SUMMARY

FROM THE EDITOR

7 **Our Cyber Optimism** — *Mikhail Yakushev*

Never before were the issues of information security and internet governance reviewed in a single Russian paper, with topics ranging from digital diplomacy to information warfare and from tackling *next Stuxnet* to transforming ICANN. Young but thorough experts differ in their approaches from *cyber optimism* praising digital millennium to *cyber alarmism* fearing cyberwars and total disintegration of global information space. This is how the future is born — when meteor development of technologies outgrows its analytical and scientific reflection, and only the young and ambitious ones are able to catch it.

Key words: *information security, Internet governance.*

INTERVIEW

11 **How to Avoid Conflict Escalation in Cyberspace?** — *Jamie Saunders*

Is it possible to establish a legally binding international regime in the field of cybersecurity? Could the Budapest Convention on Cybercrime be regarded as a potential basis for establishment of a global mechanism aimed at countering cybercrime? Correspondent of *Security Index* journal addressed these questions to the Director of International Cyber Policy at the UK Ministry of Foreign Affairs.

Key words: *information security, cyber crime, international legal regime, cybersecurity.*

17 **Information Technologies in Russia: Challenges and Prospects** — *Andrei Kolesnikov*

Today Russian and foreign experts, business leaders and diplomats are trying to foresee the future of Cyrillic domain zone — with many related issues also being in the focus of attention. Does Russia need a new doctrinal basis for effective cybersecurity policies, and do recent innovations in Russian internet security legislation reach their goal in fact? What are the priorities for Coordination Center of National Internet Domain .RU (CCNID), the administrator of *.ru* and *.рф* domains? Director of the CCNID highlighted these issues for Security Index journal.

Key words: *information security, critical infrastructure protection, domain name system, cyberstrategy, internet regulation*.

23 **New Technologies in Intelligence** — *Chris Pallaris*

What is the key difference between open source intelligence and traditional intelligence activities conducted by national secret agencies? What factors have spurred the development of open source business intelligence in recent years? How and to what extent do new information and communication technologies contribute to the development of open source intelligence markets? These and other questions are answered by the director and chief consultant of *i-intelligence* company.

Key words: *intelligence, information and communication technologies, the Internet*.

29 **Internet-2012 and the International Policy** — *Mikhail Yakushev*

Modern global architecture and basic functions of the internet almost did not change drastically over last years. Key rules of internet governance are still based upon a few basic principles, which include universal routing order of information and technical messages among internet hubs and translation of IP-address into unique domain names. Without following these simple rules proper addressing in the Net would be impossible. However, in recent years creation of new domain zones bolstered further blurring of borders between geographical domain zones and the general ones.

***Key words**: information security, cyber crime, the international legal regime, Internet governance, international security.*

43 **Global Internet Governance in the Context of Modern International Law** — *Madina Kasenova*

It would not be correct to describe the global network as a purely technical invention. Internet integrates physical, financial, intellectual, humanitarian, political, social and other resources that affect national and international processes in social and economic spheres — and also provides communication links on a worldwide scale. The Global Network due to its technological nature has to have a transnational character — partially due to the fact that its technical backbone is designed to provide global coverage. The international character of the Internet dictates the logic of its governance.

***Key words**: Internet, information security, global internet governance, domain name system, ICANN.*

65 **Social Networking Services in the Context of International and National Security** — *Oleg Demidov*

The role of social networks in today's world is not limited to being a conduit for social upheavals and protest actions, even if we limit the scope of discussion to their effects on national or international security. The use of social network services in the interest of national and international security is possible, and it has already been actively developing in many directions e.g. crowdsourcing; forming the information picture of events and shaping public opinion, informing about emergency situations etc. However, in Russia the potential of social networking services in these areas has not received due attention from governmental bodies.

***Key words**: social networking services, international security, the Arab Spring.*

87 **Identification in the Internet: International and Political Issues** — *Mikhail Yakushev*

Identification of internet users, owners of internet content and technical infrastructure, as well as persons providing various services via the internet, has undoubtedly become one of the hottest topics of discussions between representatives of government agencies and the expert community. As a rule, Russian officials and experts tend to recognize the need for more comprehensive, systemic and effective government regulation in the area of identification in cyberspace. As part of the overall effort to prevent crime, Russian law-enforcement agencies have repeatedly proposed a legal ban on anonymity in cyberspace. But the problem has an obvious international, or rather, international-policy dimension owing to the international nature of the internet itself.

***Key words**: global internet governance, user identification, authentification, cyberstrategy, Identity Ecosystem, cyberlaw, cybercrime.*

103 **Policy Approaches of the Central Asian States towards Internet Governance and Information Security** — *Galiya Ibragimova*

In Central Asia where only a few years ago the problem of digital divide was one of the most pressing, modern information and communication technologies (ICT) are actively developing today. The Internet has not yet become a common commodity for most of people — but it's not a rarity anymore. Tragic events in southern Kyrgyzstan in 2010 could be regarded as an evidence of strong impact of social networks and new ICT on social and political processes in the region.

***Key words**: Central Asia, internet, information security, information and communication technologies, social networking services.*

129 **International Information Security and Russia's National Interests** — *Oleg Demidov*

The use of sophisticated malwares against Iran's critical infrastructure — including *Stuxnet, Duqu, Gauss, Flame*, etc. — brings to a focus the aim of reaching a legally binding international agreement that would prohibit coordinated cyberattacks against nuclear infrastructure and most sensitive industrial objects. If Russia manages to promote this idea in the international arena under the proper angle there would hardly be anyone to object. Washington, if still decides to do it would risk to find itself nearly in an isolation being supported only by Israel. Besides, by denying constructive potential of this proposal the White House is likely to provoke criticism of a significant part of its own expert community.

***Key words**: international information security, cybersecurity, cyberstrategy, information and communication technologies, cyberlaw, internet security regulation.*

169 **China's Strategy in Cyberspace: the Issues Internet Governance and Information Security** — *Galiya Ibragimova*

China is aware that in case of a direct confrontation with the USA its army is would not able yet to respond adequately. Therefore, to achieve and maintain parity with the West the PRC became actively engaged in development of cyber capabilities enough to pull down the entire IT infrastructure of the enemy in case of a conflict. China's key weakness is its inability to conceive new technologies itself. The ICT applied and developed in China are usually either copied or modified samples of foreign technology. This situation is pushing the country towards the path of catch-up modernization as a means to overcome its current inability to generate its own strategic pieces of innovation.

***Key words**: China, information security, information and communication technologies, cyberwar, cyberespionage.*

ROUND TABLE

185 **International Information Security and Global Internet Governance: a View from Geneva in the Eyes of Russian and International Experts** — *Ben Baseley-Walker, Constance Bommelaer, Markus Kummer, Vladimir Orlov, Jaroslaw Ponder, Walter Reed, Victor Vasiliev, Rolf Weber, Mikhail Yakushev*

The first 12 years of the XXI century were marked by revolutionary changes stemming from skyrocketing development of information and telecommunication technologies world over. Those changes affected virtually all dimensions of social processes, including international relations — from social and political change in the Arab world to an unprecedented growth in politically motivated hacktivism draining national secrets out to open network as well as in development of cyberwarfare and cyberespionage tools. At the same time, there is growing global concern over ways of preventing wars in cyberspace. The internet itself and its evolution do not univocally define all of these processes, still they certainly provide fundamental basis for their further development.

***Key words**: information security, cybercrime, cyberwar, international security regime.*

COMMENTARY

207 **Cyber-Resilience: The Essence of Cyberpeace** — *Hamadoun Touré*

We live in a world which now has more than six billion mobile cellular subscriptions, and where there will soon be two and a half billion people using the internet. This global hyperconnectivity allows us to leverage the power of technology — and especially mobile technologies — to make the world a better place. Unfortunately, however, this indispensable new infrastructure also brings with it new challenges for preserving peace and stability.

***Key words**: cyber-resilience, information security, cyberlaw, cyberspace.*

213 **U.S. Digital Diplomacy: Opportunities and Threats to International Security** — *Elena Zinovieva*

The term *digital diplomacy* which is used alongside with terms *internet diplomacy, social network diplomacy* and *WEB 2.0 diplomacy*, was initially applied to the US foreign policy only. In particular, it implied wide use of new information and communication technologies

including the new media, social networks, blogs and other media platforms in the internet. Today digital diplomacy programs have been conducted not only by the USA but also by a number of other states. How do things work in Russia? — starts her article the researcher at MGIMO University.

***Key words**: digital diplomacy, US, Russia, international security, cyberpower, soft power.*

229 **Flame in Cyberspace** — *Oleg Demidov, Maxim Simonenko*

The aim is, first, to introduce the very notion of politically motivated aggressive behavior in cyberspace into political and diplomatic agenda. Second, to build a truly global regime aimed at tackling cyber threats not limited to the Council of Europe's Convention on Cybercrime. The final aim is to define political, diplomatic and international legal status of cyberspace in the context of national and international security. For Moscow the question is mainly whether it will be possible to launch this process before another supersophisticated virus hits Russian strategic networks instead of Iranian ones.

***Key words**: critical infrastructure protection, malware, cyberweapon, Middle East.*

233 ***Stuxnet* and Nuclear Enrichment of International Information Security Regime** — *Maxim Simonenko*

After appearance of *Stuxnet* malware, supposedly targeted at Iran's nuclear infrastructure, the importance of interconnection between nuclear and information technologies has increased drastically. Experts and IT-specialists are convinced that the experience of nuclear era could be used in order to strengthen global cybersecurity regime.

***Key words**: critical infrastructure protection, malware, cybersecurity, information security.*

L I B R A R Y

249 **Richard Clarke's Cyberwar and Cyberpeace** — *Oleg Demidov*

In most respects, the United States is the most cyber- dependent nation in the world — so that even to optimize industrial processes, the SCADA systems are often be connected not just to local networks but to the internet. A specific matter of concern for authors is the vulnerability of generation systems and power greed, which are mostly privately owned in the USA. Power greed became the most targeted object for numerous proxy actors and hackers who have already packed its networks with *trap doors* and *logic bombs* pretty hard to track and deactivate.

***Key words**: cybersecurity, cyberwar, USA, China critical infrastructure protection.*

B O O K R E V I E W S

253 *Andrey Baklitsky, Elena Chernenko, Oleg Demidov, Maksim Simonenko* — PIR Center staff, interns and alumni review new additions to PIR Center library.

T O T H E E D I T O R

261 **Information Security Today: Illogic of Development** — *Alexander Fedorov*

271 S U M M A R Y

275 A B O U T T H E A U T H O R S

279 P I R C E N T E R A D V I S O R Y B O A R D

283 S U S T A I N A B L E P A R T N E R S H I P W I T H R U S S I A G R O U P

284 I N T E R N A T I O N A L E X P E R T G R O U P

S E C U R I T Y P U Z Z L E S

Cov.III **29 Words About Cybersecurity**