry 事件的背景及其影响 / 31

(一) WannaCry 事件的发生背景 / 31

(二) WannaCry 事件的空前影响 / 32

二、WannaCry 技术分析及攻击流程 / 32

(一) “三位一体”新型网络病毒 / 33

(二) WannaCry 的整体攻击流程 / 36

三、WannaCry 与永恒之蓝关系分析 / 37

(一) 永恒之蓝研发及泄漏的简介 / 37

(二) WannaCry 攻击与永恒之蓝 / 39

(三) 外国军用武器民用化的初次尝试 / 40

四、关于 WannaCry 事件的安全反思 / 42

(一) 企业网络安全防护现存问题 / 42

(二) 网络恐怖主义威胁逐渐显现 / 47

(三) 网络攻击向各智能终端蔓延 / 48

(四) 网络安全维护需国家和企业联动 / 49

五、WannaCry 事件的法律视角分析 / 49

第三部分

未来网络安全热点及趋势预测

一、网络漏洞及其攻击威胁持续蔓延 / 53

(一) 金融网站漏洞威胁更加复杂 / 53

(二) 网站挂马攻击将会重新兴起 / 53

(三) 劫持智能硬件致使隐患迭出 / 54

二、高级持续性威胁将会呈现新特点 / 55

(一) APT 对基础设施的攻击日益活跃 / 55

(二) 对特定个人移动端攻击增多 / 56

三、互联网应用环境安全愈加不可控 / 57

(一) 未知威胁挑战传统检测方法 / 57

(二) 安全事件挑战企业响应能力 / 58

(三) 应用环境安全越来越不可控 / 58

(四) 关键信息基础设施防护不足 / 60

第四部分

维护网络安全的国际行为准则

一、公共权力主体的行为准则 / 64

(一) 有责任 and 权力维护本国网络安全 / 65

(二) 加强漏洞管理从而减少网络威胁 / 66

(三) 妥善应对 APT 攻击相关网络犯罪 / 67

(四) 支持军民融合发展促进社会协作 / 68

(五) 通过国内立法进行网络武器管控 / 69

(六) 应就网络武器管控达成国际条约 / 70

(七) 建立网络武器泄露外交通报机制 / 71

二、网络运营主体的行为准则 / 72

(一) 提供安全的网络服务和运行环境 / 72

(二) 确保网络数据和个人信息的安全 / 73

(三) 对供应链及其员工加强网络安全教育 / 74

(四) 以积极的态度参与网络安全建设 / 74

(五) 建立数据驱动协同联动防御体系 / 76

(六) 建立有效网络安全应急响应体系 / 77

三、网络安全企业的行为准则 / 78

(一) 规范网络安全漏洞挖掘行为 / 78

(二) 保障网络用户个人信息安全 / 79

(三) 参与网络安全信息共享活动 / 79

(四) 应对网络安全重大突发事件 / 80

四、网络用户主体的行为准则 / 81

(一) 加强网络安全意识, 抵御网络安全威胁 / 81

(二) 承担依法用网责任, 履行文明上网义务 / 82

(三) 利用投诉举报机制, 发挥社会监督作用 / 83

第五部分

维护网络空间安全的中国行动

一、维护网络安全法律路径 / 87

(一) 确立科学的网络安全立法思路 / 87

(二) 强调预防对网络安全维护的重要性 / 89

(三) 通过法律解释合理化法律适用 / 89

二、加强网络安全支持力度 / 90

(一) 通过政治决策强调网络安全重要性 / 90

(二) 立法保障信息共享和人才培养 / 91

(三) 提高网络安全保障的财政投入 / 94

三、着力培养网络安全人才 / 95

(一) 网络安全人才培养纳入国家战略 / 95

(二) 建立世界一流网络安全学院 / 96

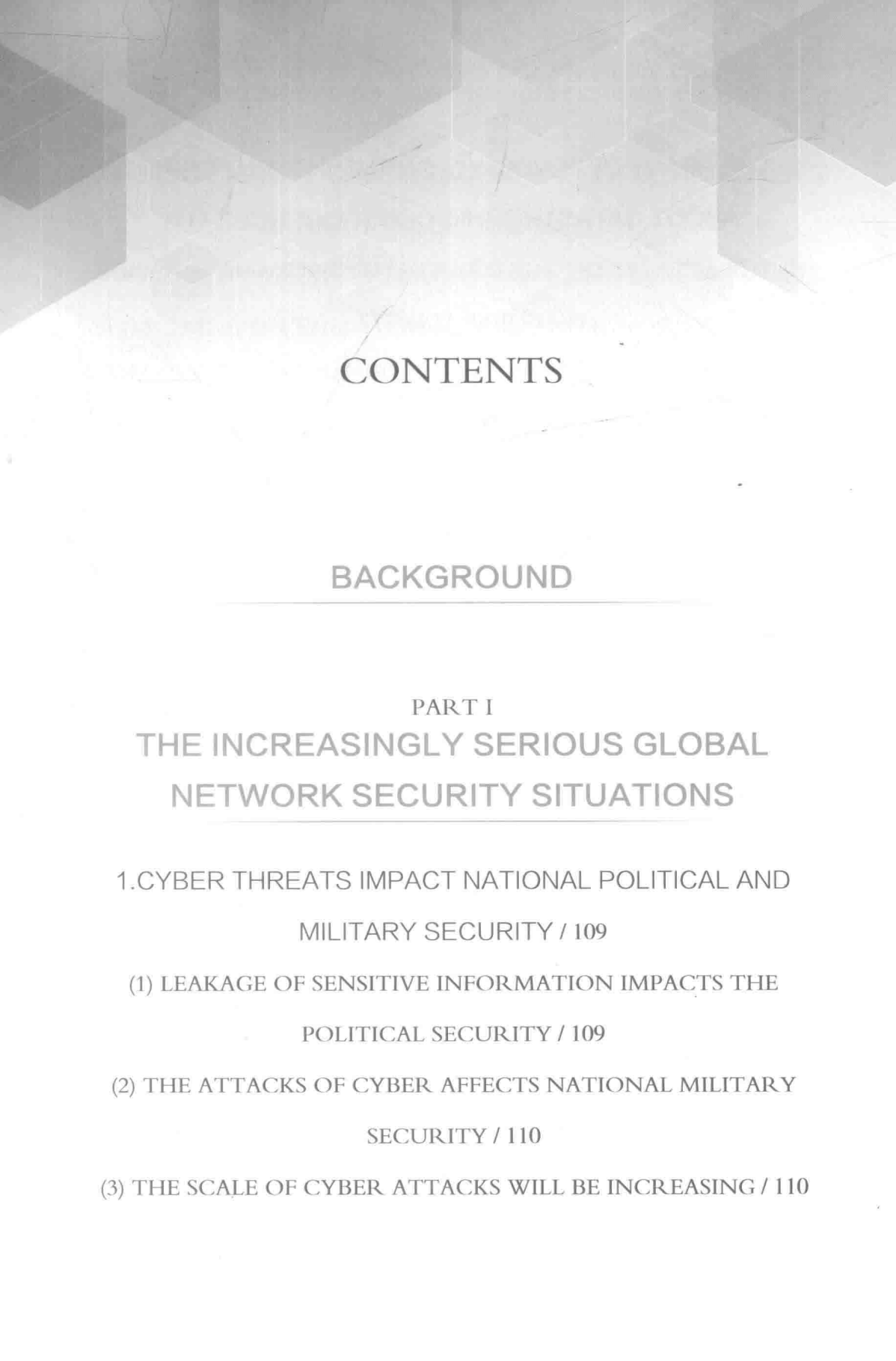
(三) 增强网络安全教育的实践性 / 97

四、落实网络安全保障义务 / 98

(一) 更新服务提供者的安全理念 / 98

(二) 强化对网络主体行为的管理 / 98

(三) 建立网络安全责任追究机制 / 99



CONTENTS

BACKGROUND

PART I

THE INCREASINGLY SERIOUS GLOBAL NETWORK SECURITY SITUATIONS

1. CYBER THREATS IMPACT NATIONAL POLITICAL AND MILITARY SECURITY / 109

(1) LEAKAGE OF SENSITIVE INFORMATION IMPACTS THE POLITICAL SECURITY / 109

(2) THE ATTACKS OF CYBER AFFECTS NATIONAL MILITARY SECURITY / 110

(3) THE SCALE OF CYBER ATTACKS WILL BE INCREASING / 110

2. THE HEAVY DEPENDENCY ON THE INTERNET BRINGS ABOUT CATASTROPHIC CONSEQUENCES / 111

(1) THE ATTACKS ON THE INDUSTRIAL SYSTEM HAVE A WIDE
COVERAGE / 112

(2) THE ATTACKS ON FINANCIAL SYSTEM ARE MORE AND MORE
SERIOUS / 113

(3) IT IS DIFFICULT TO PREDICT THE CONSEQUENCES OF
ATTACKS TO NUCLEAR FACILITIES / 114

(4) CYBER ATTACKS CAUSE PARALYSIS TO SOCIAL OPERATION / 116

3. CYBER ATTACKS COMPREHENSIVELY THREATEN THE BUSINESS DEVELOPMENT / 118

(1) LARGE KEY ENTERPRISES ARE THE MAIN ATTACKED POINTS / 118

(2) THE ATTACKS OF CYBER STEAL FINANCIAL BUSINESS SECRETS / 120

(3) THERE IS A SERIOUS SECURITY RISK IN ENTERPRISE MAILBOX / 121

4. CYBER SECURITY IS RELATED TO EACH INDIVIDUAL'S VITAL INTERESTS / 126

(1) MORE THAN HALF OF INTERNET USERS' COMMUNICATION
INFORMATION IS LEAKED / 126

(2) CYBER FRAUD INFRINGES INDIVIDUAL PROPERTY RIGHTS
AND INTERESTS / 128

(3) CYBER INTRUSION ENDANGERS INDIVIDUAL LIFE
SECURITY / 130

5. THE ENTERPRISE CYBER SECURITY PROTECTION EXISTS

SERIOUS INSUFFICIENCY / 132

(1) FEAR OF EXPOSURE PROBLEMS AND HAVE FLUKE MIND / 132

(2) FOCUSING ON THEIR OWN LOSSES AND IGNORING SOCIAL
RESPONSIBILITY / 133

(3) LACK OF CORRESPONDING AWARENESS OF DYNAMIC
DEFENSE AND EMERGENCY RESPONSE / 134

PART II

WANNACRY INCIDENT ANALYSIS AND ITS REFLECTION

1. THE BACKGROUND OF WANNACRY INCIDENT AND ITS EFFECTS / 139

(1) THE BACKGROUND OF WANNACRY INCIDENT / 139

(2) THE UNPRECEDENTED EFFECT OF THE WANNACRY
INCIDENT / 140

2. WANNACRY TECHNICAL ANALYSIS AND ATTACK PROCESS / 141

(1) “TRINITY” NEW INTERNET VIRUS / 141

(2) WANNACRY’S OVERALL ATTACK PROCESS / 145

3. ANALYSIS OF THE RELATIONSHIP BETWEEN WANNACRY AND THE ETERNAL BLUE / 146

(1) BRIEF INTRODUCTION TO ETERNAL BLUE R & D AND
LEAKAGE / 146

(2) WANNACRY ATTACK AND THE ETERNAL BLUE / 148

(3) THE INITIAL ATTEMPT OF CIVILIAN USE OF MILITARY
WEAPONS / 150

4. SECURITY REFLECTION ON WANNACRY INCIDENT / 152

(1) EXISTING PROBLEMS OF ENTERPRISE CYBER SECURITY
PROTECTION / 152

(2) THE THREAT OF CYBER TERRORISM IS EMERGING / 159

(3) CYBER ATTACKS SPREAD TO THE INTELLIGENT TERMINALS / 160

(4) CYBER SECURITY MAINTENANCE NEEDS NATIONAL AND
ENTERPRISE LINKAGE / 161

5. ANALYSIS OF WANNACRY INCIDENT FROM LEGAL PERSPECTIVE / 162

PART III

THE FUTURE CYBER SECURITY HOT SPOTS AND TREND FORECAST

1. THE NETWORK VULNERABILITIES AND THEIR THREAT OF
ATTACK CONTINUES TO SPREAD / 167
 - (1) FINANCIAL SITES' VULNERABILITY THREATS ARE MORE
COMPLEX / 167
 - (2) EMBEDDING TROJAN IN SITE WILL BE RE-EMERGING / 168
 - (3) HIJACK SMART HARDWARE TO CAUSE HIDDEN DANGER / 169
2. THE HIGH-LEVEL SUSTAINABLE THREAT WILL SHOW NEW
FEATURES / 170
 - (1) ATTACKS ON INFRASTRUCTURE ARE BECOMING
INCREASINGLY ACTIVE / 170
 - (2) ATTACKS ON SPECIFIC INDIVIDUAL MOBILE TERMINALS
INCREASE / 171
3. INTERNET APPLICATION ENVIRONMENT SECURITY IS
INCREASINGLY UNCONTROLLABLE / 173
 - (1) UNKNOWN THREATS CHALLENGE TRADITIONAL DETECTION
METHODS / 173

(2) SECURITY INCIDENTS CHALLENGE ENTERPRISE RESPONSE

CAPABILITIES / 174

(3) THE APPLICATION ENVIRONMENT SECURITY IS MORE AND

MORE UNCONTROLLABLE / 175

(4) LACK OF PROTECTION FOR CRITICAL INFORMATION

INFRASTRUCTURE / 177

PART IV

INTERNATIONAL CODE OF CONDUCT FOR CYBER SECURITY MAINTENANCE

1. THE CODE OF CONDUCT FOR PUBLIC POWER

SUBJECTS / 183

(1) HAVE THE RESPONSIBILITY AND POWER TO MAINTAIN THEIR

OWN COUNTRY'S CYBER SECURITY / 184

(2) STRENGTHEN VULNERABILITY MANAGEMENT TO REDUCE

CYBER THREATS / 186

(3) PROPERLY DEAL WITH CYBER CRIMES RELATED TO APT

ATTACKS / 187

(4) SUPPORT MILITARY AND CIVILIAN INTEGRATED

DEVELOPMENT AND PROMOTE SOCIAL COOPERATION / 189

(5) CONTROL CYBER WEAPONS THROUGH DOMESTIC

LEGISLATION / 190