VOLUME 7, ISSUE 2, 2016

per Concordiam

Journal of European Security and Defense Issues

- **BALTIC CYBER DEFENSE**
  Nations sign important agreement

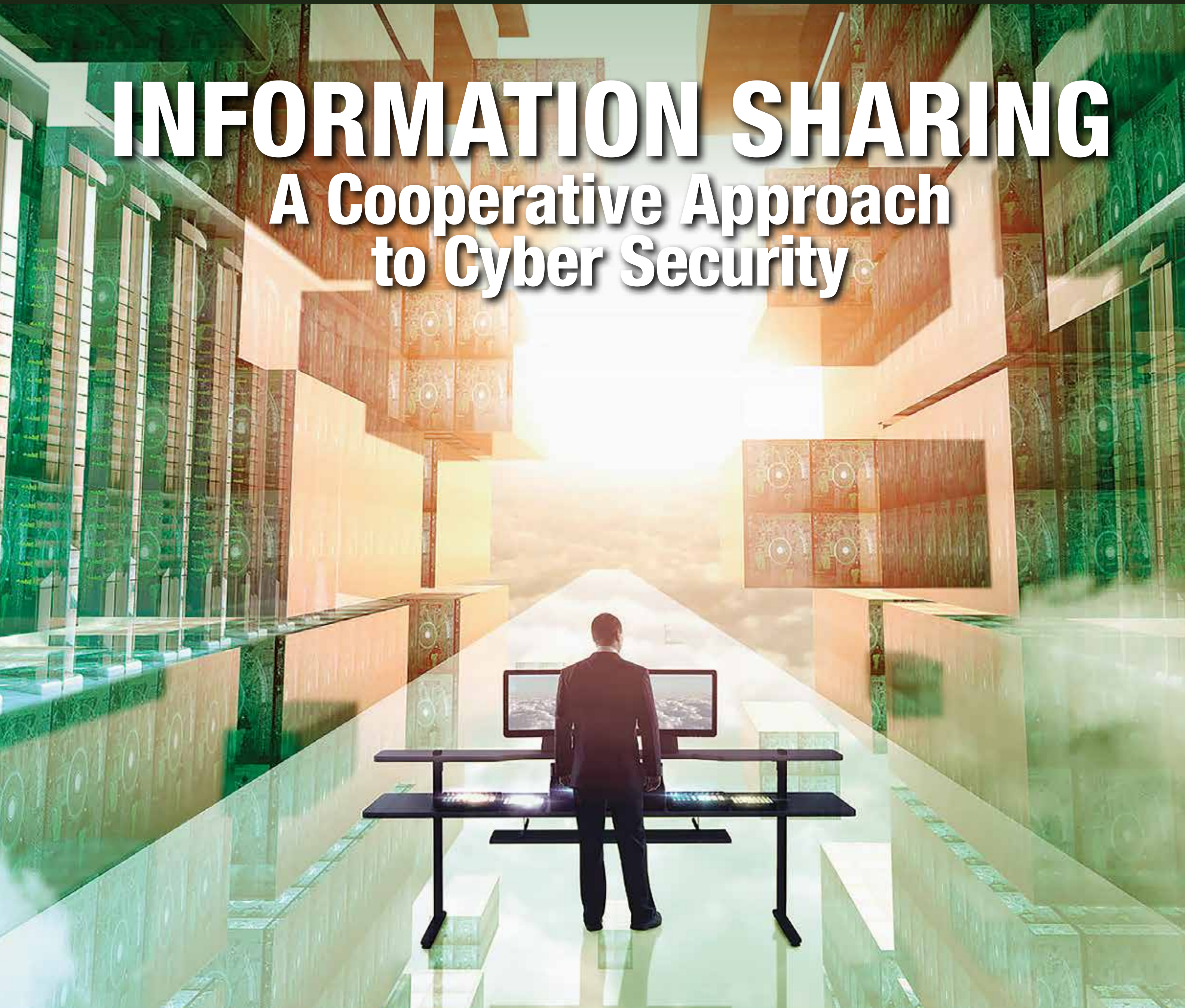
- **CYBER TERRORISM**
  Categorizing attacks by severity

- **PROTECTING UKRAINE**
  Kyiv faces an array of threats

- **BATTLING BOKO HARAM**
  Nigeria's online war against extremism

PLUS

Partnership for Peace
Kazakhstan seeks security
Georgia's approach to cyber



INFORMATION SHARING

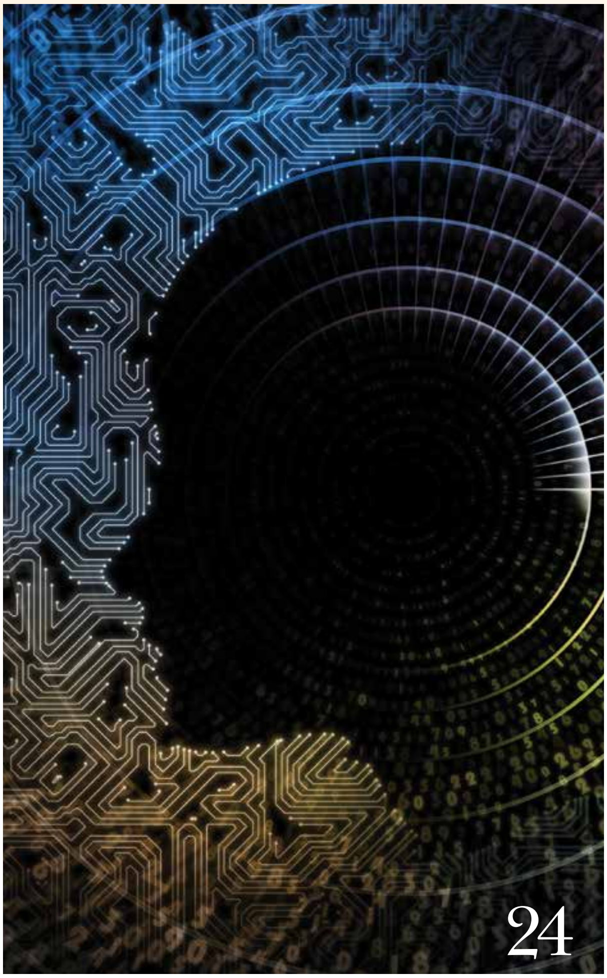
A Cooperative Approach to Cyber Security

Table *of* Contents

features

ON THE COVER

Cyber attacks rarely recognize national borders. So the strategies aimed at preventing, deflecting and responding to these attacks must also be regionally and globally oriented. GETTY IMAGES



28

52

in every issue

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 26th issue of *per Concordiam*. Cyber security is one of the most important challenges we face. The globally interconnected and interdependent cyberspace underpins modern society and provides critical support for the world economy, civil infrastructure, public safety and national security. Information technology has transformed the global economy by connecting people and markets around the world. To realize the full potential of the digital revolution, users require confidence that their sensitive information is secure and commerce and infrastructure is not compromised. States need safe and resilient networks that support national security and prosperity.

The development and implementation of national cyber-security strategies are necessary for countries to protect their cyber-critical infrastructure and mitigate cyber threats. Protecting cyberspace requires strong vision and leadership as well as the ability to manage continuous changes in priorities, policies, technologies, education, laws and international agreements. The highest levels of government, industry and civil society must demonstrate genuine commitment to cyber security for nations to innovate and adopt cutting-edge technology while protecting national security, the global economy and individual free expression. As an example, NATO responds to millions of constantly evolving cyber threats in defense of communications and information systems owned and operated by the alliance, all while enhancing inclusive information-sharing relationships with industry and academia.

Information sharing is vital to cyber security. It ensures that information circulates between the government and private sectors and among private sector entities themselves. Information sharing can facilitate faster recognition of a cyber threat and organized countermeasures against cyber threats. Network security information exchanges can be set up to facilitate information sharing among public and private sector stakeholders.

The Marshall Center's Program on Cyber Security Studies (PCSS) resident course includes presentations and discussions on strategy and policy solutions in support of cyber security. The course also includes modules on cyber-security strategy development, cyber governance, public-private partnerships, whole-of-government solutions and the importance of critical infrastructure protection. The demand for more cyber-focused education and training is enormous, and I encourage you to take a proactive role by enhancing cyber security within your organization. Innovative actions by leaders in all organizations are necessary to address the complex strategic, policy and technical challenges within the cyber domain.

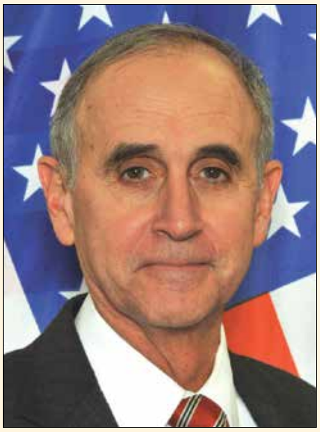
This edition of *per Concordiam* offers suggestions for addressing the top challenges in cyber security, including:

- Strengthening national cyber-security efforts across the whole of society
- Enhancing critical infrastructure security and resilience
- Strengthening public-private partnerships
- Empowering individuals and protecting privacy
- Deterring, discouraging, and disrupting malicious activity in cyberspace
- Improving cyber-incident response

We invite your comments and perspectives on this subject. Your responses may be included in our upcoming edition, which will address countering transnational criminal organizations. Please contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director



Keith W. Dayton

Director, George C. Marshall European Center for Security Studies

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor's degree in history from the College of William and Mary, a master's degree in history from Cambridge University and another in international relations from the University of Southern California.

Daniel P. Bagge is head of strategy and policy at the National Cyber Security Center, National Security Authority of the Czech Republic. He holds a master's in international security studies from a postgraduate program jointly offered by the Marshall Center and the Universität der Bundeswehr München.

Andria Gotsiridze is director of the Cyber Security Bureau of the Ministry of Defence of Georgia. He is an expert in security sector reform, fighting corruption and foreign intelligence. Under his leadership, the bureau developed Georgia's first cyber security defense policy and strategy and has initiated ongoing cyber security projects.

Anna Gussarova is a senior research fellow at the Kazakhstan Institute for Strategic Studies. She teaches diplomacy and international terrorism courses at the German-Kazakh University in Almaty. She holds a bachelor's in American studies and a master's in Central Asia security studies from the same university.

Alvaro José Chaves Guzmán is director of public security and infrastructure for the Colombian Ministry of National Defense. Previously, he served as advisor to the deputy minister of defense for politics and international affairs and was secretary to the deputy minister of defense for strategy and planning. He holds a bachelor's in political science and a master's in international relations and negotiation from Los Andes University.

Aaron Hughes is U.S. deputy assistant secretary of defense for cyber policy. He specializes in innovative technologies for the intelligence community. He holds a bachelor's from the University of Virginia, a master's in telecommunications and computers from George Washington University, and a master's in business administration from the Stanford Graduate School of Business.

Natalia Spinu leads the Cyber Security Center of the Republic of Moldova. She has been department chief of Moldova's Special Telecommunications Centre and project coordinator at the Centre of Information and Documentation on NATO. She is a 2012 graduate of the Marshall Center's Program in Advanced Security Studies and has a master's from the European Institute of the University of Geneva.

Martina Ulmanova is a cyber security policy specialist at the National Cyber Security Center in the Czech Republic. Her experience focuses on the field of cyber security exercises. In addition, she lectures at universities on the topic of cyber security. She holds a master's in strategic and security studies from Masaryk University in Brno.

per
Concordiam

Journal of European Security and Defense Issues

Defending Cyberspace

Volume 7, Issue 2, 2016

George C. Marshall European Center for Security Studies

Leadership

Keith W. Dayton
Director

Ben Reed
U.S. Deputy Director

Johann Berger
German Deputy Director

Marshall Center

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The center promotes dialogue and understanding between European, Eurasian, North American and other nations. The theme of its resident courses and outreach events: Most 21st century security challenges require international, interagency and interdisciplinary response and cooperation.

Contact Us

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam is a professional journal published quarterly by the George C. Marshall European Center for Security Studies that addresses defense and security issues in Europe and Eurasia for military and security practitioners and experts. Opinions expressed in this journal do not necessarily represent the policies or points of view of this institution or of any other agency of the German or United States governments. All articles are written by *per Concordiam* staff unless otherwise noted. Opinions expressed in articles written by contributors represent those of the author only. The secretary of defense determined that publication of this journal is necessary for conducting public business as required of the U.S. Department of Defense by law.

ISSN 2166-322X (print)
ISSN 2166-3238 (online)

per Concordiam is ONLINE

Stay digitally attuned to global security issues relevant to Europe and Eurasia

per Concordiam is a professional journal published quarterly by the George C. Marshall

http://perconcordiam.com

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org

Astana, Kazakhstan

THE ASSOCIATED PRESS

KAZAKHSTAN ADAPTS TO THE CYBER AGE

RAPID CHANGES PRESENT HOST OF CHALLENGES FOR THE CENTRAL ASIAN COUNTRY

By Anna Gussarova, Kazakhstan Institute for Strategic Studies

The influence of information and communication technologies in all spheres of human life has created new vulnerabilities. The structure of social relations and the role of states have radically changed. Cyber espionage is booming internationally, casting doubt on the effectiveness of the international legal regime. Changes in the balance of power in virtual space can lead to changes in the geopolitical balance of power. States not only operate directly in cyber space, but also actively take opportunities to discredit their political and economic competition in the real world. Defense systems and critical infrastructure have become vulnerable.

Over the past few years, Kazakhstan has integrated into the global information community at an impressive pace. Insufficient attention to new opportunities, as well as to risks and threats, can damage a country's development and push it to the periphery of international relations. In this regard, there is a need for permanent monitoring and situational analysis to adequately perceive the situation in terms of its rapid and fundamental mobility.

THE IT REVOLUTION

The rapid development of information technologies has led to the establishment of a new competitive environment in international relations, where cyber technologies play a crucial role in daily life. This is the main front in the battle for research, technical, political and economic superiority.

Digital technology development is an expensive industry, requiring huge investments not only in the hardware and digital media, but also in training personnel in its use. As a result, traditionally key actors in international relations such as the United States, the United Kingdom, China, and to some extent Russia, have retained their leading positions.

The Internet is no longer just a secure system to transmit electronic messages. It is now a place where literally millions of people live and work, buy and sell things, arrange online auctions, build families, discuss topics of interest, have fun and express themselves in different ways. Another important consequence of cyber technologies is the reduced capacity for keeping state secrets. The Edward Snowden case is an example of such insecurity.

International cyber-espionage capabilities and international penetration into national sectors of cyberspace have raised questions on the viability of the principle of state sovereignty. These new vulnerability parameters have raised the issue of cyberspace regulation under international law.

There are two main approaches; however, they are not mutually exclusive, but rather rely on different emphases. The first involves global efforts, led by the Council of Europe, through the Convention on Cybercrime to develop common security standards which could establish a basis for combating cyber threats and regulating interstate relations in the field. The second prioritizes national cyber security systems based on capabilities and interests which could establish global rules of behavior in cyberspace. The actions of technologically advanced states indicate that the second approach is currently predominant.

KAZAKHSTAN AND CENTRAL ASIA

Central Asian states remain on the periphery of the spread of information technologies. However, digital technologies are rapidly beginning to play an important role in government and society in the region. At the same time, Central Asian countries often face criminal cyber attacks, primarily aimed at financial fraud.

According to Kaspersky Security Network, Kazakhstan has been the target of 85 percent of Internet-based attacks in the region, compared with 8 percent in Uzbekistan, 4 percent in the Kyrgyz Republic, 2 percent in Turkmenistan and 1 percent in Tajikistan. The majority of cyber attacks were aimed at government websites to get financial information. It is believed that most crimes are committed in cyberspace by hackers from local organized crime groups seeking lucrative financial and industrial data.

According to World Bank data, over 10 million people use the Internet in Kazakhstan every month, or approximately 60 percent of the population. In rural areas, Internet penetration is much lower, at about 30 percent. However, the trend is sharply upward, because the ratio of Internet users has risen from 0.5 percent in 2000 to 15 percent in 2008 and 41 percent in 2011. The average user is male, age 15 to 35, with an average or high income, or a student.

E-commerce makes up only 0.45 percent of the total retail market in Kazakhstan; however, experts think that in 2015 as much as 4 percent of retail sales worth $3 billion may have been completed via e-commerce. In its 2014 e-government survey, the United Nations ranked Kazakhstan 28th out of 193 countries in e-government development, 23rd in e-participation and 23rd in online services.

The emergence of e-government has contributed to changes in the relationship between societies and their governments in favor of democratization, as well as to a reduction in spending on administration. At the same time, networking (in its cybernetic and social dimensions) has resulted in the loss of governmental monopoly on the exercise of power, defined as the possibility to influence activities and behavior and set trends in social behavior. It is obvious that the ability, primarily technical, to influence informational content enables the manipulation of social awareness.

Cyber security is a relatively new topic in Kazakhstan, and data protection has become of great importance to the state and individuals. Some cyberspace trends in Kazakhstan are:

- Increased access to information resources (Internet, digital television, mobile telephony, modern technology)
- Increased computer literacy and involvement of citizens in the information sphere (e-learning, e-banking, e-money, e-commerce, mPOS-terminals Pay-me, online shopping)
- Transformation of many spheres of public life on the basis of widespread improvements in information and communications technologies (ICT) (introduction of e-government, Operation Control Center, unified control systems)
- Integration into global information space

CYBER TECHNOLOGIES PENETRATION

E-government

Kazakhstan is a leader in providing electronic public services. Of the 675 government services, 236 are e-government accessible through e-gov.kz, and 77 are available online (about 11.4 percent).

The public e-procurement portal www.goszakup.gov.kz, operated by the Center for Electronic Commerce LLP, was established in 2010. In 2011, two systems began operations; a system of electronic licensing for private companies and a unified "e-notary" and "e-akimat" system for district administrations. Since 2012, the online platform www.egov.kz has integrated the databases of the Ministry of Health, the Ministry of Interior and the Civil Registry Office. Also on this website, you can pay 21 state payments, 16 state duties, four types of taxes and fines for traffic violations. In April 2012, 1 million digital signatures — an electronic signature that identifies citizens — were issued.

According to government statistics, by May 2012 the number of egov.kz users had increased 122 times, with 25-30 visits per day. Six percent of the population uses e-gov, and this is strongly increasing. According to data from the Program for the Development of Information and Communication Technologies, the portal received 5.2 billion tenge ($34.5 million) in 2013 and 9.7 billion tenge ($64.5 million) in 2014.

Kazakhstan established Zerde national ICT holding, which is a state-owned company for the development of modern information and communication technologies. A national "cloud" is under development to house the country's state IT-infrastructure.

E-commerce

The depth of Internet penetration in Kazakhstan has created rapid growth in e-commerce. Online trade volumes increased by 300 percent in 2011 and 180 percent in 2012. According to government statistics, the annual volume of e-commerce in 2012 approached $400 million (0.7 percent of the market), and in foreign shops Kazakhs spent more than $1.3 billion.

Kazakhstan's e-commerce marketplace consists of more than 500 online shops. Kazakhs had 13 million credit cards as of April 2013, according to the National Bank of Kazakhstan. Firms such as JSC Kazkommertsbank, Air Astana, JSC Kazakhstan Temir Zholy, Sulpak, Technodom and Meloman are successfully engaging in online commerce.

CYBER CHALLENGES

With the positive ICT developments in Kazakhstan come increasing challenges in information and cyber security. Kazakhstan is 18th in the world in spam received and the seventh most dangerous place to surf the Web. According to a December 2014 Kaspersky Labs security bulletin, "during 2013, the IT-infrastructure of 92 percent of organizations in the country were subjected to an external cyber-attack at least once, and 66 percent of companies faced internal threats to information security."

Mobile devices now represent an increasing threat. Eighty-five percent of companies in Kazakhstan have had at least one information security incident. In only the first half of 2013, Kaspersky Labs registered more than 53,000 unique samples of malicious code aimed at mobile devices.

In addition, in 2013 every second user in the country (55.5 percent) was subjected to a cyber attack. Kaznet registered more than 76 million instances of malware in 2013-2014. Residents from Almaty, Atyrau and Shymkent (western and southern parts of the state) face cyber threats and challenges most frequently.

The development of global cyberspace by public institutions is a huge step toward sustainable development. However, according to the feedback of iProf-2012 Internet conference participants, the security of state websites in Kazakhstan is quite low and requires much more attention (99 percent are unable to repel attacks by hackers). A good example of this vulnerability was a 2012 hacker attack on the official website of the Ministry of Culture and Information.

Today, skimming is not widespread in Kazakhstan, but the number of cyber attacks by this method grows, as it does all over the world. For example, in 2013 citizens of Romania and Moldova were detained in Almaty for stealing data card holders at ATMs using skimming devices, Tengri News reported. The number of cyber attacks through mobile banking and cyber fraud on the stock market is also rapidly growing.

There have been several cyber attacks on e-government, for example, when hackers tried to destroy the site of e-gov.kz as well as the official blog platform of the government of Kazakhstan (2009); an attack on the website of the National Space Agency of Kazakhstan (2010); an attack on the website of the Committee on Intellectual Property Rights of the Ministry of Justice (2012); and an attack on the official website of the Agency for Combating Economic and Corruption Crimes, the financial police (2012).

CYBER LEGAL FRAMEWORK

In Kazakhstan, cyber security initiatives often come from the head of state. In particular, during the jubilee Shanghai Cooperation Organization summit, President Nursultan Nazarbayev introduced the concept of "electronic boundaries" and creating a special unit within the organization to police Internet aggression. He also introduced the term "electronic sovereignty" into international law. At the 66th session of the United Nations General Assembly in 2011, Nazarbayev proposed that the adoption of a Treaty on Global Cyber Security be accelerated.

Kazakhstan and other participating OSCE states have built a legal framework for cyberspace. In recent years, Kazakhstan has adopted a number of bills relating to e-government, e-money, e-commerce, intellectual property, and so forth.

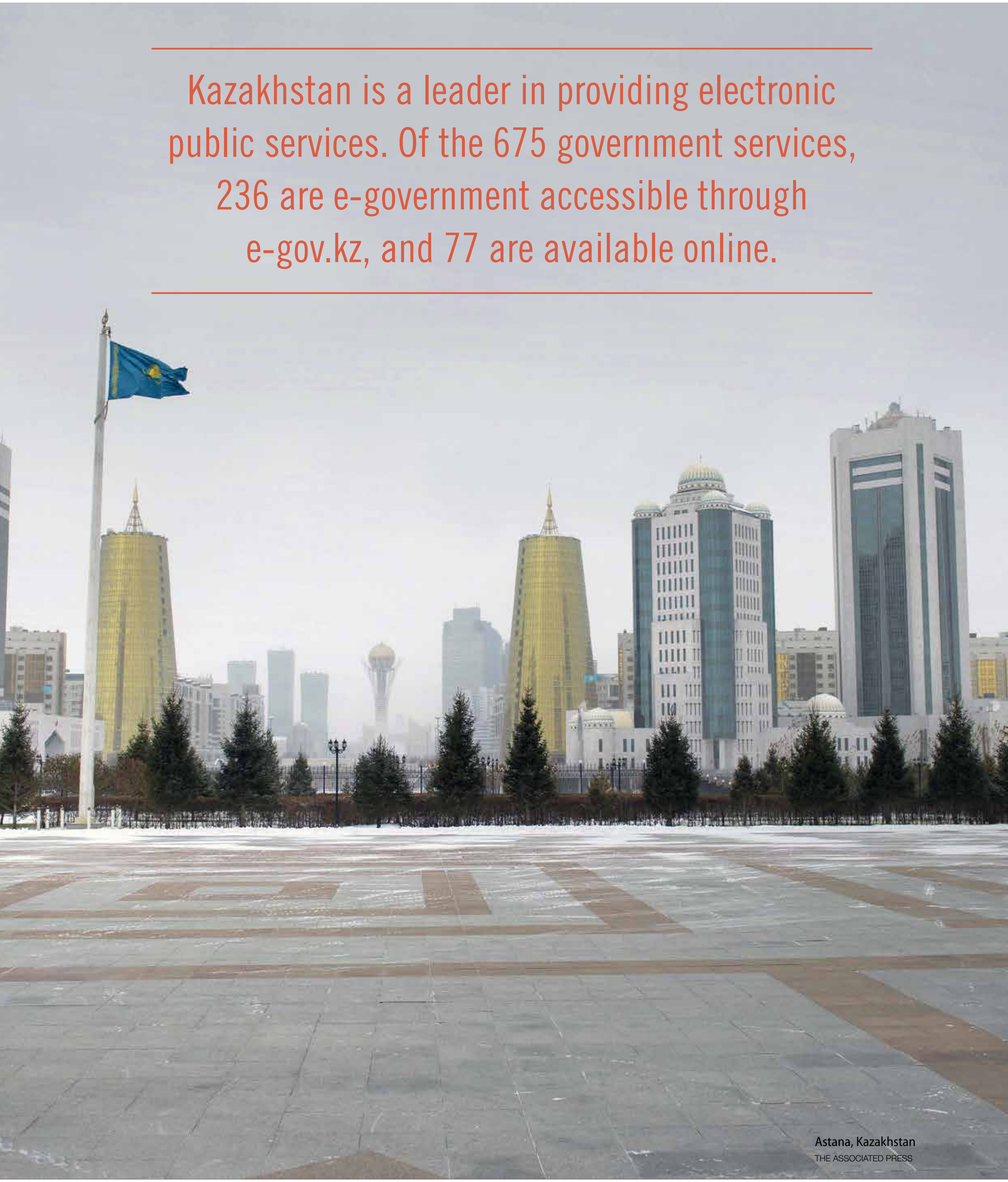
On a conceptual level, there is no clear understanding of the difference between "information space" and "cyberspace." In Kazakhstan, legal and regulatory terminology virtually eliminates the "cyber" prefix (cyberspace, cyber security, cyber crime, cyber war). The official terminology for these concepts was replaced with the more broad "information" prefix (information space, information security, information war). However, in extensive use of both variants in the media and in general, they are regarded as equivalent.

In 2013, the president signed a decree approving the state program, On Information Kazakhstan-2020, to help create the conditions for Kazakhstan's transition to an information society. The program was jointly developed by the Ministry of Transport and Communications and concerned experts. It aims to improve the efficiency of public administration, the availability of information infrastructure and the development of national information space. It is expected that through the introduction of ICT, the system of governance would be optimized, as well as open, and "mobile government" would be established. However, issues of information security were not addressed.

According to World Bank data, over 10 million people use the Internet in Kazakhstan every month, or approximately 60 percent of the population.

It should be noted that cyber security and cyber crime in Kazakhstan are, to a great extent, in the economic sphere, assessing material and intellectual resources of companies, relations with partners on corporate and production issues and the state of institutional links. Kazakhstan's criminal codes are evidence of this. Under the criminal code of Kazakhstan, economic crimes using high technology are of two variations: "illegal access to computer information, establishment, use and distribution of malicious computer programs" and illegally changing cellular unit subscriber identification codes.

Kazakhstan is a leader in providing electronic public services. Of the 675 government services, 236 are e-government accessible through e-gov.kz, and 77 are available online.



Astana, Kazakhstan
THE ASSOCIATED PRESS

Generally speaking, data from 2004 to 2010 clearly indicate the intensive growth of this type of crime: 26 crimes in 2004, 713 in 2005, 1,437 in 2006, 1,622 in 2008, 2,196 in 2009 and 2,423 in 2010. Though there is no available data for more recent years, there is a high probability that the upward trend has continued.

A new draft of the criminal code clarifies criminal offenses against security of information technology and envisaged the introduction of 10 amendments to cover offenses such as unauthorized access, illegal modification or illegal distribution of information; computer sabotage; creation, use or distribution of malicious computer programs and software; and rules violations in operating information system, among others.

At the institutional level, the president issued a message in 2010 establishing the Computer Emergency Readiness Team of Kazakhstan (KZ-CERT) to protect against cyber threats, ensure information and communication technologies and maintain cyber security. Its functions include the analysis of information, viruses, security codes and programs for "botnets" found in .kz domains, and law violations (pornography, violence, copyright infringement, etc.) by users of KazNet. KZ-CERT assists in responding to a denial of service (DoS, DDoS), burglary/assault on online resources, establishment and distribution of malicious software, phishing on the Internet, viruses and botnets.

IT THREAT AWARENESS

Low cyber threat awareness among IT users complicates the protection of Kazakhstan's national cyberspace. According to Kaspersky Lab, about 17 percent of mobile device users take no special actions to protect passwords to financial and/or payment services, while 39 percent of users worldwide prefer to use only one or just a few passwords for the full range of sites they visit. Awareness of cyber threats is critically low — only 6 percent of respondents are familiar with vulnerabilities and "zero day" attacks, 21 percent are somewhat aware, and 74 percent do not have any idea in this area. For example, only 4 percent of respondents were aware of the Zeus/Zbot Trojan virus, which infected 196 countries around the world, while 73 percent were completely unaware.

Low cyber threat awareness leads to noncompliance with basic rules of information security. In addition, more than half of Kazakh companies (52 percent) do not allocate time and resources to the development of IT-security policies and purchasing of licensed versions of antivirus programs. Thus, Kazakhstan has an urgent need to raise threat awareness in public institutions, private enterprises and among ordinary Internet users. As of April 2016, government agency employees will be required to leave smartphones and tablets at entrance checkpoints to minimize confidential information leakage via WhatsApp and other messengers. For example, in the U.S. there are programs to educate high school students and teachers as well as the general public on information security, and federal government employees undergo information security training.

IT EXPERTISE IS LACKING

Today, Kazakhstan has a severe shortage of skilled IT specialists. It is difficult to retain staff with technical skills because of the high demand for such skills on the global labor market. Eighty-seven percent of Kazakh companies have IT specialists who are unable to adequately assess new threats and to prevent their occurrence. Meanwhile, according to Kaspersky Lab, corporate IT infrastructure, which can be infected through employees' mobile devices, is a prime target for cyber attacks. Kazakhstan needs to better attract and retain highly skilled information security professionals.

A primary objective of strengthening the nation's cyber security is the development of public-private partnerships. Today, cooperation between the state and private companies in the field of cyber defense is critically low. There is also a lack of cooperation between public institutions and private companies in computer technology and software development. Good cyber security requires further development of cooperation between the government and public-private partnerships — operators of critical infrastructure and the state.

NEW CYBER SECURITY MEASURES

Kazakhstan's new law, On Telecommunications, in effect since January 1, 2016, implements national security certificates for Internet users. All cyber operators are obliged to pass traffic using a protocol that supports encryption using the security certificate, except for the traffic encrypted by means of cryptographic protection. The national security certificate aims to protect Kazakhstanis at home while using encrypted protocols when accessing foreign Internet resources.

There are many challenges to implementing the law throughout the country and the project will cost millions of dollars. However, as Kazakhstan advances into the cyber age, the government must take steps to protect its networks, critical infrastructure and citizens from the expanding range of new threats. □