VOLUME 7, ISSUE 2, 2016

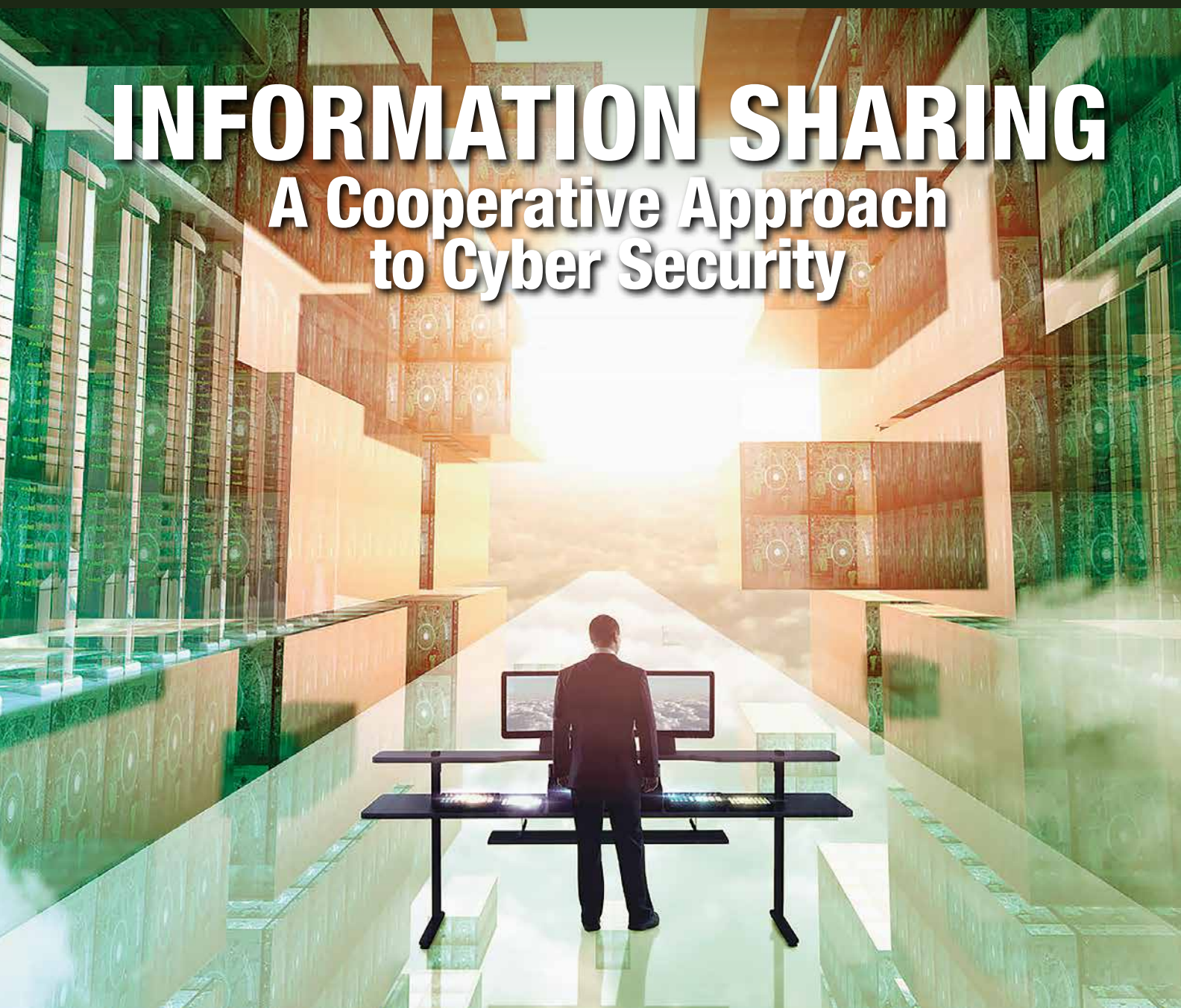
per Concordiam

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

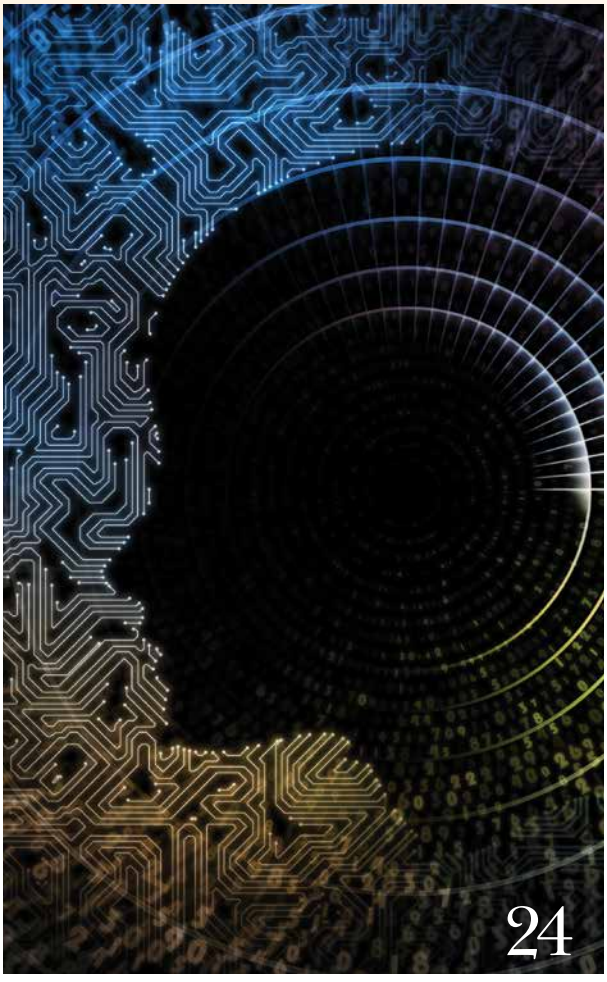
A Cooperative Approach to Cyber Security

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



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.

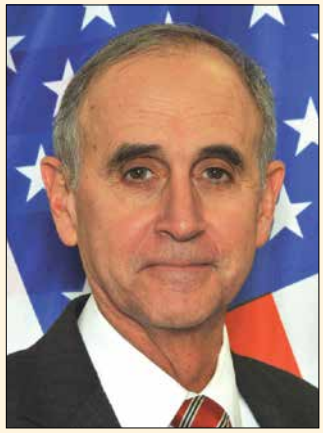
This edition of *per Concordiam* offers suggestions for addressing the top challenges in cyber security, including:

- 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

http://perconcordiam.com

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

Building Deterrence in CYBERSPACE

The U.S. Department of Defense's new strategy focuses on prevention

By **AARON HUGHES**, U.S. deputy assistant secretary of defense for cyber policy

Malicious actors in cyberspace pose a complex and dynamic set of threats that leaders and policymakers will need to address in the 21st century. The cyber threat against United States' interests is increasing in severity and sophistication, and it comes from state and nonstate actors alike.

Just as nation-states have advanced cyber capabilities and strategies ranging from stealthy network penetration to intellectual property theft, criminal and terrorist networks are also increasing their cyber capabilities and operations. The low cost and global proliferation of malware have lowered barriers to entry in this domain and have made it easier for smaller actors to strike out maliciously in cyberspace. The world is also seeing blended state and nonstate threats in cyberspace, which not only have the potential to undermine stability, but complicate potential responses for the U.S. Department of Defense (DoD) and for others.

During the last few years, numerous high-profile malicious cyber or cyber-enabled events have grabbed the public's attention, including incidents that have affected Sony Pictures Entertainment, the U.S. Office of Personnel Management, the DoD unclassified Joint Staff network, the French TV5 Monde network and the Ukrainian power grid. These continuing high-profile incidents make it only natural for national security professionals and international relations scholars to question whether anything can be done to deter malicious activity in cyberspace.

This is an important question that the DoD is working to answer, since we rely heavily on cyberspace for virtually everything we do. The DoD has three missions in cyberspace. The first is defending our own networks, systems and information. Second is to defend the U.S. and its interests against cyber attacks of significant consequence. Our third mission is to provide integrated cyber capabilities, including offensive cyber options, which, if directed by the president, can augment our other military capabilities.

Adm. Michael Rodgers, commander of U.S. Cyber Command, director of the National Security Agency and chief of Central Security Services, leads U.S. efforts to combat 21st century cyber threats. AFP/GETTY IMAGES

Fostering Cyber Deterrence

In the face of the growing cyber threat and the need to fulfill our cyberspace missions, the DoD is developing and implementing a comprehensive strategy to deter cyber attacks against the department and U.S. interests. One challenge is ensuring that the strategy is broad enough to address the wide variety and number of threat actors in cyberspace. The strategy must also take into account the types of cyber attacks we are trying to deter. Given the sheer scale of cyberspace and the broad availability of malware, the DoD must face the reality that it is impossible to deter all cyber attacks. As the DoD continues to build its Cyber Mission Force and its overall cyber capabilities in the face of the escalating threat, the DoD believes that deterring cyber attacks on U.S. interests will best be achieved through the totality of U.S. actions and capabilities. This includes key elements and tools such as U.S. declaratory policy, enhanced indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. Deterring state and nonstate groups in cyberspace requires a whole-of-government approach, and the DoD will play its part as one of the instruments of national power available to the president.

Deterrence works by persuading a potential adversary that it will suffer unacceptable costs in response to an attack (cost imposition) and by decreasing the likelihood that any attack will succeed (denying the objective). As such, the U.S. must be able to declare and display effective response capabilities to deter an adversary from initiating a cyber attack; develop effective defensive capabilities to deny a potential cyber attack from succeeding; and strengthen the overall resilience of U.S. systems in the event that a cyber attack does penetrate our defenses. As part of an effective deterrent posture, the U.S. requires strong intelligence, cyber forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution. Here is a closer look at the four points that are the foundation for fostering deterrence:

U.S. Secretary of Defense Ashton Carter testifies before the U.S. Congress in February 2016. Carter pushed to create Cyber Command within the U.S. military to improve cyber capabilities. THE ASSOCIATED PRESS

Response: Through various documents, reports, and public statements by the president and secretary of defense, the U.S. has articulated that it can respond to a cyber attack on U.S. interests. In such a case, the effects of a cyber attack are assessed on a case-by-case and fact-specific basis by the president and his national security team. Significant consequences resulting from an attack may include loss of life, property destruction, or significant adverse foreign policy and economic consequences. If a decision is made by the president to respond to a cyber attack on U.S. interests, the U.S. reserves the right to respond at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power. Adversaries should know that our preference for deterrence and our defensive posture do not diminish our willingness to use military options — including cyber capabilities — when necessary. And when we do take action — defensive or otherwise, conventionally or in cyberspace — the DoD will operate in accordance with international and domestic legal obligations.

Denial: The DoD is working to increase its defensive capabilities to defend its networks and to defend the nation from sophisticated cyber attacks. In doing so, we are working with other departments and agencies, international allies and partners, and the private sector to strengthen deterrence by denial through improved cyber security.

When U.S. Secretary of Defense Ashton Carter introduced the DoD Cyber Strategy in 2015, he mentioned an example of a recent malicious cyber incident in which the sensors that guard DoD unclassified networks detected Russian hackers accessing one of our networks through an old, unpatched vulnerability. Although it is worrisome that the intruders were able to achieve some access to our unclassified network, we were nevertheless able to identify the compromise quickly, and we had a team of incident responders hunting down the intruders within 24 hours. After obtaining valuable information about their tactics and analyzing their network activity, we kicked them off our network in a way that minimized their chances of returning. This story has a happy ending, but that is not the only reason Secretary Carter chose to tell it — publicly discussing our ability to rapidly detect, attribute and expel an intruder from our military networks also has an important deterrent effect.

U.S. Cyber Command, the National Security Agency and the Central Security Service lead the United States cyber defense and response mission. AFP/GETTY IMAGES

Resilience: Because we cannot guarantee that every cyber attack will be denied, the DoD is investing in resilient and redundant systems so that we are able to continue our vital operations in the face of disruptive or destructive cyber attacks. A vital component of such "mission assurance" is identifying and protecting the networks and systems that are most critical to DoD operations.

More broadly, other agencies of the government must also work with critical infrastructure owners and operators and the private sector to develop resilient and redundant systems that can withstand attacks. Such measures can help convince potential adversaries of the resiliency of U.S. networks and systems and, therefore, the futility of attempting cyber attacks.

Attribution: The perception that anonymity prevails in cyberspace helps to enable malicious cyber activity by state and nonstate groups. Improved attribution capabilities are therefore a fundamental part of an effective cyber deterrence strategy. The DoD and the U.S. intelligence community have invested significantly in all-source collection, analysis and dissemination capabilities, which serve to reduce the anonymity of activity in cyberspace. Attribution enables the DoD and other departments and agencies to more confidently conduct response and denial operations against an incoming cyber attack.

Attribution — both in public and in private — can play an important role in dissuading cyber actors from conducting attacks. The DoD will continue to collaborate closely with the private sector and other departments and agencies of the U.S. government to strengthen attribution capabilities. This work will become an even more important factor in deterrence as activist groups, criminal organizations and other actors acquire advanced cyber capabilities in the future.

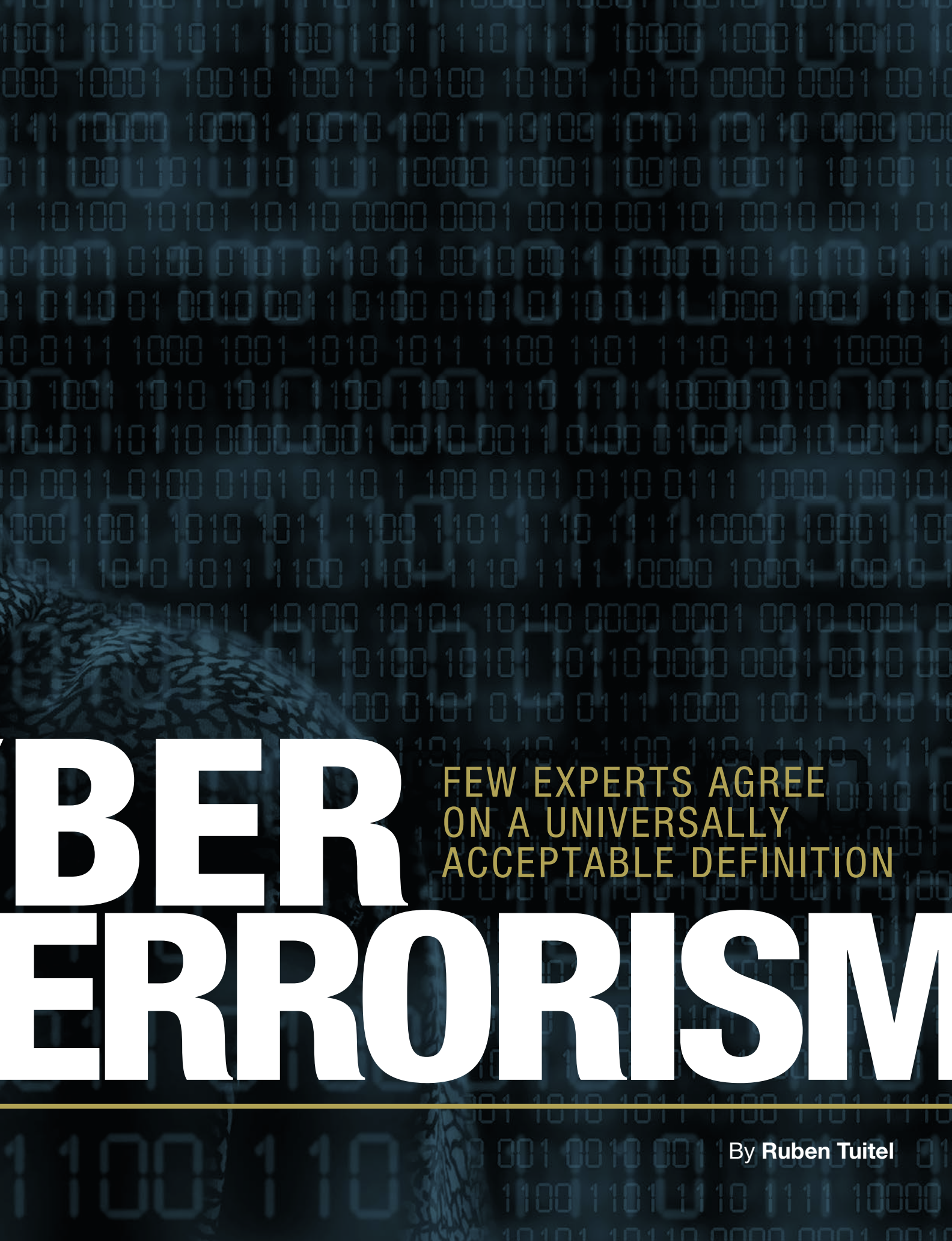
Conclusion

Many pundits and scholars refer to the role of deterrence in preventing nuclear conflict during the Cold War. Although many often draw parallels to the success of deterrence strategy during the Cold War, we must remember that deterrence in cyberspace today is much more complex. Because of the high cost and complexity of nuclear weapons, there were only a few actors — all nation-states — that needed to be deterred. That is not the case today in cyberspace, where even sophisticated malware can be found on the Internet with little effort and at low cost. As we seek to apply the lessons of the Cold War to the modern threat of cyber attacks, we also need to remember that the concept and practice of deterrence in the nuclear age did not emerge fully formed overnight, but instead developed over time. So, too, the DoD will continue to build deterrence by investing in the development of the Cyber Mission Force and its associated capabilities. Response, denial, resilience and attribution are the foundations upon which our deterrent posture rests. □

ISTOCK

Defining CY

T



BER ERRORISM

FEW EXPERTS AGREE ON A UNIVERSALLY ACCEPTABLE DEFINITION

By **Ruben Tuitel**

Cyber terrorism is a difficult phenomenon for scholars, legal practitioners and international organizations to define. Additionally, confusion exists over the differences between cyber crime and cyber terrorism. While this article is focused on cyber terrorism, I will briefly discuss cyber crime to highlight the differences. Existing cyber terrorism definitions leave room for debate; therefore, I have proposed my own definition: Cyber terrorism is the use of cyberspace by a nonstate entity to disrupt computer systems, causing widespread fear or physical damage and, indirectly, bodily injury, or causing disruption to such an extent that the credibility of the victim is seriously threatened, in furtherance of political, ideological or religious objectives.

CYBER ATTACK DEFINITIONS

Possible scenarios that resemble a cyber attack include a virus that scrambles financial records or incapacitates the stock market, a false message that causes a nuclear reactor to shut down, or an air traffic control system disruption that results in airplane crashes. Knowing the definition of a cyber attack is essential to differentiate it from cyber terrorism. Although there are many cyber attack definitions, a few are listed below.

The U.N. Office on Drugs and Crime describes a cyber attack as:

> "Cyber terrorism generally refers to the deliberate exploitation of computer networks as a means to launch an attack. Such attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure, through the use of hacking, advanced persistent threat techniques, computer viruses, malware, phlooding or other means of unauthorized or malicious access."

In the Joint Doctrine for Information Operations by the U.S. Joint Chiefs of Staff, cyber attacks are:

> "… deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or the information they hold."

The Oxford Dictionary defines a cyber attack as:

> "An attempt by hackers to damage or destroy a computer network or system."

Mauno Pihelgas, researcher at the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, defines a cyber attack in the chapter he wrote for the book *Peacetime Regime for State Activities in Cyberspace*, as:

> "… the term attack is considered to be any attempt to destroy, expose, alter, disable, steal, or gain unauthorised access to or make unauthorised use of anything that has value to an organization."

Defining cyber terrorism is more complicated. There are numerous aspects that make it difficult to determine whether a cyber attack can be labeled as cyber terrorism. However, before discussing this, it is important to understand the characteristics of terrorism.

The following characteristics of terrorism, as described in Bruce Hoffman's book, *Inside Terrorism*, are generally accepted. By distinguishing terrorists from other types of criminals and irregular fighters, and terrorism from other forms of crime and irregular warfare, we come to appreciate that terrorism is:

- Ineluctably political in aims and motives.
- Violent — or equally important — threatens violence.
- Designed to have far-reaching psychological repercussions beyond the immediate victim or target.
- Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia), or by individuals or a small collection of individuals directly influenced, motivated or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders; and perpetrated by a subnational group or nonstate entity.

DEFINING CYBER TERRORISM

Attribution

For a cyber attack to be regarded as cyber terrorism, it must have been conducted by a terrorist group. This is a matter of attribution, and attributing a cyber attack is difficult. Unlike the real world, cyberspace does not recognize country borders. An Internet user in Country A can buy a product in Country B without realizing he is buying a product in a foreign country. Additionally, it is possible for an Internet user to work through different IP addresses using "proxies" to conceal one's identity online or make use of an anonymous Internet browser such as Tor, and the so-called Deep Web — the "hidden Internet," as detailed in a 2001 white paper published in *The Journal of Electronic Publishing*. Pedophiles have been known to use the latter two to share pornographic pictures and videos, making it difficult for law enforcement agencies to identify and locate them, an article in *The Telegraph* reported in 2012.

UNLIKE THE REAL WORLD, CYBERSPACE DOES NOT RECOGNIZE COUNTRY BORDERS.

Another method of concealing one's identity online is using a virtual private network (VPN). It is often used to connect to company networks from outside the office, enabling employees to work with internal company assets without being exposed directly to the Internet, and thus, possible malicious users, Pihelgas wrote. Setting up a VPN is relatively easy and could be abused by malicious actors since their Internet traffic would be encrypted. "Backtracing," also called backtracking, involves a technical process using "traceroute" tools to acquire the IP address of the attacker. Law enforcement agencies use the process to determine whether the attack was done by a group of hackers or an individual.

However, there is no such thing as complete anonymity on the Internet. Backtracing should, in theory, always lead to the perpetrator. But, law enforcement agencies can misattribute, meaning that someone who isn't involved in the cyber attack is falsely accused. This makes backtracking a difficult task for law enforcement agencies. Pihelgas explains:

> "With the evolution of different anonymity techniques, the difficulty of attribution is one of the primary challenges in reducing the overall insecurity originating from cyberspace and in tracing specific malicious actors. Accurate attribution is required to respond to cyber incidents in both the operational and legal terms. Misattribution is a contrariwise problem, where an attack is made to appear to have originated from another source (incriminating someone else). In addition to slowing down correct attribution, this can result in risky situations where the blame is attributed to an innocent individual, organisation or country. Consequences can vary from conflicts and mistrust between parties to embarrassing incidents becoming public."

Violence in cyberspace

One characteristic of terrorism is violence, or the threat of violence. The World Health Organization defines violence as: "The intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation." However, cyberspace is a virtual world — a space of computers, servers, modems and the Internet — so it is questionable whether any violence occurs. While the Stuxnet virus was capable of damaging the centrifuges of the nuclear plant in Iran, no direct physical force damaged the machines. The cyber attack affected a computer system, which led to physical damage. A truck bomb, for instance, results in direct physical damage, while Stuxnet required an extra step to achieve physical destruction. But what

about violence in cyberspace — digital attacks that are initiated from a cyber element aimed at disrupting another cyber, or virtual, element? To bridge the gap between the physical and the virtual world in terms of violence, it is necessary to distinguish between physical violence and cyber violence. Necessary definitions could also include physical cyber attacks and virtual cyber attacks or physical cyber terrorism and virtual cyber terrorism.

Cyber terrorism vs. cyber crime

Distinguishing between criminal and terrorist acts in cyberspace, as well as other malicious activities, is challenging. Creating a clear distinction between different forms of malicious cyber activities is important for the investigation and prosecution of these crimes.

Cyber crimes are seen as the digital versions of traditional crimes, according to a 2013 Congressional Research Service report titled *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. For instance, identities can be stolen by hacking into customer databases of online shops, while the traditional criminal had to physically steal a wallet. Other cyber crime examples include credit card fraud, hacking company systems, and distributing and/or watching child pornography. Next to that, the activities of cyber criminals are different from those of cyber terrorists because they pursue a different goal and have different motivations. Cyber criminals are motivated by profit and involve crimes such as acquiring money or stealing information that can be sold, according to a 2010 report.

Terrorists, and thus cyber terrorists, are motivated by ideology, according to an International Centre for Political Violence and Terrorism Research article, or a political opinion that involves crimes that are more damaging to society and instill fear and anxiety. Yet, it also seems as if crime and terrorism are converging. The main source behind terrorist operations is money. Without that, it becomes almost impossible to acquire the materials needed to carry out an attack. To finance their actions, terrorists resort to crime such as drug trafficking, but they also make use of digital sources. This convergence however, would also make it increasingly difficult to classify a person as either a criminal or a terrorist.

DISTINGUISHING BETWEEN CRIMINAL AND TERRORIST ACTS IN CYBERSPACE, AS WELL AS OTHER MALICIOUS ACTIVITIES, IS CHALLENGING.

The difference between cyber crime and cyber terrorism is quite clear; however, it is difficult for law enforcement agencies to expose the perpetrator's identity and the motivation behind an attack in the cyber world, and therefore determine whether the attack was crime or terrorism.

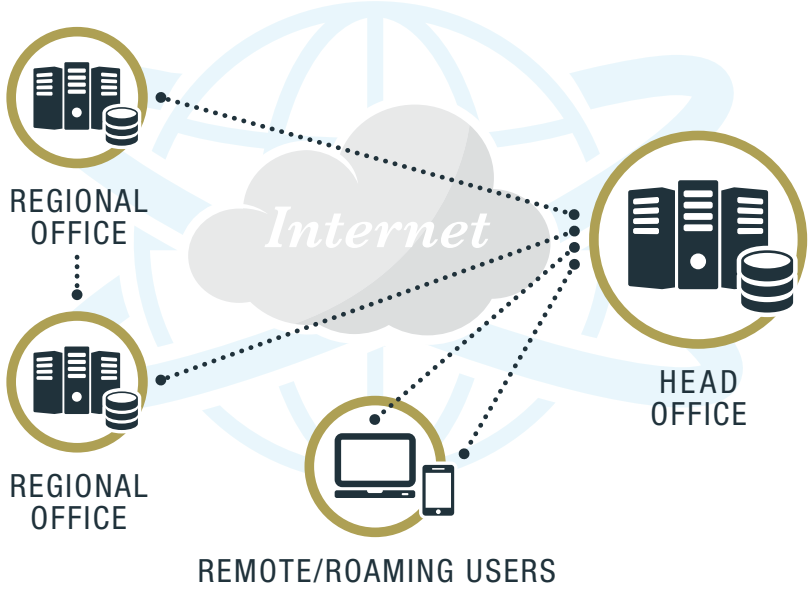
Terrorists seek attention

Less difficult, but still worth mentioning, is that terrorists and other nonstate entities often seek attention from the public. Terrorists want governments to know that the bomb explosion or airplane crash was their responsibility and that they conducted the attack for ideological or political reasons. Terrorists inform the public by posting a YouTube video or sending a "tweet" on their Twitter account, *The Daily Mail* reported. However, so far there is little evidence that a terrorist group such as al-Qaida has committed a cyber attack that caused significant damage. Terrorists may not yet have the knowledge and experience to attack a high-value target, or cyberspace is too covert for them. While cyber attacks are capable of disrupting critical infrastructure such as banks, a truck bomb is probably more destructive and might even be cheaper. Besides, a truck bomb makes a bigger impact on the public and has larger psychological repercussions. Therefore, it is questionable whether cyberspace is attractive enough for terrorists. However, there are several

BANKS *are* POPULAR TARGETS

Banks are popular targets for hackers. Common cyber attacks are distributed denial of service (DDoS) and spear phishing. Both aim to acquire information from clients, which is used to gain more information by calling customer service. Eventually the hackers ask for money transfers. Hackers time this so the DDoS attacks serve as a distraction so they can make use of the overburdened customer service employee. While this does not reach the level of cyber terrorism, banks are a critical aspect in every society. If they fail to operate, many businesses will not be able to continue their daily affairs, which will harm an economy.

VIRTUAL PRIVATE NETWORK (VPN)



The VPN connection is encrypted and protected from the public Internet.

PER CONCORDIAM ILLUSTRATION

Source: http://www.bankinfosecurity.com/banking-cyber-attack-trends-to-watch-a-6482/op-1

scenarios in which a cyber attack could be classified as cyber terrorism, such as an attack on a national electricity system.

POSSIBLE CYBER TERRORISM?

Critical infrastructure and industrial control systems are attractive targets. Failure or disruption could lead to casualties and have a substantial psychological impact. Marc Elsberg describes a worst case scenario in his 2012 book *Black Out*:

> "Cyberterrorist hackers have gained access to TenneT B.V. control systems, the national electricity transmission system operator of the Netherlands, responsible for supplying electricity to the Netherlands and part of Germany. A few hours ago, hackers shut down the electrical grid with a distributed denial-of-service attack which caused a country-wide electrical outage. Hospitals, increasingly dependent on digital systems for patient care are not able to treat patients properly, which leads to a large number of deaths. Emergency services cannot be reached, and communication lines are down. Citizens have no idea what is happening, and while the outage seemed rather innocent in the first few hours, people now are beginning to panic. The authorities are investigating, if possible at all, and only help people needing emergency treatment. Water refinery systems are shut down, which leads to low quality drinking water. The food industry is disrupted, eventually leading to food shortages. It is highly likely that people will soon begin to loot in order to survive."

EXISTING DEFINITIONS OF CYBER TERRORISM

In 2000, information security expert Dorothy E. Denning, when testifying before the U.S. House of Representatives' Special Oversight Panel on Terrorism, defined cyber terrorism as:

> "… the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."

Denning's definition is quite complete and includes many facets. She states that an attack and "threats of attack" should result "in violence against persons or property," and "attacks that lead to death or bodily injury … would be examples." However, an attack by a nonstate entity is not mentioned. This would mean that the Stuxnet attack by the U.S. and Israel could be regarded as a cyber terrorist attack or even an act of war, based on international law.

Kevin Coleman, an information security expert, defines cyber terrorism as:

> "… the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

This definition covers intimidation and the use or threat of "disruptive" activities. Also, this definition does not state that the attack needs to be committed by a nonstate entity.

An article in the *Information Security Journal: A Global Perspective* titled "How can we deter cyber terrorism?" defines cyber terrorism as "an activity implemented by computer, network, Internet, and IT intended to interfere with the political, social, or economic functioning of a group, organization, or country; or to induce physical violence or fear; motivated by traditional terrorism ideologies."

This final example of a cyber terrorism definition comes closest to the original definition of terrorism. It differs in that it describes the use of computers and other IT devices to conduct an attack. Coleman and Denning both define cyber terrorism as being directed against computers, not through the use of them. This is a good example of how definitions on cyber terrorism differ. *Information Security Journal* implies that computers and other IT devices are used as an instrument to commit a terrorist act.

LEAVING THE CONCEPT OF CYBER TERRORISM?

The term "cyber terrorism" may not be appropriate for describing large-scale cyber attacks. The word "terrorism" is used mostly when attacks have killed people or destroyed buildings. Considering that this has not happened thus far, the term "terrorism" should not be used to describe large cyber attacks. There should be a clear distinction about whether cyber terrorism is meant to target computers, uses computers, or both.

Lee Jarvis and Stuart Macdonald also question the use of the term "cyber terrorism" in their 2014 journal article published in *Perspectives in Terrorism*: "Perhaps the best illustration of this boundary problem can be found in debates over whether it is ever appropriate, useful or desirable to describe state violence of any sort as terrorist." The same applies to cyber terrorism. We coin new words and

terminologies for things that might already exist that causes confusion: "This profusion of new terminologies throws up considerable challenges for clarifying terms such as cyber terrorism. Not least amongst these is the inconsistent and interchangeable use of such terms whereby, as [Gabriel] Weimann [of the U.S. Institute of Peace] illustrates: '… the mass media frequently fail to distinguish between hacking and cyber terrorism and exaggerate the threat of the latter.' " This "profusion of new terminologies" is important to consider when determining a cyberterrorism definition.

SIMILAR STUDY

Research findings from another study by Jarvis and Macdonald, summarized in the article "What is cyber terrorism? Findings from a Survey of Researchers" also address how to describe cyber terrorism. Their study involved a survey of 118 researchers and focused on three definitional issues: (a) the need for a specific definition of cyber terrorism for either policymakers or researchers; (b) the core characteristics or constituent parts of this concept, and (c) the value of applying the term "cyber terrorism" to a range of actual or potential scenarios. Jarvis and Macdonald conclude that while most researchers believe a specific definition of cyber terrorism is necessary for academics and policymakers, disagreement on what this might look like has the potential to stimulate a rethinking of terrorism more widely.

THERE SHOULD BE A CLEAR DISTINCTION ABOUT WHETHER CYBER TERRORISM IS MEANT TO TARGET COMPUTERS, USES COMPUTERS, OR BOTH.

PROPOSING A DEFINITION

Existing definitions of cyber terrorism are quite complete, but leave room for debate. Therefore, I would like to contribute to this discussion by restating my definition: Cyber terrorism is the use of cyberspace by a nonstate entity to disrupt computer systems, causing widespread fear or physical damage and, indirectly, bodily injury, or causing disruption to such an extent that the credibility of the victim is seriously threatened, in furtherance of political, ideological or religious objectives. This definition covers the more essential parts of the term terrorism, such as fear, physical violence and the range of motives, but also the cyber part, by using computers to target computers.

CONCLUSION

While much more can be written on cyber terrorism, this article has shed light on the difficulty of defining it and encourages further discussion. Questions exist on violence in cyberspace and whether it comprises the mere use of the Internet by terrorists. Attributing an attack is probably the most difficult task and can lead to problems for law enforcement agencies. It is important to note that we may never reach a universal definition. Reaching an acceptable definition of cyber terrorism is also dependent on the definition of terrorism, which is still subject to discussion.

But if renowned terrorism experts like Walter Laqueur and Alex Schmid, who both studied hundreds of definitions of terrorism, cannot come to a universally acceptable definition, then who can? Perhaps the term cyber terrorism should not be used to define a disruptive cyber attack. With any luck we can achieve an understanding that improves international cooperation on the difficult subject of terrorism and cyber terrorism. Defining cyber terrorism thus seems to be a real dilemma. □

BALTIC

Estonia, Latvia and Lithuania sign a historic document to align their cyber defense policies

CYBER COOPERATION

PER CONCORDIAM ILLUSTRATION

Vytautas Butrimas,

senior advisor, Cybersecurity and IT Department, Ministry of National Defense, Republic of Lithuania

It was a historic moment for regional cyber security cooperation when representatives of three Baltic countries — the minister of economic affairs and communications of Estonia, the minister of defense of Latvia and the minister of national defense of Lithuania signed a memorandum of understanding (MoU) on November 4, 2015. Three neighbors with a rich history of cooperation in traditional areas of defense recognized that they were also cyberspace neighbors and agreed to formalize the cooperation that had started informally several years prior. This article will discuss the process that led to the development of this new form of cyberspace cooperation, why the MoU is important and discuss some of its content. It will serve as a guide for other countries that wish to enter into similar agreements with their cyber neighbors.

THE ORIGINS

The idea for the cyber cooperation MoU emerged in late April/early May 2007, when NATO held a cyber security workshop hosted by the U.S. Department of Defense and Microsoft at the company's headquarters in Redmond, Washington. Participants learned of new possibilities for information technology use in defense for the then-new Microsoft operating system Windows Vista. Organizers announced that a Security Cooperation Agreement had been signed with China (later also with the Russian Federation) that allows its government access to Microsoft Windows source code.

But the mood of the conference changed dramatically as the next speaker, an Estonian, announced to the crowd that "my country is under cyber attack." Participants looked at each other with surprise and bewilderment. Here we were, in a NATO meeting with all the top cyber security officials present, and no one knew what to do. NATO had established no verified procedures to deal with a member state under cyber attack. No agreements, point-of-contact lists or mechanisms of coordination for assistance were in place to promptly react to this event. Later that evening, phone calls were made to capitals, and assistance was organized and provided to address the cyber attack underway in Estonia. Later, NATO developed and offered members the opportunity to sign MoUs for cooperation in cyber defense. Lithuania was one of the first to sign in the summer of 2010. The idea of the MoU took hold at the Lithuanian Ministry of National Defense, which also signed a local MoU with a national computer emergency response team (CERT) operated by the National Communication Regulatory Authority and later with the Ministry of Foreign Affairs. It became clear that it was a good idea to have a written agreement that could be drawn upon to handle future cyber incidents. This idea took root among the other Baltic countries as well.

HISTORY OF COOPERATION

In 2009, cyber security experts from the three Baltic countries met formally for the first time in Riga, Latvia. They subsequently agreed to meet regularly and rotate meeting locations among the three capitals. Cyber security experts from a wide range of institutions involved in securing the safety of cyberspace attended these meetings. In 2012, for example, the list of institutions represented included the three national CERTs and the ministries of transportation and communications, defense, foreign affairs, interior and police. It was decided as far back as 2010 to form a legal basis for these meetings in an MoU. The first working draft was prepared, discussed and modified in later meetings. This process went on for several years as personnel changed and national coordinating institutions for cyber security policy shifted to other institutions.

In Latvia, for example, the coordinating institutions changed from the Ministry of Transportation and Communications to the Ministry of Defense, while in Lithuania, the last alteration took place in January 2015, when the Ministry of National Defense was assigned responsibility for policy coordination, according to the Law on Cyber Security passed in December 2014. The last change provided stability in terms of institutional coordination, to finalize and ratify the MoU draft with each respective government and prepare for the official signing planned for the spring of 2015.

The official signing was delayed for several months, however, because of an additional requirement to make use of state of the art electronic signature technology. Many technical issues had to be overcome before the three national electronic signatures could be recognized by each signatory on the same document. Finally, after a great deal of work among the respective certificate authorities and institutions, on November 4, 2015, the Baltic ministers responsible for coordinating national cyber security policy signed the Baltic MoU for cooperation in cyber security.

WHAT IS IN THE MOU?

The Baltic MoU on cooperation in cyber security consists of statements on common beliefs that each nation shares and agreements on forms of cooperation among participating institutions. The "considering that" section lists these common beliefs:

- Information systems and networks are interconnected and interdependent both nationally and internationally.
- Governments and militaries are seeking cyber offense capabilities.
- Cyber threats emanating from cyberspace include cyber crime; nation-state attackers; cyber espionage; and politically, economically and/or socially motivated hacktivists.
- National security includes protecting information systems, computer networks, and critical infrastructure.
- To successfully address all of the above requires international cooperation.

Noteworthy among the stated beliefs is that cyber security is understood to be more than just dealing with the activities of cyber criminals and socially motivated hacktivists seeking to disrupt IT systems. The critical infrastructure that forms the foundation upon which modern society functions is also under threat from cyberspace. Cyber attacks that degrade the ability of control systems to monitor and control processes found in energy, transportation or water supply systems can harm the well-being of society, the economy and national security. That is why this infrastructure is called "critical."

The next section is the more concrete "agree to" part. There is nothing new here in

Baltic cyber experts meet in Riga, Latvia, in 2012.
VYTAUTAS BUTRIMAS

The Baltic cyber security cooperation memorandum of understanding is signed electronically during a video conference on November 4, 2015.

MINISTRY OF NATIONAL DEFENCE LITHUANIA

terms of Baltic cyber security cooperation; the activities listed in this section have been ongoing unofficially since the first meetings of Baltic cyber experts in 2009. The difference is that the MoU established a legal basis for the informal collaboration. Some of the activities include:

- Sharing knowledge and experience to develop domestic cyber security policies and practices
- Focusing on collaboration applicable to reducing risk and vulnerabilities associated with cross-border dependencies of interdependent information systems, networks and critical infrastructure
- Exchanging information about detected cyber incidents that can affect the cyberspace of other participating countries
- Sharing early warning information about potential attacks against another's information system or network
- Appointing points of contact (PoC) and exchanging contact information for regular and emergency communication

These points illustrate that a Baltic Cyberspace Community of Interest (BCCI) has been established to monitor, prevent and react to recognized cyber threats to each other's critical and information infrastructures. The appointment of a PoC is useful in that each party knows "who to call" in an emergency. Knowing the PoC in advance avoids confusion and potential difficulty when responding to cyber emergencies.

A NEW WAY OF SIGNING

The MoU could have been signed with traditional pen and ink followed by an exchange of fully signed copies. However, the electronic signature method using national identification cards was chosen. This was a good way to demonstrate technical cooperation and problem solving. It took several months to perfect the process in which different electronic signing software and standards could be applied and recognized by all parties.

While this trial and error problem-solving work was at times frustrating, it yielded a good thing: It provided an opportunity for Baltic countries to learn about each other's electronic signing technologies. Solving the issues enhanced the technical knowledge of each organization that could be used to make electronic signatures more popular among the Baltic countries in the future.

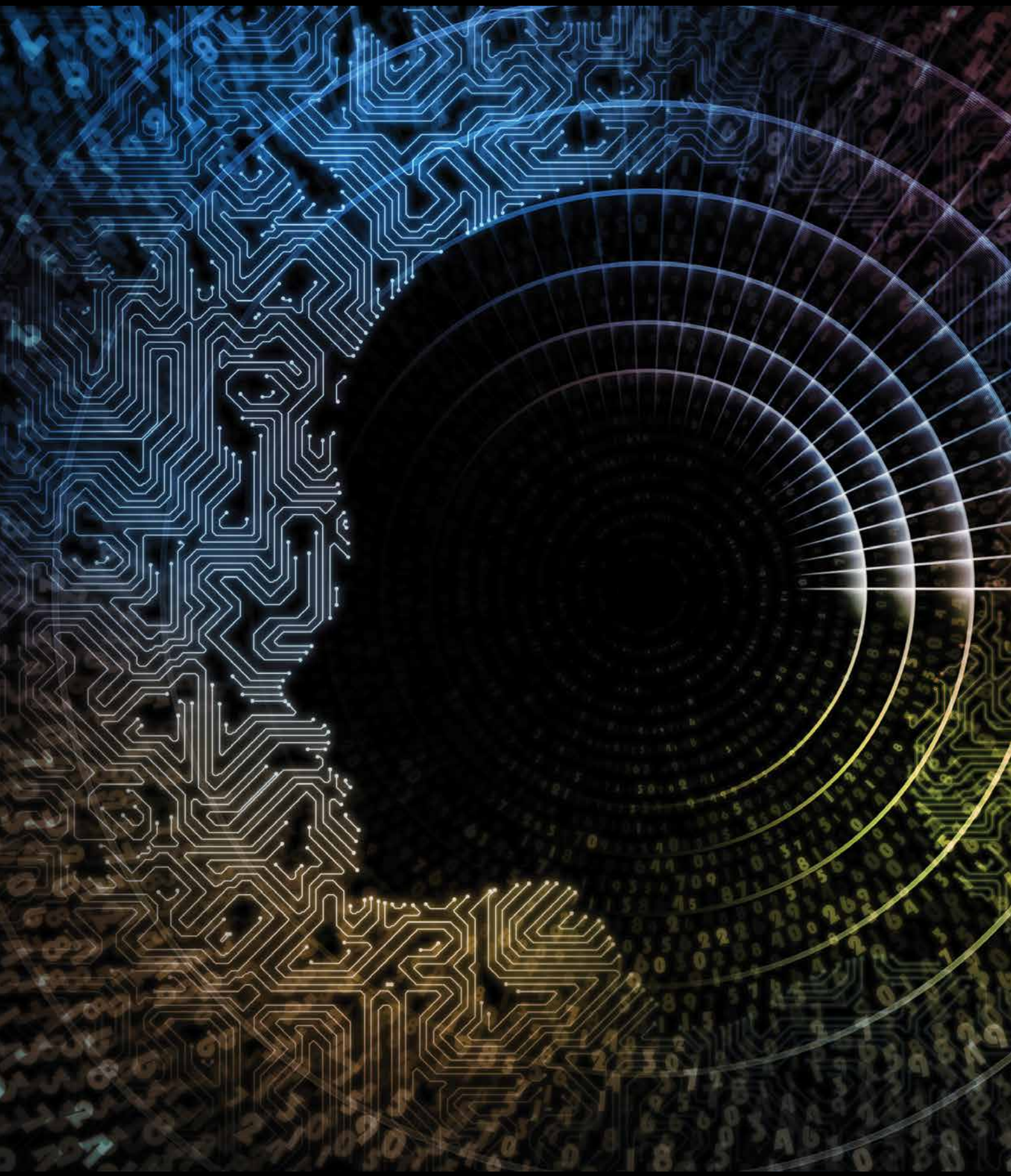
CONCLUSIONS

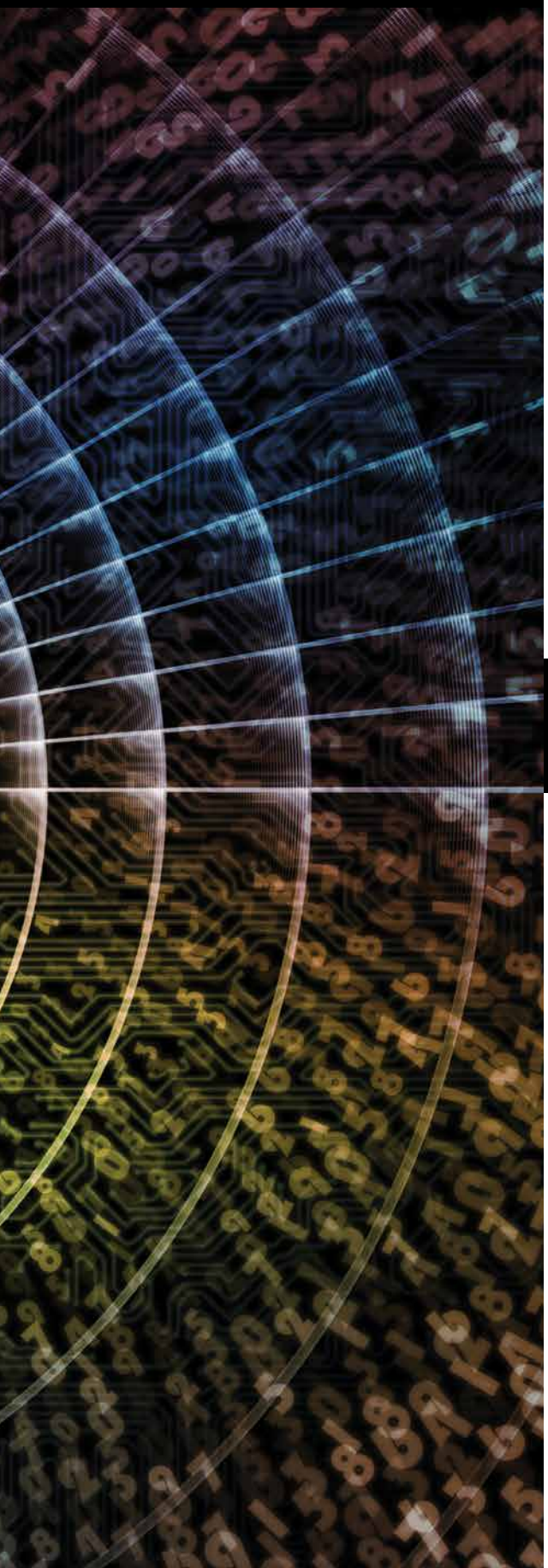
The signing of the MoU took more than five years to accomplish. Conceivably, it did not have to, but several factors contributed to making the process so lengthy. There are some lessons to be learned from the MoU process. First, it is always advantageous to meet and talk with cyber neighbors. It is often said that cyberspace "has no borders," which technically may be true but is not so in the electromagnetic reality of cyberspace. It makes sense to reach out to a neighboring country that has a physical border with you. You will find that you have much more in common in terms of cyber security than you may think. You will likely recognize that you are dependent on the same infrastructure for your nation's well-being. Electric grids, gas pipelines, fiber optic cables used in communications, and Internet links and transportation systems all cross cyber borders, making each neighbor dependent on the other in terms of providing and accessing critical services. A break in a cable providing links to international communications or a cascading failure in an electric grid affects not only the country where the fault originated, but may extend throughout the region.

A poem by Robert Frost called *Mending Wall* introduced the famous phrase "good fences make good neighbors." In the poem, each year two neighbors "meet to go down the line" checking and repairing the common wall that separates and forms the border between their two properties. The poet questions the need for a fence. One does not need to worry if his "apples" fall among the other neighbor's pine trees. However, the poet recognizes the need to deal with hunters crossing and damaging their lands. In today's cyberspace, cyber neighbors should "meet to go down the line" together to ensure each other's safety when dealing with threats to critical infrastructures emanating from commonly used and accessible cyberspace.

These are the structures that modern society depends on every day to function. The vulnerabilities and interdependencies of these structures cannot be secured by any one institution, but through cooperation with other interested parties. After a nation has first put its own cyber "house in order," signing an MoU with cyber neighbors is a practical first step for reducing risk and improving cyber security for everyone.

At the time of writing, there was a grand opening ceremony for new Lithuanian electric power links to Poland and Sweden. Critical infrastructure that includes power grids have both transborder and cyber dimensions, as IT-based control systems are used in electric power generation and distribution. With this latest event in mind, it is possible to foresee a need to expand the Baltic MoU to include two other cyber (and energy trading) neighbors of Lithuania: Poland and Sweden. □





ISTOCK

A NEW cyber security CURRICULUM

THE PARTNERSHIP FOR PEACE CONSORTIUM OFFERS A GUIDE FOR CYBER SECURITY EDUCATION

By Sean Costigan and Michael Hennessy

Today's news headlines regularly refer to commercial data hacks and breaches, electronic fraud, the disruption of government service or critical infrastructure, intellectual property theft, exfiltration of national security secrets, and the potential of cyber destruction. What used to be the domain of electronic warfare, information warfare and network security experts — often labeled "information operations" or "information warfare" — is transforming into a much broader domain referred to as cyber security. This emerging field of study and practice has challenged defense education institutions to consider topics and methods that traditionally fell outside standard defense education.

With that awareness shift in mind, the rapid and unrelenting pace of changes and challenges in cyber security prompted the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group to request the development of a new cyber security curriculum for defense academies.

establishing the necessary balance between access, usability and security is the challenge. this new curriculum explores approaches to threat and risk assessment, identification and mitigation at the technical and policy levels of agencies and governments.

The resulting curriculum, published in the spring of 2016, is the work of a multinational team of over 30 volunteer academics and researchers from 14 nations associated with the PfPC of Defense Academies and Security Studies Institutes. Our effort aimed to produce a flexible and comprehensive approach to cyber security by offering a logical breakdown by specific categories, suggesting the level of knowledge needed by various audiences and indicating useful key references so that each adopting state could adapt this framework to its needs.

security and risk education

Security measures are most often informed by evaluating threats and risks. In this new curriculum, both concepts are explored at length. However, in simple terms, cyberspace is full of threats but measures to mitigate threats need to be informed by measures of risk. The International Standards Association defines risk as "the effect of uncertainty on objectives." The effect may be a positive or negative deviation from what is expected. Measures taken to "secure" must be commensurate with the amount of risk that is acceptable. As such, securing cyberspace entails a number of considerations to mitigate risks and threats while encouraging open communication across various types of interconnected networks.

Establishing the necessary balance between access, usability and security is the challenge. This new curriculum explores approaches to threat and risk assessment, identification and mitigation at the technical and policy levels of agencies and governments. It explores recommended best practices and comparisons to known policies of particular states or organizations.

This curriculum seeks to provide a coherent launching point to develop or enhance the teaching of cyber security issues to senior officers or civil servants and midlevel military and civilian staffs. Like other curricula developed by the PfPC, the aim of the document is conservative. It does not present a single master course outline for all to follow. It is not exhaustive in content, details or approaches. However, we believe it will furnish a useful heuristic approach to the various domains, constituting a comprehensive introduction to the spectrum of issues involved with cyber security. Those with little technical background will find an introduction at a manageable level of complexity and gain a better appreciation of where technical depth is required and why. Those with technical backgrounds may find the material a useful overview of areas they are familiar with and an introduction to broader issues of international, national and legal policies and practices.

This proposed curriculum is presented through a series of four broad themes:

1. Cyberspace and the fundamentals of cyber security
2. Risk vectors
3. International cyber security organizations, policies and standards
4. Cyber security management in the national context

It is assumed that institutions adopting this curriculum will work together with an expert team to identify national policies and procedures at a level of detail required for the target audience. Rote knowledge of transitory technical matters may be necessary, but the objective of this curriculum is to establish a broader understanding of cyber security challenges across the spectrum.

This new cyber security reference curriculum is not a single or proposed course structure. Rather, it is a key reference providing a broad outline of issues and topics. It may serve as a guide for technical staffs to identify their particular focus. Similarly, it may guide introductory courses for senior national security policymakers, providing them technical context to shape national policies.

Attendees at a NATO Military Committee Partnership for Peace Cyber Workshop in Georgia
SFC CARRIE FOX, MARSHALL CENTER

lessons learned

While drafting the curriculum, we canvassed PfPC member institutions, other defense colleges and reviewed military training programs of NATO and PfPC partner countries to establish what is being taught. We sought to identify gaps and shared approaches that cut across traditional boundaries of governmental and military structures. Country workshops were instrumental to the curriculum team, helping them acquire a deep understanding of the different challenges each country faces when grappling with cyber security.

Across the board, the largest single gap we observed was the lack of sufficient understanding of cyber-security-threat and risk-mitigation practices among national-security and defense-policy leaders. A similar gap was identified among technical experts' understanding of national policy frameworks. The boundaries between these groups are not simply represented by military or bureaucratic rank; thus, we have not compartmentalized this reference curriculum into blocks according to the potential rank of students.

Additional lessons were noted in several key areas, particularly:

1. Gender — The cyber security field remains largely a male enterprise. Defense education institutions have the opportunity to narrow this gap.
2. Age — The concept of being "born digital" continues to present cognitive problems for policy leaders who perceive cyber security to be a young person's field instead of a critical domain for policymakers of any age to understand.
3. Technical Capability — Far too few cyber security labs exist across Eastern Europe. Western defense institutions would do well to help create better labs for students.
4. Policy Understanding — Many different points of view, some cultural, must be taken into account when discussing national cyber security issues. A number of countries have developed their own terminology and eschewed some widely used terminology as a matter of informed choice.
5. International Differences — Some countries are attempting to take advantage of perceived ambiguity to push agendas that run contrary to the best interests of democracies and the global exchange of information.
6. Misplaced Emphasis on Technical Matters — Cyber security isn't exclusively a technical field, yet it is generally treated as one by educators and policymakers alike. If cyber security is to become a normal part of the policymaker's portfolio, the two fields must be integrated to a certain degree.
7. Legal Landscape — There is wide variation in how states address cyber security within domestic law. The attribution challenge — the difficulties associated with tracking the source of malign, threatening or illegal cyber activity — compounds problems in both the domestic and international spheres. There is no one-size-fits-all solution.
8. Whole of Government — Approaches to managing cyber security differ significantly among countries, but cyber security cuts across many institutional and organizational boundaries. The best solutions must be built on a comprehensive whole of government approach. □


EXTREMISM
ISTOCK

ONLINE *in* NIGERIA

The country tries to counter Boko Haram's adept use of social media

TOMMY VICTOR UDOH, *Nigerian Defense Space Agency*

Social media refers to the wide range of Internet-based and mobile services that allows users to participate in online exchanges and online communities or contribute user-created content. The kinds of Internet services commonly associated with social media include blogs, wikis, social bookmarking, Twitter and YouTube, among others. Social media technologies provide a wide range of flexibility, adaptability and usability.

Terrorists and insurgent groups — in the case of Nigeria, the Boko Haram terrorist group — exploit social media for nefarious activities. This article offers an overview of Boko Haram terrorist activities in Nigeria, highlights the group's use of social media, considers government initiatives for countering terrorism using social media, and considers the wider challenges associated with terrorist use of social media.

BOKO HARAM ACTIVITIES IN NIGERIA

The *jamaa'atu ahl as-sunnah lida'wati wal jihad,* popularly known as Boko Haram, is a pseudo-Islamic terrorist group based in northeastern Nigeria. The group's nickname colloquially translates into "Western education is sinful." Thus, the group is opposed to Western education, ideologies and systems such as democracy.

Boko Haram was created in 2002 by Mohammad Yusuf, a radical Islamist cleric from Maiduguri, Borno state. The Boko Haram sect came to prominence in 2009 when it participated in sectarian violence in northern Nigeria. Yusuf was killed that year and replaced as leader by Abubakar Shekau.

Boko Haram has killed thousands of innocent citizens, destroyed numerous properties, including the United Nations building in Abuja, and abducted citizens, including the Chibok students. Boko Haram activities later spread to neighboring countries such as Chad, Niger and Cameroon.

The group has pledged allegiance to the Islamic State of Iraq and al-Sham (ISIS) and intends to represent that group's interests in the West African subregion. Though Boko Haram claims to oppose Western education, the group uses the Internet and social media to interact and promote its activities.

Use of social media

Once ISIS accepted Boko Haram's allegiance, its online activities expanded to copy ISIS' techniques. Subsequently, the groups adopted social media platforms such as Facebook, Twitter and YouTube because of their cheapness, convenience and enormous reach beyond borders or nationality. Social media has enabled Boko Haram to release messages directly to its audience without intermediaries. Like most terrorist groups, Boko Haram uses cyberspace — especially social media — for recruitment, propaganda, fundraising and communication.

Recruitment

With the help of the Internet, Boko Haram gets wide access to vulnerable young people. Social media is used to entice the audience. To reach more recruits and evade media platform policies, Boko Haram began addressing the public informally. For instance, it targeted Twitter users who appear open to its ideas. Although some are lured into participating in terrorist acts for financial gain, many recruits from rich and middle class families are enticed by the extreme material the group spreads online.

Propaganda

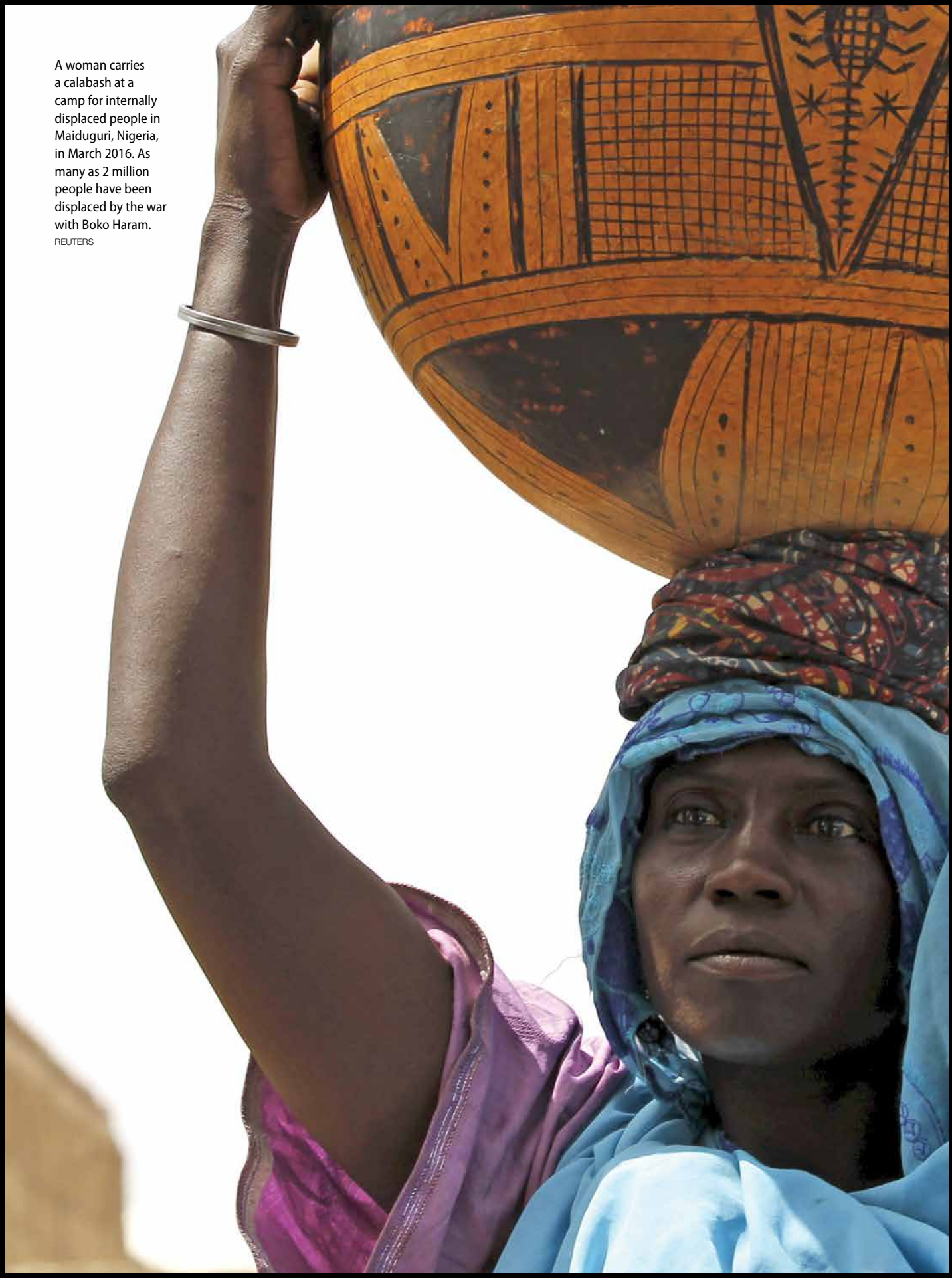
At the onset, Boko Haram disseminated its propaganda through radio messages and distributed its footage to international media such as Agence France-Presse through the use of middlemen. Later, the group graduated to Twitter, where it posted videos and photos showing the killing and beheading of security agents. Similar clips were posted on YouTube and translated into Arabic, presumably to capture a larger audience. The pictures and clips sometimes feature idyllic scenes of villages and people living their lives seemingly without fear and pledging support and allegiance to the group.

Fundraising

As the size, scope and structure of terrorist organizations have evolved, so too have their methods of raising and managing money. The rapid expansion of social media has been exploited by terrorist groups to raise funds from sympathetic individuals and organizations globally. Widespread access to the Internet and its relative anonymity encourages exploitation by terrorist fundraisers. Innocent citizens have been lured via social media and kidnapped to sometimes be exchanged for ransom from relatives or employers. The group also uses social media fundraising with prepaid cards and large-scale crowdfunding schemes using e-wallets. The money is used to recruit, motivate and train volunteers; procure arms, ammunition and explosives; spread propaganda; and conduct research and development.

Communication

Social media is becoming the primary means of keeping in touch with one another and with traditional media sources and channels of public



A woman carries a calabash at a camp for internally displaced people in Maiduguri, Nigeria, in March 2016. As many as 2 million people have been displaced by the war with Boko Haram.
REUTERS

Pictures of 100 wanted Boko Haram suspects are displayed on a poster released by the Nigerian Army in the northeastern town of Damboa in February 2016. AFP/GETTY IMAGES

communication. Social media allows this generation to experience the full reality of English poet John Milton's view of the "free market of ideas" where falsehood and truth are seemingly published concurrently by new media users. Boko Haram employs communications platforms such as Skype, chat groups, Instagram, Twitter, Facebook and WhatsApp. The terrorist group chooses these channels of communication because of their low cost, ease of use, and anonymity. Communication can reach those near or far and links terrorists groups to ISIS to share ideas or raise money.

COUNTERING TERRORIST SOCIAL MEDIA USE

Financial intelligence gathering

The Bank Verification Number (BVN) program strengthens the security of banking transactions and improves national financial intelligence collection. This government initiative improves detection of laundered money and shares information on emerging risks. Unique BVNs in Nigeria make it easier for banks to manage depositors' identities regardless of the number of accounts they have. The program has reduced the practice of depositors using multiple identities to launder funds through various banks and accounts. With the BVN, banks can track irregularities within accounts. The area of focus extends to identifying and targeting financial collection/aggregation/accounting points among criminal and terrorist organizations. BVNs allow law enforcement agencies to focus on the recipient of the funds, rather than just the source.

Cyber security program

The federal government of Nigeria has championed a national cyber security program that encompasses the Cyber Security Policy and Strategy and the Cyber Crime Law. The Cyber Crime law provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crime in Nigeria. This law ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. It mandates that service providers retain all traffic data and subscriber information with regard to an individual's constitutional right to privacy and take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.

Computer emergency response team
The Nigeria Computer Emergency Response Team was established to monitor and respond to security incidents within the nation's cyberspace — both proactively and reactively. The proactive service protects and secures Nigerian cyberspace in anticipation of attacks, problems or events. The services include technology watch, intrusion detection services, vulnerability assessment and penetration testing. The reactive services are designed to respond to requests for support against any threats or attacks on information systems in Nigeria's cyberspace. This includes incident analysis, on-site incident response, incident response coordination, incident response support, forensic evidence collection and forensic analysis.

Strategic online narratives
The strategic online narrative is a statement of identity, cause and intent, behind which the Nigerian government, the people and the Armed Forces are uniting in the fight against terrorism. It is propagated consistently to Boko Haram members, the general populace and security forces. The counternarrative for Boko Haram members, which is consistently disseminated, promotes a moderate form of Islam. It suggests that the Holy Prophet never killed innocent children or kidnapped women to propagate the Islamic cause. It further enjoins them to be true Muslims and surrender or submit to the authorities, who will embrace and treat them well. The narrative for security forces strengthens their morale and reminds the troops that the cause they are fighting is just.

Social media crisis communication centers
Crisis communication centers can monitor social media activities. The center involves civil society, the press, social media enthusiasts/activists, young people and nongovernmental organizations that share ideas and provide information to counter violent extremist ideology.

Detecting and preventing online terrorist activity
Nigerian security agencies have acquired modern technology to help collect information on terrorism. This technology enables the lawful interception of electronic communication when there are reasonable grounds to suspect that the content is required for the purposes of a criminal investigation or proceedings.

Public education and warning alerts
The government urges Nigerians to be vigilant and volunteer information to authorities to enable security agencies to prevent Boko Haram attacks. Similarly, tips for spotting a terrorist and forwarding information that can lead to an arrest are circulated online. Social media platforms are littered with sponsored dramatic sketches, as well as the use of comedy, musical clips, jingles, testimonies from surrendered and deradicalized Boko Haram members, and documentaries. Additionally, leaflets and factual press releases are distributed in Boko Haram controlled areas and at civil-military cooperation activities, at the operational and tactical levels, in the areas of health care and infrastructure.

SOCIAL MEDIA CHALLENGES

Changing tactics
It has proven difficult over time to distinguish between sympathizers, supporters and actual terrorists. The identification of those contributing money, either intentionally or unwittingly, is a serious challenge for security authorities. It is difficult to obtain evidence associated with the use of terrorist funds when money is transferred via the Internet. Social networks could be used to show relationships, but finding proof is still difficult.

Privacy versus security
Sometimes it is beneficial for government to block a citizen's access to websites or servers used by terrorists. However, when considering the right of freedom on the Internet, it becomes difficult to implement such policies.

Denying access to known terrorists
YouTube, Twitter and Facebook are some of the social media platforms often used by terrorists like Boko Haram for propaganda. When a known terrorist leader like Abubakar Shekau posts a propaganda video on social media, it is always difficult to get the cooperation of the owners or the administrators of such platforms to deny the terrorists the use of their platforms/servers, even when the user is a known terrorist.

CONCLUSION

Boko Haram terrorists in Nigeria, like other terrorist organizations, have continually tried to exploit social media for recruitment, propaganda, fundraising and communication. The Nigerian government is mindful of the risk inherent in cyberspace. Therefore, for its citizens to continue to benefit from the full potential of the information and communications technology revolution, it must take cyber risks seriously. It is against this backdrop that the government is determined to confront threats, uphold and support the openness of cyberspace, as well as balance security with respect for privacy and fundamental rights.

The government of Nigeria is constantly embarking on new initiatives to counter terrorists' use of social media through comprehensive national cyber security programs, the use of financial intelligence to track funds and the establishment of a communications center to counter terrorist ideology and radicalization. Other initiatives include Internet surveillance, censorship, cyber operations, as well as mass education and public awareness.

Several challenges still exist, and efforts are ongoing to overcome them. These challenges include the ability to identify funds transferred through social media and why the money is being transferred. Another challenge is striking a balance between citizens' freedom on the Internet and national security. Lastly, the difficulty in getting owners and managers of social media platforms to deny access to known terrorists is also a challenge. □

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.

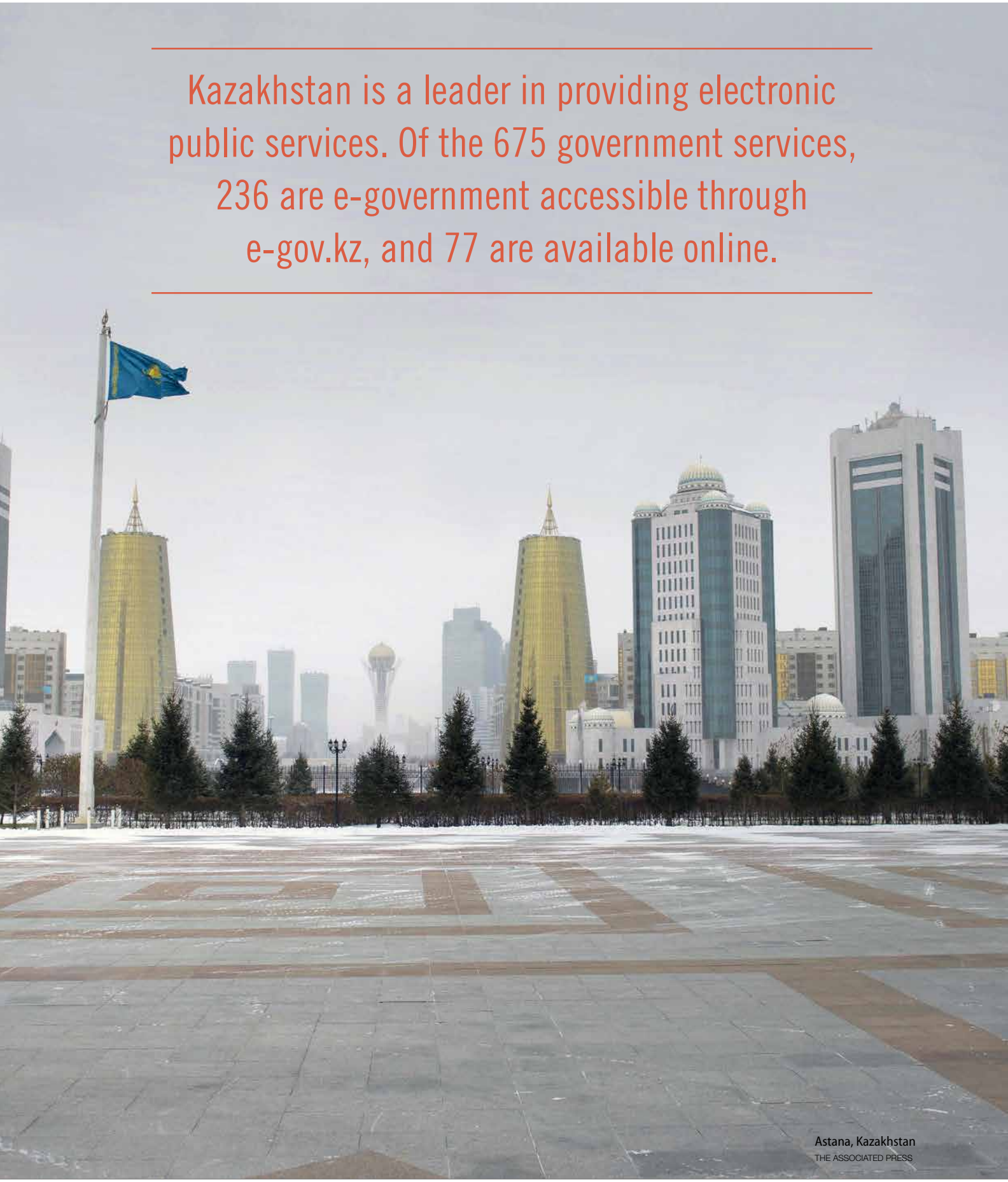
On a conceptual level, there is no clear understanding of the difference between "information space" and "cyberspace." In Kazakhstan, legal and regulatory terminology virtually eliminates the "cyber" prefix (cyberspace, cyber security, cyber crime, cyber war). The official terminology for these concepts 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

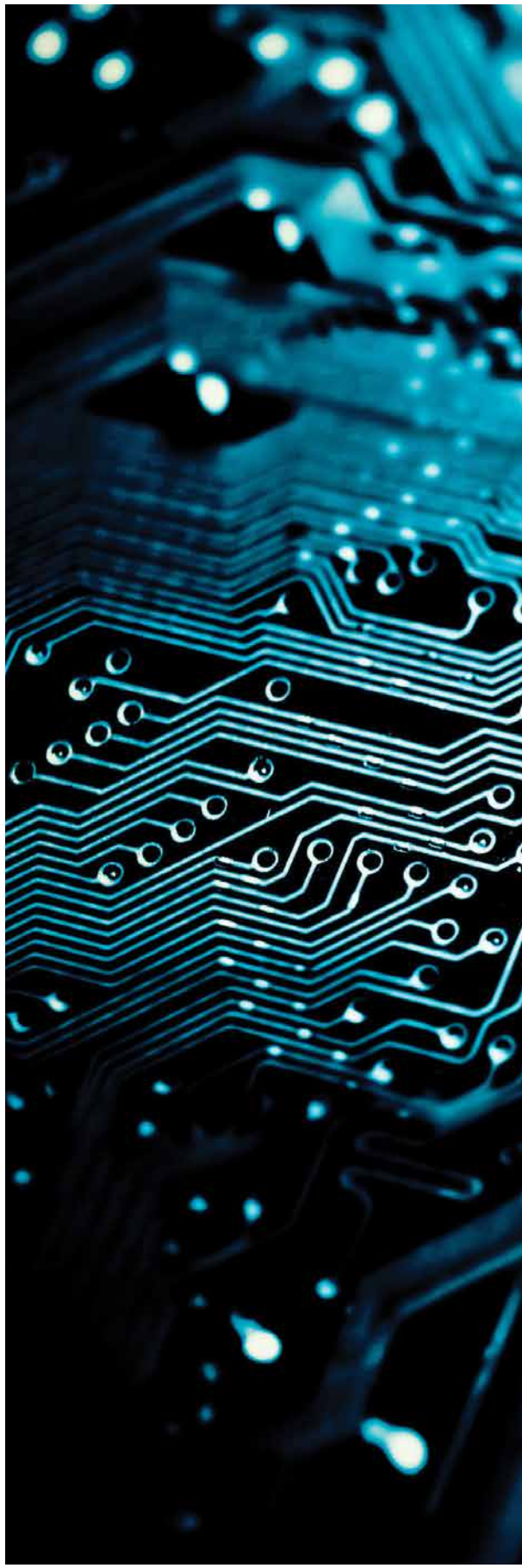
Kazakhstan's new law, On Telecommunications, in effect since January 1, 2016, implements national security certificates for Internet users. All cyber operators are obliged to pass traffic using a protocol that supports encryption using the security certificate, except for the traffic encrypted by means 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. □

MOLDOVA'S CYBER SECURITY CENTER

Contacts, trust and communication are key to robust cyber capabilities

By **Natalia Spinu**,
Chief, Moldovan Cyber Security Center,
E.S. Center for Special Telecommunications



Today's cyberspace poses innumerable risks to the security of private companies and public institutions, making them easy targets for cyber attacks by "hacktivist" groups, terrorist organizations or state-sponsored hackers. The days when an organization could withstand that onslaught alone have passed. A collective response based on information sharing can make organizations better prepared and more resilient to these emerging challenges.

Information sharing is voluntary in most cases and is based on a particular need or trust built over time. In some developed countries, legal initiatives have been implemented to encourage and sustain such activities, while reducing risks to the private sector with government as a trusted third party. That is an area where public-private partnerships take place.

In the Republic of Moldova, public-private partnerships don't exist in the cyber domain. Therefore, information sharing typically occurs on an ad hoc basis. This informality severely affects the ability of business and governmental organizations to meet the challenges posed by cyber attacks. Just such a circumstance played a role in recent high-impact incidents in Moldova (CTB-Locker mass infections, Starnet database leak and others).

ISTOCK

Moldovan President Nicolae Timofti passes an honor guard while attending a meeting of the EU's Eastern Partnership in Prague. Moldova's executive branch has led the push to improve the country's cyber security. THE ASSOCIATED PRESS

Many issues hinder information sharing between the private and public sectors and within the public sector alone. They include:

- Uncertainties in national legislation.
- No points of contact between private companies and public institutions.
- Not knowing the structure and responsibilities of the state institutions involved in cyber security, or how and to whom illegal actions or security incidents should be reported.
- Lack of qualified specialists.
- No joint training exercises.

According to current legislation, seven organizations in Moldova are involved in fighting cyber threats and should engage in cyber information sharing at political, technical and civil levels:

- ***Supreme Security Council*** — a consultative body overseeing the execution of governmental policies on national security.
- ***Intelligence and Security Service*** — a specialized organ of state security responsible for combating cyber threats nationwide.
- ***Ministry of Information Technology and Communications*** — department that develops and promotes state policy in the information and communications technology (ICT) domain, including cyberspace.
- ***Office of the Prosecutor General*** — responsible for the coordination and prosecution of cyber crime.

- ***Center for Combating Cyber Crimes*** — a police department specializing in the investigation and arrest of cyber criminals.
- ***National Center for Personal Data Protection*** — an autonomous public authority responsible for the compliance of personal data processing.
- ***Cyber Security Center CERT-GOV-MD*** — a government computer emergency response team.

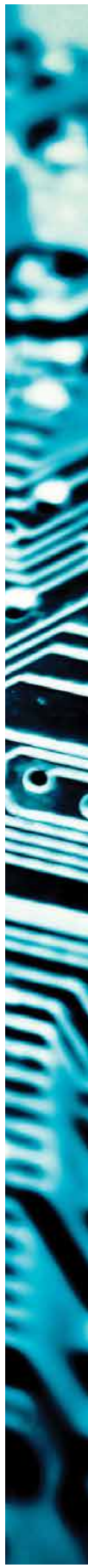
The Cyber Security Center CERT-GOV-MD is a government-level institution involved in national cyber security development. But that prestige comes with the responsibility to solve complex cyber issues. In recent years, CERT-GOV-MD has performed a number of activities aimed at improving cyber information sharing nationwide. Some noticeable improvements have occurred that can be divided into three areas:

- ***Establishing national and international points of contact.*** In June 2013, CERT-GOV-MD produced an initiative in accordance with an order from the prime minister that requested public administration authorities share information regarding threats and vulnerabilities and report any malicious activity to CERT-GOV-MD. That established an additional pillar in the public-sector information sharing framework and identified contacts at a technical level within government institutions. Another achievement was reached in 2014 when CERT-GOV-MD became an accredited member of Trusted Introducer, an organization that unites European computer emergency response teams. This establishes direct and trusted communication channels within the international cyber security community.
- ***Building trust.*** From 2013 to 2015, CERT-GOV-MD organized a series of international conferences and workshops that brought together representatives from private companies, governmental structures and universities, as well as leading cyber security experts who helped remove the barriers of misunderstanding and cultivated personal relationships.
- ***Fostering communication.*** By engaging simultaneously in the hands-on activities of countering state-targeted cyber incidents, in policy development, and with local, national and international groups and projects, CERT-GOV-MD has developed a unique and holistic understanding of cyber security in Moldova.

Cyber security requires a comprehensive approach. Political will, a nationwide engagement and the involvement of leading experts are key to creating conditions for state institutions to ensure an adequate level of cyber security.

That allows critical information on the most acute issues to be communicated from the most distant points of government to the highest officials of the country.

Cyber security requires a comprehensive approach. Political will, a nationwide engagement and the involvement of leading experts are key to creating conditions for state institutions to ensure an adequate level of cyber security. A successful realization of that goal depends on contacts, trust and communication. These are the components that define the role and mission of Cyber Security Center CERT-GOV-MD in Moldova's national cyber information sharing. □



Mastering Cyberspace in MILITARY OPERATIONS

EUCOM GAINS BATTLEFIELD ADVANTAGES THROUGH THE USE OF INFORMATION SYSTEMS

By **U.S. European Command**

Attack your enemy where he is unprepared, appear where you are not expected.
— Sun-Tzu, *The Art of War*

As the information age continues to change our world dramatically, an understanding of cyberspace using a familiar set of terms and a logical battlefield framework is essential to victory. Today, as throughout history, successful leaders must identify and take advantage of key moments in time and space to win. Operations in cyberspace are no different. Understanding the potential impact that cyberspace has on operations, developing a framework to understand and manage these effects, and empowering cyber mission forces can offer a distinct advantage.

Cyberspace adds a level of complexity in which actors can generate effects across a full range of military and civil activities because information systems are becoming increasingly prevalent in nearly every aspect of military operations. To win in the 21st century, leaders must know the capabilities and limitations of their systems through a methodology that brings coherence and understanding to the potential impacts of cyberspace.

Understanding the significant potential impact of cyberspace is essential to maintaining cyber superiority: It's the ability to effectively use systems at the right time and tempo. Cyberspace is a man-made dominion that consists of geography, hardware, logical networks (software/apps), personas (user ID and logon information) and people. Today, nearly 40 percent of the world's population has Internet access compared to less than 1 percent 20 years ago. So maintaining safety in cyberspace is becoming increasingly more difficult. The number of Internet users increased tenfold between 1995 and 2001, reaching 1 billion in 2005, with another billion by 2010, and surpassing 3 billion total users in 2015, according to the Internet Live Stats website. With over 7 billion people on the planet today, nearly half the world's population has access to this operational environment, the International Telecommunications Union's website stated.

A British Signals Regiment soldier prepares communications equipment for Exercise Combined Endeavor, the pre-eminent command, control, communications and computer exercise for NATO and Partnership for Peace multinational operations. MAJ. JASON ROSSI/U.S. AIR FORCE

When you include the coming wave of the Internet of things, including lights, cameras and cars, the number will surge to an estimated 20 billion to 30 billion — approximately three to five times the number of people on the planet. This means that, because all networks are linked in some manner, commanders will face increasing challenges to recognize change, act to assure cyber superiority and conduct operations.

Developing a framework to improve understanding of cyberspace enables leaders to rapidly recognize change and lead transitions. The Capstone Concept for Joint Operations in 2020 describes how future adversaries can become more capable using cyberspace and continue to challenge our ability to operate. Leaders must have a methodology to rapidly relate geography, hardware, logical networks, personas and people into a simple framework that enables change recognition and allows them to act, because both framework and methodology are essential to winning.

One method is to use the terrain analysis model known as observation, cover and concealment, obstacles, key terrain, avenues of approach, or OCOKA, a term that most military planners are familiar with. Just as these factors must be analyzed with respect to the mission, type of operation, level of command and composition of forces, along with weapons/equipment expected to be encountered, leaders can also use this framework in cyberspace. Observation of fields of fire can be used to identify potential engagement areas where maneuver force systems and platforms are most susceptible to observation and kinetic or nonkinetic fire. Understanding these danger areas will help protect assets.

The importance of cover and concealment in placing tactical military hardware is analogous to the importance of personas in protecting network access. The process of devising cover and concealment of tactical hardware is straightforward, but logical networks, personas and people require much more thought and teamwork to reduce risks and exposure. In a tactical environment, obstacles are typically natural or man-made terrain features that stop, impede, slow or divert movement. These same concepts apply in cyberspace. Understanding how to create obstacles by using hardware, such as firewalls and proxy servers, and software, such as digital identification and two-factor authentication, is essential to disrupting an adversary's ability to influence operations.

Identifying key or decisive terrain is more than relating hardware to a physical location; it involves identifying key systems like missile defense, fire control, and electric power plants that are essential to successful operations. Each of these are examples of logical networks and could be key terrain. People and personas could also be key terrain because they serve as access points to systems. Identifying key terrain enables leaders to turn each feature into a named area of interest and determine placement of the appropriate overwatch.

A Ukrainian soldier attends a 2014 Cyber Endeavor seminar, part of a U.S. European Command initiative to improve collective cyber security of NATO allies and partners. MAJ. JASON ROSSI/U.S. AIR FORCE

Finally, understanding avenues of approach, also known as attack vectors, is central to understanding the vulnerabilities of your formation. Leaders who analyze avenues of approach against their cyber systems, including those that could impact the hardware, logical networks, personas and people, are better prepared to allocate cyber mission forces and set defensive postures as they conduct operations. Using OCOKA to analyze geography, hardware, logical networks, personas and people improves awareness while helping leaders develop a better understanding to act faster and lead change, providing them and their formations an advantage.

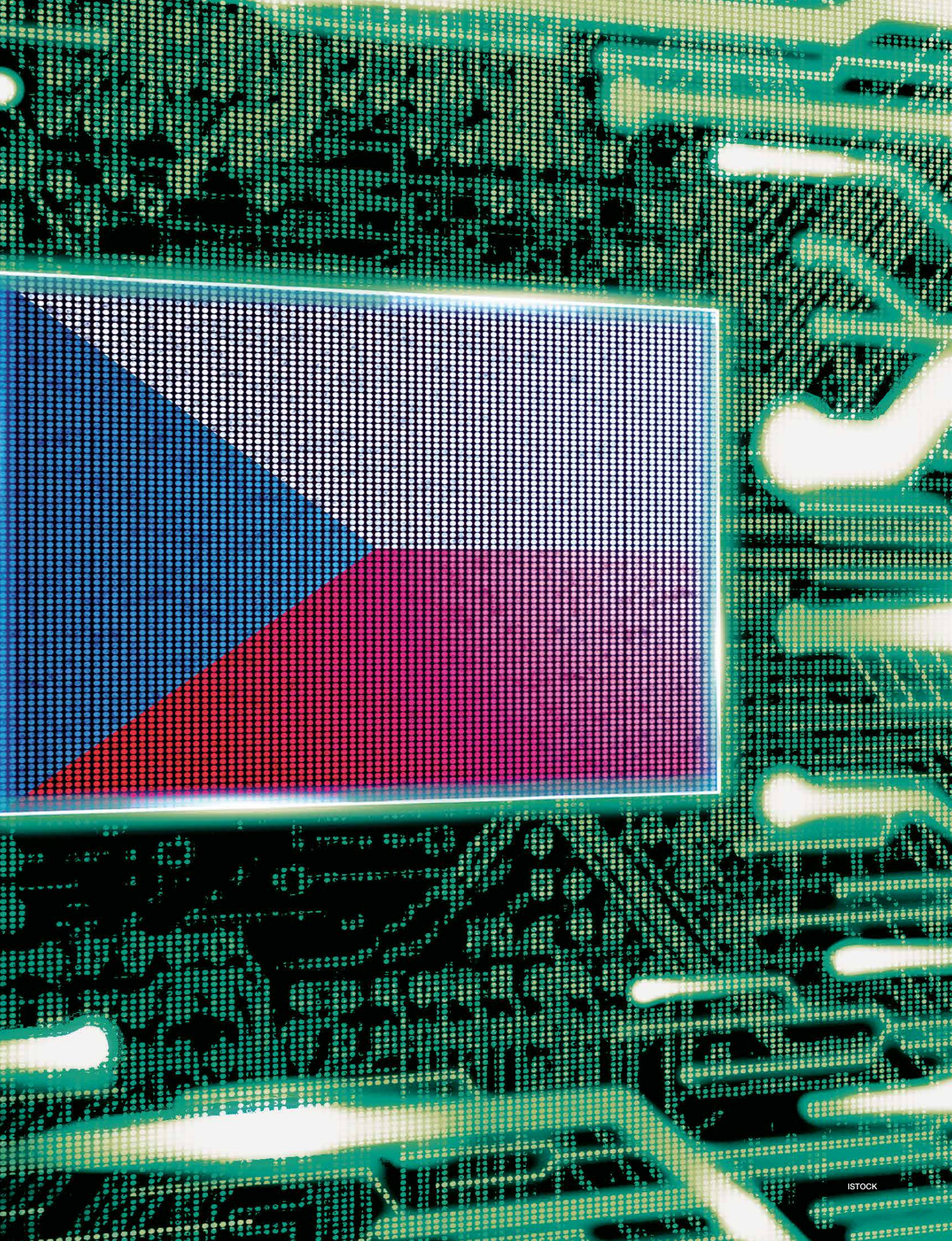
Empowering formations to act as part of the cyber mission force is essential to victory. As the number of threats continues to grow, leaders should encourage teams to get "into the cyber fight" to maximize the effectiveness of our cyber mission forces. The Capstone Concept for Joint Operations states: "Being able to operate on intent through trust, empowerment and understanding" is part of the joint strategy to ensure our leaders can operate in complex environments to prevent conflict, shape security environments and win wars while operating as part of a joint force.

Mastering cyberspace in operations requires an understanding of the environment, a framework to recognize and lead change, and the ability to empower every person as part of the cyber mission team. Leaders will continue to adjust their military decision-making and battlefield calculus as they play out conflicts in their minds through phasing, branches, sequels, and sequencing to determine key terrain, key tasks and key decision points. As cyberspace continues to grow, leaders must adopt a common frame of reference that empowers their teams to recognize change and lead transitions to win in the 21st century. □

THE CZECH REPUBLIC'S APPROACH TO CYBER SECURITY

ALL-INCLUSIVE EXERCISES ARE A NECESSARY TOOL IN SECURING CYBERSPACE

By Daniel P. Bagge and
Martina Ulmanova
National Cyber Security Center of the Czech Republic



ISTOCK

The rapid pace of technological innovation makes it difficult for those who aren't immersed in the cyber security field to fully understand the threats posed by cyber-savvy terrorists and criminals. This is especially true for governments and private institutions that are mostly unaware of the potential impacts when these technological innovations are turned against them. The new methods and sophistication of attacks and the expanding number of targets are frequent topics of public reports and debates. A society exposed to this kind of information expects its government to be prepared by creating a resilient and secure cyberspace. But how can a government stay ahead of evolving technology, particularly when bureaucratic systems tend to be slow in responding to challenges that are mostly unknown to the decision-makers?

Consequently, staying up to date on technology developments, and being able to quickly adapt to new threats, requires being cyber-knowledgeable. However, information technology (IT) experts and those employed in the technology industry cannot be fully aware of the implications that IT products and solutions have on national security. Technical personnel on operational levels and cyber security managers are not familiar with the processes of political, diplomatic and strategic decision-making. They often live in the narrow tech world. Likewise, senior leadership, law enforcement officials and policymakers face difficult challenges in their work without knowing the technological implications and impacts associated with cyber incidents.

Getting technically skilled professionals to understand the governmental challenges, while at the same time getting government representatives to deepen their understanding of the possible impacts of cyber-related incidents, presents a real challenge. Because of limited time and a lack of tools on a national level to educate people on a large scale and in a timely manner, the best way to address this challenge is through cyber security exercises.

Not only do they have a direct impact on the skill set of participants, they can provide a real-time evaluation of lessons learned. Cyber security exercises can be divided into a few types: tabletops, technical, hybrid or procedural, with slight overlaps among them. All types enable participants to tackle the important aspects of responding to incidents, such as teamwork, information sharing and institutional cooperation.

While technical exercises can be easily imagined by our general audience — a group of IT professionals and Computer Emergency Response Teams battling over each other's infrastructure and defending perimeters through keyboards and screens — decision-makers on a higher level cannot solve the complexities of a cyber crisis by hitting a keyboard button. Senior leaders do not face cyber-related challenges on a daily basis and may not be capable of adequately assessing the crisis and giving the right orders to lower echelons. Therefore, exercises aimed at decision-making processes are a unique opportunity for exposing senior leaders to relevant cyber-security matters. This, combined with realistic scenarios, is the best way to educate senior leadership on the importance of cyber security and its relevance to national security. One might argue that having the technical capacity might be sufficient to solve a cyber security incident or crisis, but that is not true. Although technical/operational cyber experts possess the skills and best technologies, without the relevant command and control, there is no use for them.

Moreover, there is another trend that we must be aware of in this digital age. Alongside the knowledge gap between technical staff and decision-makers, we must deal with varying capabilities and skills between younger and older generations. While young people have been widely exposed to an increasingly open Internet and find it easily accessible, the Internet age was unimaginable to many senior executives when they started their careers.

THE CZECH EXPERIENCE AND PRACTICES

In the Czech Republic, we understand the need to continually train in both the technical skills and the communication and procedural aspects of cyber security. Therefore, the National Cyber Security Center (NCSC) participates regularly in exercises on an international level, including the Crisis Management Exercise and Cyber Coalition, both organized by NATO; the Locked Shields exercise organized by the Cooperative Cyber Defense Centre of Excellence; and Cyber

IN THE CZECH REPUBLIC, WE UNDERSTAND THE NEED TO CONTINUALLY TRAIN IN BOTH THE TECHNICAL SKILLS AND THE COMMUNICATION AND PROCEDURAL ASPECTS OF CYBER SECURITY.

Europe, organized by the European Union Agency for Network and Information Security. Apart from participation in these international exercises, NCSC organized and participated in two national exercises in 2015: one tabletop designed for strategic leaders and decision-makers and a technical exercise for information and communications technology (ICT) administrators and specialists.

The Strategic Decision Making Exercise and Exercise on Cyber Crisis Management held in Prague in June 2015 was a joint initiative of the Czech National Security Authority, the European Cyber Security Initiative (Estonia) and the European Defense Agency. The exercise examined the state's ability to make decisions and efficiently use available resources to counter a cyber crisis. During the three-day event, nearly 40 participants, representing national government, military, intelligence services, the private sector, police, prosecutors and other law enforcement agencies, faced an escalating and very realistic scenario. The scenario was divided into six phases and continuous storylines with various forms of cyber threats presented. Each working group had different sets of information, requiring members to cooperate effectively. The results, including a graphic visualization of the exercise, were closely analyzed and a follow-up event was held with the main stakeholders and participants. The aim of the exercise was not to name a winner, but to identify gaps and shortcomings in decision-making and verify communication channels during a crisis based on real-world scenarios that escalated from minor incidents to military involvement and a state of emergency.

In September 2015, the NCSC was tasked with developing and carrying out a tailor-made tabletop exercise based on a real-world threat actor for the Department of Defense and U.S. Cyber Command in Washington, D.C. The exercise covered cyber/information warfare, cyber espionage campaigns, electoral propaganda, leakage of sensitive information, and code versus content hacking, among other topics. The exercise sought to raise awareness of the political and national security implications associated with significant cyber incidents and highlight the complexities of a decision-making process. The event was evaluated by participants

as a success and will be repeated in 2016. The tailor-made tabletop exercise was updated in early 2016 and conducted in June at the NATO ACT, Norfolk. The exercise was also conducted within the Visegrad 4 Cyber Security Workshop, organized by the presiding Czech Republic, in Washington D.C. The Czech

Participants at the international cyber defense exercise Locked Shields 2016 HANS-TOOMAS SAAREST, ESTONIAN DEFENCE FORCES

Republic is willing and has the capacity to share its expertise in conducting tailor-made cyber security exercises at the strategic level. At the end of 2015, the NCSC carried out a special tabletop exercise for students in the master's program for security and strategic studies at Masaryk University in Brno.

TECHNICAL EXERCISES

The first national technical cyber security exercise, Cyber Czech 2015, was conducted last year. It was organized by the National Security Authority, which is the overarching body of the NCSC, in collaboration with the Institute of Computer Science (ICS) at Masaryk University. It took place in a special, virtualized training environment called the Cyber Proving Ground (KYPO) at ICS. The opposing forces squared off in this unique, sealed-off computer system, where any code or solution can be tested without risk to external networks. The exercise was designed to expose participants to real-world cyber attacks. The scenario placed teams into a fictional rapid-reaction force of the Czech Republic. The teams were asked to assist a nuclear power plant where the ICT and ICS systems had been under massive attack. Although the defending teams were competing, the exercise encouraged information sharing and cooperation.

It was the first technical exercise in which participants from key governmental entities and other relevant authorities of the Czech Republic could participate alongside each other. Subsequently, another iteration of the exercise was conducted in March 2016. Private entities of critical information infrastructure, operating particularly in the energy sector, were given the same opportunity to participate. To underline the importance of such exercises, the prime minister of the Czech Republic personally attended the exercise. The exercises were novel in their magnitude and for allowing participants and observers to gain experience defending a significant piece of critical infrastructure. Cyber Czech was the first test of the scenario, which is also meant for use for academic research as well as by public institutions and private companies. Not only did the teams respond to attacks and technical problems, they also assessed potential legal and media impacts. Those two aspects — legal and media — are included in all national exercises because they are considered integral parts of solving potential crises and necessary to ensure cyber security.

To date, two kinds of exercises have been presented. However, based on the experience gained during these events, the NCSC realized that there is time for a hybrid approach. That means connecting the technical exercises with strategic level tabletops along with conventional crisis procedures to ensure that all national security entities are prepared for a large-scale crisis. This involves crisis management entities, the intelligence community, national security bodies, and stakeholders from the military, academia and the private sector.

FURTHER DEVELOPMENT OF EXERCISES

Exercises in the past were divided mainly in two domains — technical and tabletop. However, these domains are intertwined with the complexities and tools necessary to solve the problem set. It is

insufficient to train only technical or top-level leadership through specific exercises based on their lines of work. In a cyber crisis, they will have to coordinate responses and actions and share information not only horizontally, but also vertically. Exercises where these two worlds cooperate must be encouraged. Additionally, the private sector, academia and the media must be involved. The media is a relevant stakeholder, possessing a key to solving cyber crises. They play a crucial role in not only informing the public during cyber security events, but also in forming general public opinion. This is important in light of the rising importance of strategic communications and the overall resilience of society in understanding information operations campaigns. Last but not least, the media have a significant role in the aftermath of cyber crises. Events are often assessed not by the way they were technically handled, but how it was handled publicly. Therefore, the NCSC is planning a series of workshops for journalists to acquaint them with the techniques and importance of strategic communications and how to recognize information warfare techniques. Media representatives are regularly invited to participate or observe the exercises. The private sector often holds information vital to the solution, but governmental bodies still do not appreciate their position at the table.

Apart from conducting hybrid exercises on a national level, the future of cyber security also lies in greater international cooperation and exercises involving diverse technical and cultural backgrounds. This can be done through enhanced international cooperation between states, academia and the private sector. In the Czech Republic, we have the aforementioned KYPO, which is of academic origin based on security research and collaboration with the National Security Authority. Another cyber exercise arena is the privately owned Cyber Gym, the European branch of the Israeli Cyber Gym Co. Connecting these two cyber exercise ranges with similar installations around the world will greatly enhance the ability to train with teams that, despite the universal language of information and communications technology, have different cultural approaches to problem solving, as well as capabilities aimed at different threats.

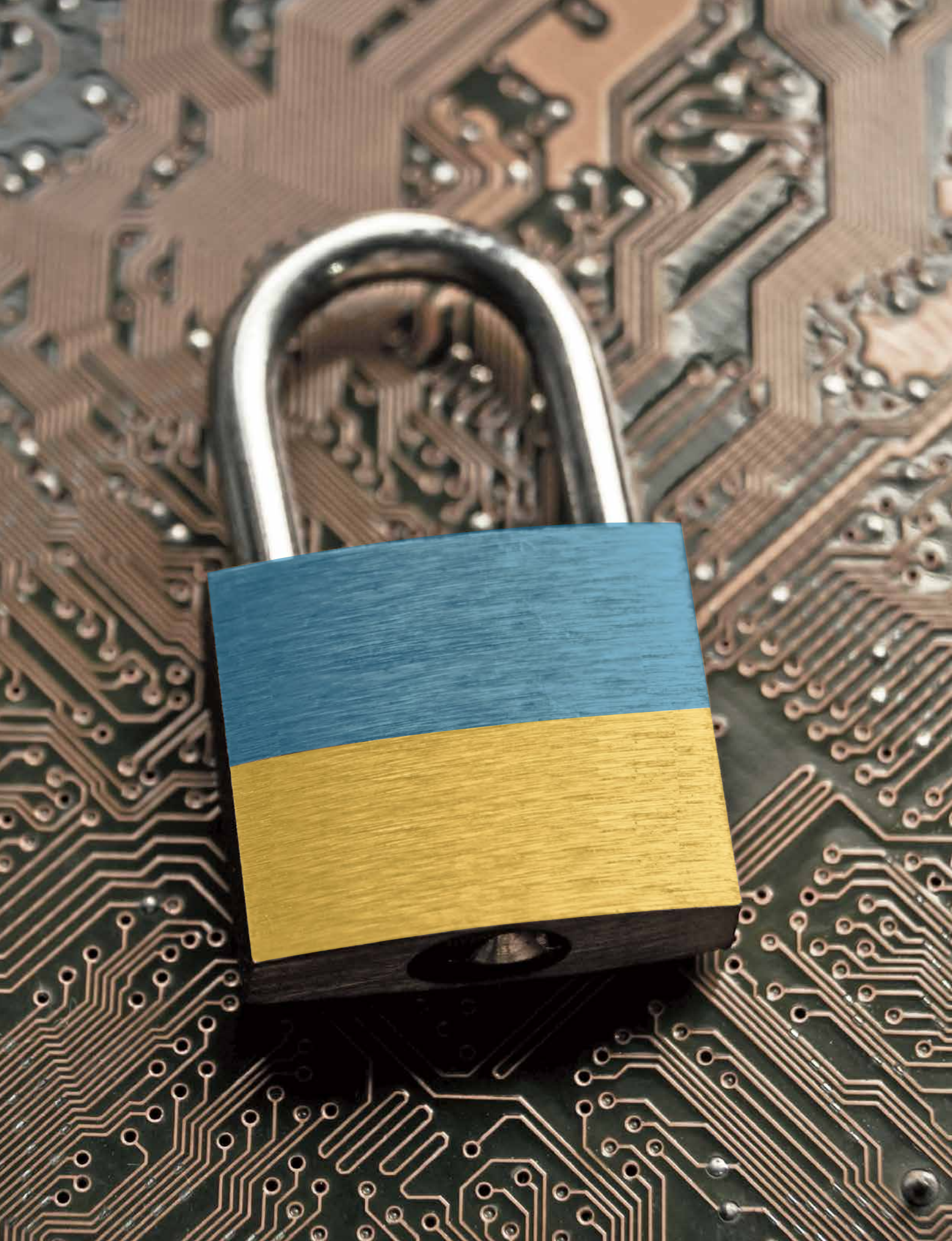
Interconnecting private, governmental and academic entities in a global cyber security exercise might not be a new concept; however, incorporating the technical part, the tabletop and spanning continents with cyber arenas is indeed new. It could simulate, in the best possible way, future conflicts between state and nonstate actors.

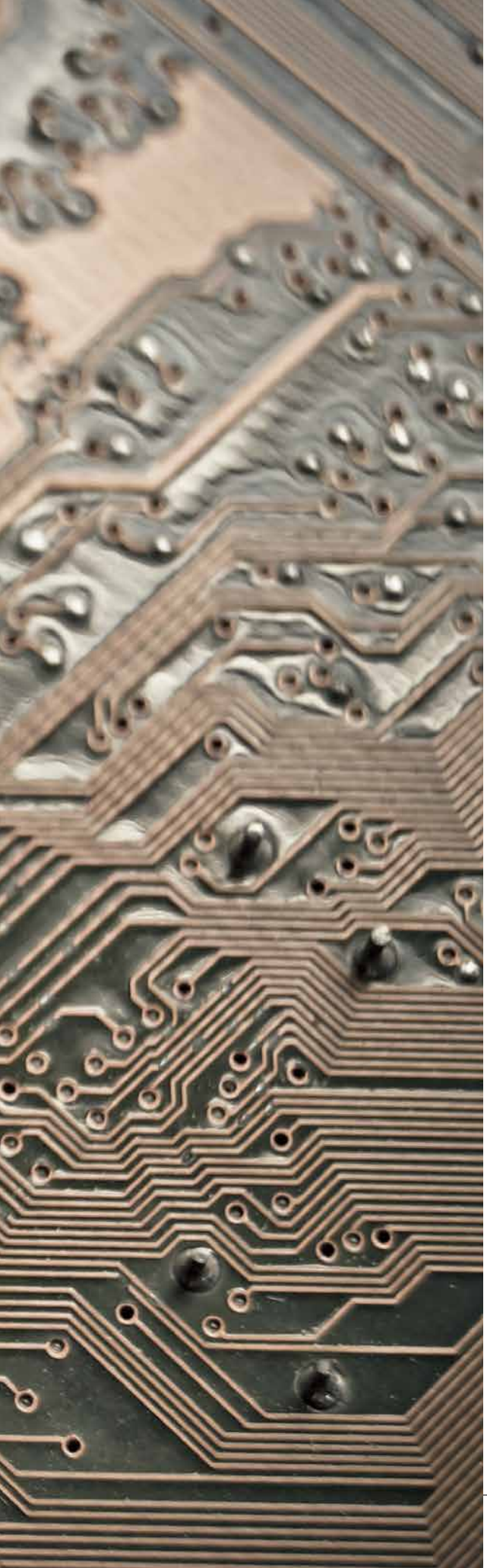
Widening the scope of the exercises and including scenarios that follow recent events are useful, but that's not enough anymore. Exercises using past incidents as a model are great for enhancing the situational awareness of participants. However, to best utilize the advantages of a cyber security exercise, it is crucial to forecast and prepare for the unexpected. Therefore, the NCSC is creating a fluid structure within the exercise-planning working group called the red cell. It is designed to enhance forecasting of possible trends and incidents and to design events that are unlikely within regular planning structures. Another issue of great concern is incorporating intelligence services into technical exercises. Therefore, the NCSC facilitates remote participation from its facilities to respect the nature of their clients' covert activities.

CONCLUSION

If policymakers understand the aspects of cyberspace through participation in exercises and thus grasp the technical basics, they are better suited for making policy. Through cyber security exercises, the gap between the policy world and technical world is narrowed and the outcomes of policy planning are tied to technical possibilities.

Getting top leadership involved in decision-making during exercises results in better decisions during crises. With a deeper appreciation gained during mockups, they do not perceive cyber as strictly IT stuff and something utterly impossible to comprehend. In preparing complex exercises, the NCSC strives to incorporate all levels of the "food chain" from the operational level to the tactical level and to the strategic level. □





PER CONCORDIAM ILLUSTRATION

COUNTERING *CYBER THREATS* TO NATIONAL SECURITY

UKRAINE DEFENDS ITS CYBER INFRASTRUCTURE IN THE FACE OF ATTACKS FROM RUSSIA

By Nataliya Tkachuck

The rapid development of information and communications technology in Ukraine, the dependence of all spheres of life on cyberspace, and the increase in cyber crime and cyber aggression on the part of Russia in its hybrid war against Ukraine all prove that cyber security is an essential element of national security.

Traditionally, cyber security in Ukraine was viewed broadly as a component of information security. However, existent cyber threats not only underline the urgent need to build efficient cyber capacity and cyber defense systems, but are also significantly changing the role of cyber security. The 2015 National Security Strategy of Ukraine, at last, recognized cyber security as a full-fledged and important part of national security.

According to reports from Ukraine's Computer Emergency Response Team, the main target of cyber attacks remains the public sector (information and telecommunication systems of the state) and critical infrastructure, mainly in the energy domain.

Recent cyber attacks on energy facilities in several regions of Ukraine resulted in electrical power outages. Thousands of people spent several hours without electricity, and the work of local industry was paralyzed. These attacks, attributed by many experts to the Russian Federation, could be considered as the first example of cyber war, or so-called hybrid war, because they accompanied an ongoing military conflict and caused substantial damage to critical infrastructure in another country.

The use of cyber attacks as a tool of information warfare is another distinctive feature of cyber threats to Ukraine's national security. Hackers, presumably connected with Russian special services, have been attacking official Ukrainian government websites to post false information and statements. This disinformation is aimed at discrediting the state's authority and increasing social tensions.

Cyber crime, another threat to Ukrainian cyber security, grew dramatically in recent years. On one hand, Ukraine is among the top five countries in the world in producing highly skilled information technology (IT) specialists, many of whom are outsourced abroad, and each year 16,000 new IT professionals earn degrees in Ukrainian universities. However, some of these specialists can be manipulated by cyber criminals and international organized crime. Often, they are unaware of the real purpose and end use of their work.

On March 15, 2016, Ukrainian President Petro Poroshenko signed a decree enforcing the Ukrainian National Security and Defense Council's resolution dated January 27, "On the Cyber Security Strategy of Ukraine."

The strategy was adopted after taking into account the challenges Ukraine faces: the aggressive actions of the Russian Federation and amplification of cyberspace usage by intelligence and special military structures, as well as by terrorists and criminals.

The purpose of the strategy is to create conditions for the safe operation of cyberspace for the benefit of individuals, society and the state. The strategy envisages a wide range of measures to ensure Ukraine's cyber security. In particular, these measures include the adaptation of state policy aimed at developing and securing cyberspace, compliance with European Union and NATO standards, the formation of a competitive environment in the sphere of electronic communications and the provision of cyber protection services.

According to the document, the Ukrainian Defense Ministry, the State Service of Special Communications and Information Protection of Ukraine, the Security Service, the National Police, the National Bank and intelligence agencies are the cornerstones of the national cyber security system.

Ukrainian authorities will review how to improve the defense of government computer systems, including at airports and railway stations, after a cyber attack on Kyiv's main airport was launched from a server in Russia in January 2016.
REUTERS

The coordinating body in the sphere of cyber security is the National Security and Defense Council of Ukraine under the President of Ukraine, now tasked with creating the National Cyber Security Coordination Center that will be part of the Council.

Yet Ukraine faces challenges to building an efficient cyber security system able to protect the country from emerging cyber threats. These include the need to approve an action plan for implementing the Ukrainian Cyber Security Strategy in 2016, to enhance mechanisms of coordination and interagency cooperation, to develop public-private partnerships based on trust, to enhance technical capabilities and education, to raise awareness about cyber threats, and to become a full member of international initiatives and collaborate in the cyber security domain.

Considering the transnational character of cyber threats, international cooperation with NATO, the Organization for Security and Co-operation in Europe (OSCE) and the European Union, as well as bilateral collaboration with partner states, plays an important role in enhancing Ukrainian cyber security.

At the September 2014 NATO Summit in Wales, the Alliance established a NATO-Ukraine Cyber Defence Trust Fund, whose main goal is to help Ukraine develop technical capabilities to counter cyber threats. The project also trains personnel in the use of these technologies and equipment and provides practical advice on policy development.

Recognizing the importance of developing common international approaches to the cyber sphere and building trust with other countries in cyberspace, Ukraine takes an active part in cyber security international initiatives. Since 2013, Ukraine has been an active member of the OSCE's informal working group on confidence-building measures, which has developed and implemented a set of measures to reduce the risks of conflict stemming from the use of information and communication technologies.

In 2005, Ukraine ratified the Council of Europe Convention on Cybercrime, though implementing it through national legislation continues. One of the most urgent tasks in the interests of national cyber security is to implement provisions concerning the empowerment of Ukraine's inquiry and investigation authorities to issue mandatory regulations for network providers on immediately securing and further storing computer data when required for investigation of crime.

The Convention on Cybercrime is an important tool of international cooperation in combating cyber crime, but there is also a strong need to optimize existing information sharing mechanisms, including a mutual legal assistance treaty to ensure quick and adequate response to cyber threats and investigations of cyber crimes at the national and international level.

Today, Ukraine faces a vast range of diverse and sophisticated cyber threats, many of which are totally new. Cyber intrusions are among the most serious challenges to national security. Enhancing cyber security is a must for guaranteeing Ukrainian national security. This requires the development and further management of an effective cyber security system and adequate comprehensive measures based on global best practices and international support. The goal is not only to counter existent cyber threats, but to ensure a balance between national security and fundamental European values. □

DEFENDING
Cyberspace *in Georgia*

A strong cyber defense requires infrastructure, legal support and multinational cooperation

BY ANDRIA GOTSIRIDZE,
director of the Cyber Security Bureau, Georgia Ministry of Defense

The cyberspace domain is growing rapidly, and with it the level and complexity of the threat to states, their information technology (IT) systems and associated critical infrastructure. Likewise, the number of cyberspace actors has grown, widening the scope of attack methods and the number of potential targeted systems. Government information/communication networks, military, and commercial projects are becoming more vulnerable to cyber attacks or cyber espionage. Governments must respond by building stronger cyber defense systems.

For a country like Georgia, in the process of ongoing digitization, these trends are a major concern, as is the potential deployment of cyber assaults by adversaries in recent conflicts and in geopolitical confrontations.

Georgia's government building in Tbilisi, where the government has adopted a cyber security policy that stresses cooperation among state, private and international organizations. REUTERS

THE THREAT

The use of cyber elements to achieve political, economic or military goals — or for gaining geopolitical advantage — is a modern day reality. Georgia's cyberspace is no exception. The nation's critical infrastructure, existing information systems, networks and infrastructure belonging to other countries and international organizations, along with foreign commercial structures, are all targets because of Georgia's membership in anti-terrorist coalitions and the Euro-Atlantic course it has taken.

The following actors pose a potential threat:

- Countries with a highly developed offensive cyber potential (Especially from Russia)
- Cyber operations of terrorist organizations
- Financially motivated cyber criminals

Cyberspace has become an important component of war and conflict. Because the Kremlin considers Georgia to be within its sphere of influence, protecting our cyberspace should be a top national security priority. Cyberspace is one sphere where a small country can confront a much larger aggressor and mount an asymmetric response.

CYBER SECURITY INFRASTRUCTURE

Good cyber defense requires a sizable investment, starting with the development of cyber architecture and modern strategic documents and ending with the integration of cyber capabilities into military operations. Georgia fully supports NATO's position that the first step toward successful joint cyber security development is building one's own cyber defense mechanism.

Georgia's first cyber security strategy and action plan was developed in 2013. This 2013-2015 document defines Georgian government policy on cyber security, reflecting the strategic goals and main principles, as well as establishing action plans. The primary strategy goal is cooperation among state, private and international organizations. Cyber security strategy involves five essential elements: research and analysis, a legal foundation, coordination on an institutional level, raising public awareness with outreach and education, and international cooperation.

At the end of 2015, at the initiative of the State Security and Crisis Management Council, Georgia's Cyber Security Strategy and Development Action Plan (2016-2018) was developed. It covers new projects and necessary events to provide cyber security.

Legal framework

The main legal framework for the sphere of cyber security is the law on information security — the purpose of which is to support effective implementation of information security, establish duties and responsibilities for the public and private sectors, and establish state control mechanisms that ensure information security policy. The law defines the Data Exchange Agency and Cybersecurity Bureau of the Ministry of Defense (MoD) as the government agencies responsible for the country's cyber security.

Under the Criminal Code of Georgia, unauthorized access to computer information; creation, utilization or distribution of malware; and the exploitation of network systems are considered crimes, as is cyber terrorism. On the international level, in 2012 Georgia ratified the Convention on Cybercrime, which was developed by the Council of Europe. Georgia now shares the common governing principles of the convention's member states and aims to create a comprehensive legal foundation on the national level while strengthening international cooperation.

Institutional infrastructure

The "Law of Georgia on National Security Planning and Coordination" defines information security as a component of national security and designates the National Security Council and the State Security and Crisis Management Council as the national security policy planning bodies. The National Security Council is a presidential advisory body, headed by the president, created to manage military development and the country's defense.

After the 2009 Russo-Georgian war, a national security review process began in coordination with the National Security Council. Cyber security was recognized as an important component of national security, and the National Security Council took on the responsibility of coordinating cyber security on a national level. However, after constitutional changes in 2014, the prime minister became the head of government. An advisory board to the Prime Minister State Security and Crisis Management Council was created, and cyber security became its responsibility. The council manages information security and is responsible for identifying and preventing internal and external threats. It also coordinates the development of a national strategy for cyber security.

In 2010, the Data Exchange Agency (DEA) of the Ministry of Justice was established to develop standards in Georgia for e-governance, data exchange infrastructures and the information and communication spheres, along with creating and implementing an information-security policy. The data exchange agency is one of the main bodies responsible for the implementation and

development of cyber security. It is within the agency's purview to ensure the cyber security of the entire government network (except for the defense sphere), which includes 36 critical infrastructure concerns.

The Computer Emergency Response Team (CERT) operates under the DEA and is responsible for responding to cyber incidents and monitoring the functionality of Georgia's governmental network. CERT has the right to demand access to critical information systems or assets. DEA sets minimum information security requirements for critical information systems.

Criminal prosecution and cyber crime investigations are conducted by the Central Criminal Police Department Division for the Fight against Cybercrime (of the Ministry of Internal Affairs). The division staffs the 24/7 contact point, which exchanges information about cyber crime with members of the Council of Europe Convention on Cybercrime.

Georgia fully supports NATO's position that the first step toward successful joint cyber security development is building one's own cyber defense mechanism.

Implementation

In 2014, the Cyber Security Bureau implemented a cyber security policy that defines Georgia's defense sector approaches and priorities for cyber security and strategic issues, and the execution of effective, stable and secure functioning of the defense sector. Since then, the Cyber Security Bureau of the MoD has been developing effective and secure information and communication technology systems for the Civil Office of the MoD and for structural subdivisions of the military's general staff. The bureau's Computer Security Incident Response Team monitors and protects the MoD's critical information and communication technology infrastructure from cyber threats and risks.

A Cyber Security Development action plan was developed based on the cyber security policy. It includes the Cyber Security Bureau's main objectives for the years 2016-2018: effective development of cyber defense capabilities, awareness building, inter-division coordination, creation of the necessary legal framework, and deepening of international cooperation. The main objective is to ensure information confidentiality, authentication and unity, including the defense of human rights.

COOPERATION

An analysis of recent conflicts involving Russia makes clear the challenges Georgia will face while developing cyber capacities. The primary challenge, as noted above, is integration of cyber security into broader strategic and practical aspects, within offensive, as well as defensive operations. Unfortunately, the best example of strategic integration that NATO can provide is Russia's actions during the Ukraine crisis. The cyber element, as events in Ukraine have shown, plays a key tactical role and is being utilized with greater frequency. The recent incorporation of cyberspace within military training, and the involvement of government departments in international cyber exercises, bodes well for cyber security development in Georgia.

The first time cyber-defense elements were used was during Exercise Didgori in 2014-2015. Alongside the general staff of Georgia were the Ministry of Internal Affairs, the State Security and Crisis Management Council and other agencies.

For the development of the Georgian Cyber Defense sphere, cooperation in information sharing, participation in technical exercises such as Locked Shields and Cyber Coalition, valued cooperation with the NATO Cooperative Cyber Defence Centre of Excellence, as well as participation in NATO Smart Defense programs, are of vital importance. In 2014, the bureau's representatives participated in the above-mentioned exercises as observers. Georgia is looking forward to strengthening cooperation with NATO in order to become full participants in Alliance exercises.

The 2014 NATO Summit in Wales asserted the fundamental importance of cyber security to NATO's future and the development of a unified defense. The Alliance has declared that joint cyber operations are not only desired but necessary. Georgia, which has experienced the results of cyber attacks and cyber espionage, realizes the importance of cyber security and shares NATO's understanding that cyber security is a global challenge that transcends national borders and demands cooperation on an international level. □

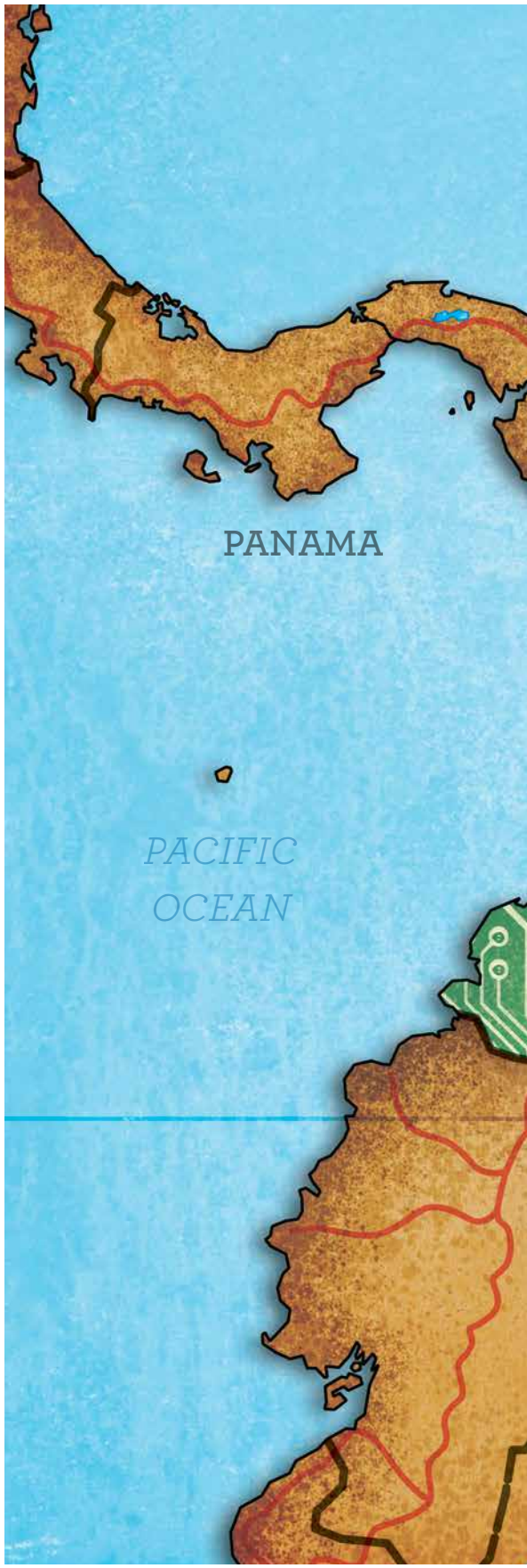
CYBER SECURITY *in* SOUTH AMERICA

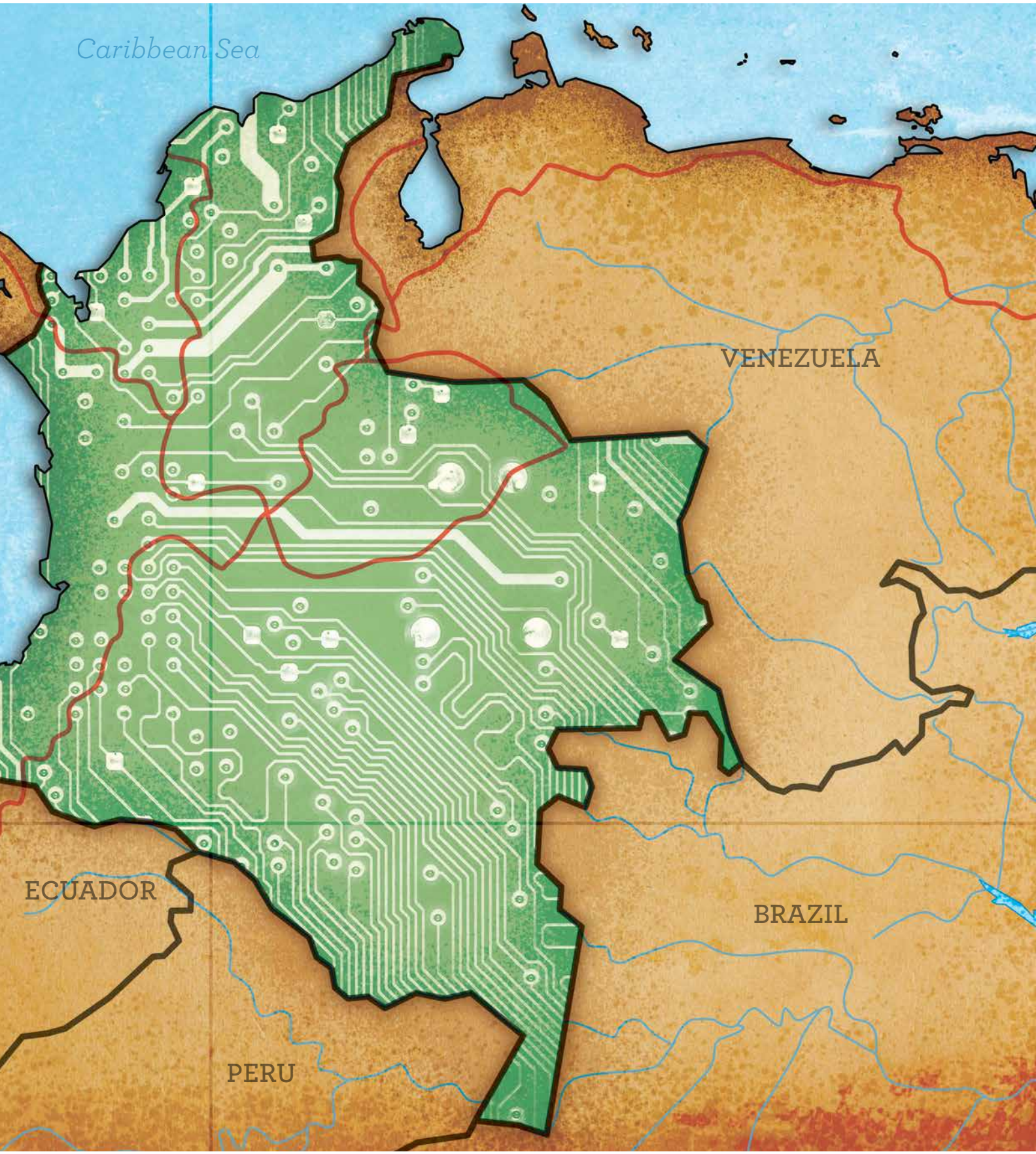
Colombia develops a comprehensive new cyber security policy

By **Alvaro José Chaves Guzmán**,
Ministry of National Defense, Colombia

The digital economy and Internet culture are spreading through the developing world at an increasingly rapid pace, and Colombia is leading the way. According to the *Affordability Report 2014*, published by the Alliance for Affordable Internet, Colombia ranked second among 51 emerging economies in Internet connectivity. The honorable second place ranking was due, the report concludes, to a series of efforts made by public and private entities to heavily invest in infrastructure in rural parts of the country, and a concerted effort to increase literacy in information and communications technology (ICT) issues. These two efforts helped the country provide access to the Internet to more than half the population.

Colombia's effort boosted Internet users significantly — from 2.2 million Internet connections in 2010 to over 9.2 million in 2014. In this regard, Colombia became the first country in Latin America with high-speed Internet coverage for all of its municipalities.





PER CONCORDIAM ILLUSTRATION

However, in recent years, the Internet has been increasingly used for criminal purposes. Since 2007, Colombia has been building a national strategy to combat cyber crime, focusing on cyber defense and cyber security. The strategy rests on three pillars:

- Pillar 1: Adopt appropriate institutional framework to monitor threats and prevent attacks, coordinate responses, and generate recommendations to address threats and risks in cyberspace.
- Pillar 2: Train personnel in information security and expand research on cyber defense and cyber security.
- Pillar 3: Strengthen legislation, international cooperation and advance adherence to international instruments to fight cyber crime.

To develop these strategies, Colombia designed and implemented four entities:

- Intersectoral Commission: Sets the strategic vision of information management and policy guidelines for technological infrastructure, public information, and cyber security and cyber defense.
- Colombia Computer Readiness Team (colCERT): Coordinates national aspects of cyber defense and cyber security.
- Joint Cyber Command General Command of the Armed Forces: Defends against cyber threats, in particular it protects national critical infrastructure and the defense sector.
- Police Cyber Center: Supports and protects through the Comprehensive Strategy against cyber crime.

The planned strategy meets three goals:

- Improves coverage and technical capabilities by creating specialized units.
- Pairs and ensures the active participation of stakeholders in the strategy through a stewardship thereof, articulates the strategy to the private sector, strengthens citizen education and improves all levels of prevention through social networks and other channels.
- Disrupts criminal structures through comprehensive crime analyses, investigates and impedes the cyber crime economy by linking the national police to different international scenarios, all aligned with the national policy document that defines the guidelines of cyber security and defense.

> Undoubtedly, the objectives of economic and social prosperity in Colombia are fundamental, and overcoming the challenge of securing and defending the nation's cyberspace is important to achieve these objectives.

Colombia's national cyber crime strategy was implemented through the Ministry of National Defense. While these efforts acknowledge the importance of the subject internationally, it is important that the national government strengthen its leadership and build a new, clear overview for an integrated approach that recognizes international best practices for addressing the risks in cyberspace.

Internet access has increased dramatically in Colombia, emphasizing the importance of good cyber security. AFP/GETTY IMAGES

Today, advances in digital networking require the establishment of a safe and secure digital environment throughout society. Even though institutions and agencies created by the Ministry of National Defense have been tasked with the responsibility to defend against and respond to cyber attacks and cyber crime, it is necessary to integrate more coherent actors in the national government, private organizations and civil society to reduce the risks of dangerous behavior or lack of information regarding necessary security measures.

This new policy document seeks to update cyber defense and cyber security goals and articulate the capacities created thus far. Its development has been supported by high levels of government with efficient and comprehensive involvement in all institutional models by each of the interested actors; namely the national government, public and private organizations and civil society. The policy objectives of the document are economic and social prosperity in the country with the goals of establishing a capable cyber defense, fighting cyber crime in the digital environment and implementing a set of fundamental principles that advance specific actions under the strategic risk management of digital security dimensions.

Undoubtedly, the objectives of economic and social prosperity in Colombia are fundamental, and overcoming the challenge of securing and defending the nation's cyberspace is important to achieve these objectives. That is why the new cyber policy document should become the foundation of a national strategy that will bring Colombia's cyber capabilities to a new level. By properly recognizing constitutional rights and freedoms in the virtual world, with a focus on risk management, the protection and defense of cyber critical infrastructure and national interests in cyberspace, protection of personal data and privacy for citizens, we can create an environment that contributes effectively to the economic and social prosperity of the country. □

A History of CYBERSPACE

BOOK EDITOR: Eneken Tikk-Ringas; published by the International Institute for Strategic Studies, London; December 2015.

REVIEWED BY: Joseph W. Vann, Marshall Center

EVOLUTION OF THE CYBER DOMAIN: THE IMPLICATIONS FOR NATIONAL AND GLOBAL SECURITY is a rare collection that explains how the cyber domain began. What makes this book appealing is the skill with which the editor and contributors take a technical subject and present it in a superb storytelling style. The book details a sequence of events that come together to inform, remind and educate the reader about what is easily taken for granted — the evolution of the cyber domain.

At first glance, the book could be mistaken for a technical publication. But every paragraph is rich in content, and the layout and style propel the book forward as if it's a technical thriller rather than an encyclopedic publication.

For cyber security strategy and policy professionals, this book is a must read and should be added to personal professional libraries. The book is documented with excellent references that allow for additional research and understanding. Moreover, the individual chapters are useful as stand-alone documents that can educate readers who don't have the time or inclination to read the entire book.

The chapters are skillfully arranged and detail the development of the cyber domain logically and understandably. The use of a glossary in the opening breaks with tradition and smartly aligns cyber terminology in alphabetical order to specific chapters. This approach furthers the reader's ability to grasp terminology specific to cyber evolution. This book will appeal to both the novice and expert. For the novice, it beautifully introduces the unknown; for the expert, it provides all historical and technical events that gave rise to the cyber domain.

The second part of the book's title can't be overlooked because it is equally central to the authors' theme. The implications for national and global security are skillfully woven into the book. The reader is reminded of the geopolitical situation in the 1950s and 1960s and how the technological

surprise of the Soviet Union's launch of Sputnik 1 triggered the Eisenhower administration to take deliberate measures to respond to fears that the United States was falling behind the Soviet Union in science and technology. This history offers perspective, before it was apparent to the inventors and users of cyberspace, on why the cyber domain would play a significant role in national and global security.

While most know the role the U.S. Department of Defense's Advanced Research Projects Agency (ARPA) played in the development of the Advanced Research Projects Agency Network (ARPANET), the book explains the role of ARPA in relation to the bigger defense industrial complex and its role in developing computer information sharing technologies needed to meet military challenges. The authors nicely reveal how many of the ideas and concepts that kicked off the ARPANET were actually germinating elsewhere at the same time. It also explains how the U.S. identified a compelling need to develop better command and control (C2) networks that reduced the fragility of early missile C2 systems. This bit of storytelling advances the reader's appreciation of the number of non-ARPA individuals and entities involved in the cyber evolution and its technological impact on national security.

With the number of contributors outside of ARPA quite large, the Pentagon financed what was then expensive equipment and made it available to the best and brightest. Effectively linking computers to one another supported pooling of resources and accelerated further sharing of ideas. The potential of what began as a bold ARPA experiment that became the ARPANET was quickly recognized for its potential to improve U.S. operational C2 systems. By giving the reader a sense of the logic of the day within the context of Cold War concerns, the authors infuse a sense of perspective of what dominated national-level decision-making of the day. The book stresses why the U.S., and to a lesser extent Western governments, understood the economic importance of developments in the cyber domain and why they purposefully restricted dissemination of cyber knowledge and related technologies to the Soviet Union, for fear the communists would use them for military applications.

In successive chapters, the book walks the reader through technical developments in the cyber domain in a cadence that highlights new technical discoveries and solutions to challenges while focusing on the importance of the cyber domain to national security. When the military branch of the ARPANET was separated from the civilian portion, the civilian side was able to establish links with scientists around the world. This created a need for technologies that could support and improve ever-growing connectivity requirements. This connectivity proved to be a key enabler that stimulated growth in new technologies and further widened the technology gap with Eastern Bloc countries.

The book consistently exposes the reader to technical and software developments and how each prompted innovation that would contribute to the much larger evolution of the cyber domain. When mapping the evolution of cyber technology from the 1970s through the 1990s, the writers provide a clear appreciation of how and why the cyber evolution was impacted by growing commercial applications that created new customers and, in turn, demand for new technology.

The increasing sophistication of hardware and software created the need for Internet governance. The authors focus on the evolution of various government forums and the challenges and considerations of managing connectivity. This provides a clear understanding of how Internet governance evolved and why limited "government" intrusion in the Internet may actually be responsible for its enormous utility and growth.

The final chapters paint a clear and surprisingly contemporary picture of the importance of cyber security and the value that cyber plays in supporting the intelligence community. While carefully avoiding or promoting a debate as to the role of the cyber domain in the revolution in military affairs, readers cannot help arriving at their own assessment of the pivotal role that cyber plays in the modern day military and national security.

This exceptional book should enjoy wide readership among those interested in the cyber field, but herein is the book's greatest flaw: its price. At 90 British pounds, about U.S. $128, its steep price will likely limit availability, robbing this book of the readership it deserves. □

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship

Registrar
George C. Marshall European Center
for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650

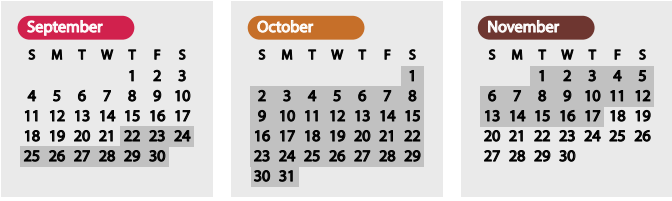
www.marshallcenter.org
registrar@marshallcenter.org

Admission
The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

The Marshall Center's flagship resident program, an eight-week course, provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

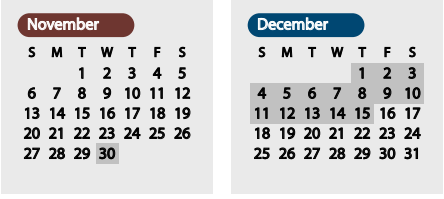
PASS 16-15
Sept. 22 -
Nov. 17, 2016



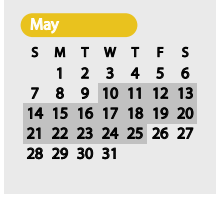
PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)

This two-week resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

CTOC 17-01
Nov. 30 -
Dec. 15, 2016



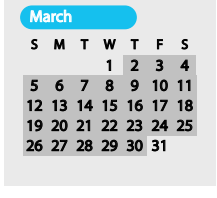
CTOC 17-09
May 10 - 25, 2017



PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

This four-week program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

PTSS 17-05
Mar. 02 - 30, 2017

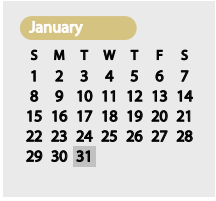


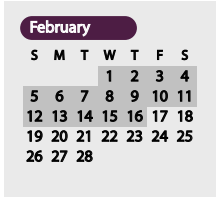
PTSS 17-13
July 06 -
Aug. 03, 2017

PROGRAM ON CYBER SECURITY STUDIES (PCSS)

The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

PCSS 17-04
Jan. 31 -
Feb. 16, 2017

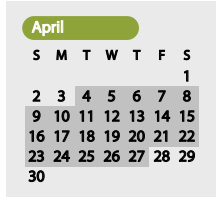




SEMINAR ON REGIONAL SECURITY (SRS)

The three-week seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

SRS 17-07
Apr. 04 - 27, 2017



SENIOR EXECUTIVE SEMINAR (SES)

This intensive five-day seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

SES 16-9
Sept. 12 - 16, 2016

SES 17-10
June 05 - 09, 2017

Alumni Programs

Dean Reed
Director, Alumni Programs
Tel +49-(0)8821-750-2112
reeddg@marshallcenter.org

Alumni Relations Specialists:

Barbara Wither
Southeast Europe
Languages: English, Russian, German, French
Tel +49-(0)8821-750-2291
witherb@marshallcenter.org

Christian Eder
Western Europe
Languages: German, English
Tel +49-(0)8821-750-2814
christian.eder@marshallcenter.org

Marc Johnson
Central Asia, South Caucasus, Russia, Moldova, Ukraine, Belarus - Cyber Alumni Specialist
Languages: English, Russian, French
Tel +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Christopher Burelli
Central Europe, Baltic States - Counterterrorism Alumni Specialist
Languages: English, Slovak, Italian, German
Tel +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org

Donna Janca
Africa, Middle East, Southern and Southeast Asia, North and South America - CTOC Alumni Specialist
Languages: English, German
Tel +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Contribute

Interested in submitting materials for publication in *per Concordiam* magazine? Submission guidelines are at **http://tinyurl.com/per-concordiam-submissions**

Subscribe

For more details, or a **FREE** subscription to *per Concordiam* magazine, please contact us at **editor@perconcordiam.org**

Find us

Find *per Concordiam* online at:
Marshall Center: **www.marshallcenter.org**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **www.facebook.com/perconcordiam**
GlobalNET Portal: **https://members.marshallcenter.org**
Digital version: **http://perconcordiam.com**

The George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany

MARSHALL CENTER