VOLUME 5, ISSUE 2, 2014

per Concordiam

Journal of European Security and Defense Issues

- **COMBINED ENDEAVOR**
  Exercise builds interoperability
- **REGIONAL ROUNDUP**
  Eastern Europe's cyber readiness
- **NATO SCHOOL**
  Training to thwart attacks
- **CENTRAL ASIA ONLINE**
  Balancing freedom and security

PLUS
Containing Afghan heroin
Free movement of labor
EU Eastern Partnership

DEFENDING CYBERSPACE

Table *of* Contents

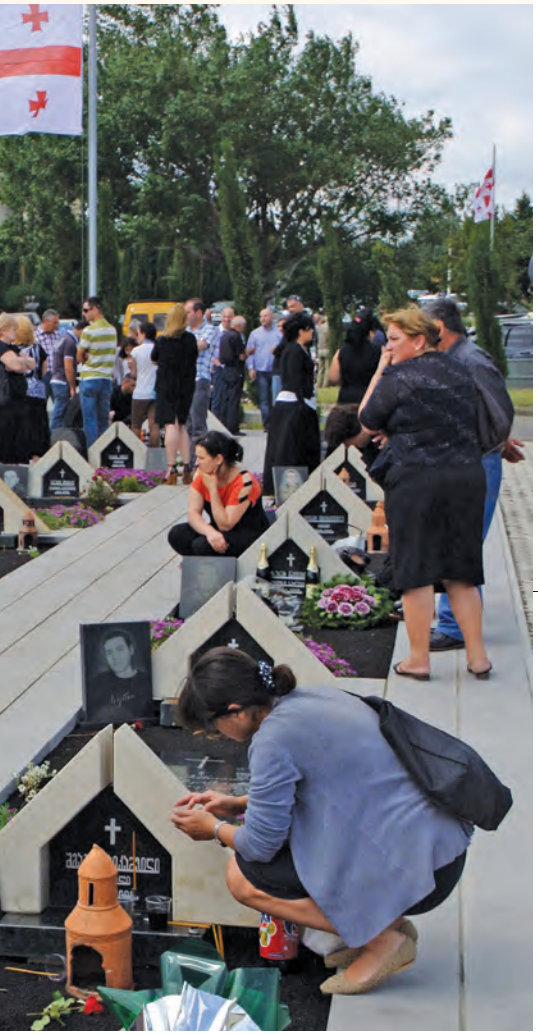
features

ON THE COVER

PER CONCORDIAM ILLUSTRATION

The defense of cyberspace is a task that transcends individual nations. Nefarious actors use the Internet not just to steal money and information but to destabilize countries and disrupt commerce. To thwart this growing problem, multinational coordination of cyber security policy is critical.

departments



in every issue

COOPERATION

SECURITY

POLICY

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 18th issue of *per Concordiam*. This issue covers the complex problem of cyber security, from the legal framework required to prosecute cyber criminals to the whole-of-government approach necessary to protect critical public and private infrastructure from cyber threats. As societies become increasingly reliant upon information technology systems and networks to provide essential daily services , the need for policy, strategy and enforcement agencies to protect networks, capabilities and services also increases. In addition, the cyber dimension is not geographically delineated, nor is participation in the cyber arena limited to identifiable state actors, which makes policing, investigation and prosecution more difficult. Governments and societies should strive to create comprehensive cyber security policies that consider the public and private nature of cyber, and the balance between privacy and protection.

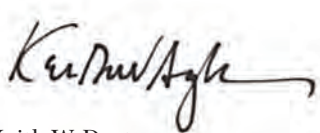
In recent years, we have seen improvements in cyber security throughout Europe and Central Asia. Both Estonia and Georgia have implemented tailored cyber security programs and policies, after experiencing significant cyber attacks in 2007 and 2008. Georgia developed a comprehensive cyber strategy that included the public and private sectors, and Estonia continued to improve the NATO Cooperative Cyber Defence Centre of Excellence based there. In 2014, United States European Command celebrated the 20th anniversary of Combined Endeavor, a longstanding human and systems interoperability exercise among NATO and Partnership for Peace nations. Cyber Endeavor was created in 2009 to increase partner capacity in cyber defense, and improve the skills of several nations participating in Combined Endeavor. Combined Endeavor included 40 nations sharing information at the human and system level. In 2013, the NATO Cooperative Cyber Defence Centre of Excellence published the *Tallinn Manual,* a legal framework that applied established international laws to both hostile offensive cyber operations and legitimate cyber self-defense measures. The Czech Republic recently created the National Cyber Security Centre to coordinate a whole-of-government approach to cyber security, and consolidate all cyber-related efforts. Several nations have created computer emergency response Teams (CERTs), and have begun designing legal and policy frameworks to establish cyber defense and responses. These are great examples of nations understanding the cyber threat and implementing policies, creating capabilities and adopting procedures to mitigate threats and improve security in the cyber domain.

As nations continue to address the growing reliance on the cyber domain, it is important that decision makers understand these threats and develop policy and strategy to implement robust cyber security programs. It requires leadership involvement in establishing priorities, policy, legal frameworks and international agreements. It also requires whole-of-government and whole-of-society approaches, including cooperation between public and private sectors. As states improve their capabilities to combat cyber crime, they will face the task of balancing security with privacy and establishing partnerships with the private sector.

At the George C. Marshall European Center for Security Studies, we are proud to inaugurate the Program in Cyber Security Studies (PCSS) to meet the needs of senior government officials aiming to improve their knowledge and understanding of transnational cyber security challenges. Our program is a nontechnical course that can help legislators, diplomats, ministerial staff, law enforcement and military leaders gain familiarity with cyber security best practices. This program is taught by world leaders and experts from government, industry and academia. Our program will include a two-week resident course, non-resident events throughout Europe and Central Asia and cyber-specific alumni events. The PCSS will focus on whole-of-government approaches to cyber challenges and developing cyber strategy and policy. It will help leaders understand the cyber environment, and build a framework for international collaboration.

We welcome your comments and perspective on these topics and will include your responses in future editions. Please feel free to 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.

CONTRIBUTORS

Daniel P. Bagge is a cyber security/policy specialist at the National Cyber Security Center, National Security Authority of the Czech Republic, where he coordinates national cyber security strategy, strategic planning and development. He leads the Industrial Control Systems Cyber Security Protection working group and has worked for various government ministries. He holds a master's degree in International Security Studies, a post-graduate program jointly offered by the Marshall Center and the Universität der Bundeswehr München.

Zvonimir Ivanović, a head police inspector in Serbia, is an assistant professor at the University of Criminalistics and Police Studies in Belgrade. He specializes in criminal tactics, police questioning and interrogation, criminal profiling, cyber crime, and evidence gathering. He has participated in several international projects, including Police and Cybercrime, 2009-2012, and the Standards and Procedures for Fighting Organized Crime and Terrorism in a Climate of International Integration, 2011-2014.

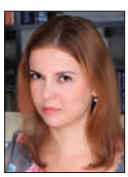
Nuria Kutnaeva is an independent researcher from the Kyrgyz Republic. Previously, she led the international relations program and served as vice president of the International University of Central Asia in Tokmok. She earned a master's degree in political science from Eichstätt University in Germany and another from the Organization for Security and Co-operation in Europe Academy in 2005. In 2013, she received a doctorate in nuclear security issues in Central Asia.

Dr. Hans-Georg Maaßen is director general of the German Domestic Intelligence Service, BfV. He led various directorates-general in the German Federal Ministry of the Interior since 1991, including ones devoted to counterterrorism and the legal rights and responsibilities of foreigners living in Germany. He is a legal advisor and studied law in Cologne and Bonn.

Maj. Daniel Singleton is a U.S. Army foreign area officer. He has served in the Office of Defense Cooperation in Riga, Latvia, and as a political-economic officer at the U.S. Embassy in Baku, Azerbaijan. He is pursuing a graduate degree in the University of Wisconsin's Russian, East European and Central Asian Studies program. He also holds a master's degree in philosophy from the University of Colorado.

Natalia Spinu is the head of the Cyber Security Center CERT-GOV-MD, S.E. Center for Special Telecommunications, State Chancellery of the Republic of Moldova. She has been department chief of Moldova's Special Telecommunications Centre and project coordinator at the Information and Documentation Centre on NATO. She is a 2012 graduate of the Marshall Center's Program in Advanced Security Studies, a graduate of the European Training Course in Security Policy at the Geneva Centre for Security Policy, and has a master's degree from the European Institute of the University of Geneva.

Police Lt. Giorgi Tielidze is a senior advisor to the State Security and Crisis Management Council, Department of Internal Security and Public Order at the Ministry of Internal Affairs of Georgia. Since December 2012, he has served on Georgia's Cybercrime Convention Committee. He earned a bachelor's degree at Tbilisi State University and is pursuing his master's at Ilia State University in Tbilisi.



Liis Vihul is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Her work focuses on the legal requirements for attributing cyber operations to states. She also educates legal professionals on cyber matters. She holds master's degrees in law from the University of Tartu and information security from the University of London.

Robert Watson is chief of the combined interoperability branch at the U.S. European Command C4 and Cyber Directorate. He retired from the U.S. Army as a lieutenant colonel specializing in operations research analysis. He has taught at the United States Military Academy at West Point.

per Concordiam

Journal of European Security and Defense Issues

Cyber Security

Volume 5, Issue 2, 2014

George C. Marshall European Center for Security Studies

Leadership

Keith W. Dayton
Director

Hermann Wachter
German Deputy Director

Ben Reed
U.S. 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 pubb lished 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 magazine addresses security issues relevant to Europe and Eurasia and aims to elicit thoughts and feedback from readers. We hope our previous issues accomplished this and helped stimulate debate and an exchange of ideas. Please continue to share your thoughts with us in the form of letters to the editor that will be published in this section. Please keep letters as brief as possible and specifically note the article, author and magazine edition to which you are referring. We reserve the right to edit all letters for language, civility, accuracy, brevity and clarity.

EDITOR'S NOTE: In *per Concordiam* Volume 4 Issue 4 the article "Securing the Internet" refers to the NATO Cooperative Cyber Defence Centre of Excellence as an Estonian Centre. The NATO CCD COE is a multinational entity accredited by NATO and is located in Tallinn, Estonia.

Send feedback via email to: editor@perconcordiam.org

ARTICLE SUBMISSIONS

per Concordiam is a moderated journal with the best and most thoughtful articles and papers published each quarter. We welcome articles from readers on security and defense issues in Europe and Eurasia.

First, email your story idea to editor@perconcordiam.org in an outline form or as a short description. If we like the idea, we can offer feedback before you start writing. We accept articles as original contributions. If your article or similar version is under consideration by another publication or was published elsewhere, please tell us when submitting the article. If you have a manuscript to submit but are not sure it's right for the quarterly, email us to see if we're interested.

As you're writing your article, please remember:

- **Offer fresh ideas.** We are looking for articles with a unique perspective from the region. We likely will not publish articles on topics already heavily covered in other security and foreign policy journals.
- **Connect the dots.** We'll publish an article on a single country if the subject is relevant to the region or the world.
- **Do not assume a U.S. audience.** The vast majority of *per Concordiam* readers are from Europe and Eurasia. We're less likely to publish articles that cater to a U.S. audience. Our mission is to generate candid discussion of relevant security and defense topics, not to strictly reiterate U.S. foreign policy.
- **Steer clear of technical language.** Not everyone is a specialist in a certain field. Ideas should be accessible to the widest audience.
- **Provide original research or reporting to support your ideas.** And be prepared to document statements. We fact check everything we publish.
- **Copyrights.** Contributors will retain their copyrighted work. However, submitting an article or paper implies the author grants license to *per Concordiam* to publish the work.
- **Bio/photo.** When submitting your article, please include a short biography and a high-resolution digital photo of yourself of at least 300 dots per inch (DPI).

Email manuscripts as Microsoft Word attachments to: editor@perconcordiam.org

EPA

FORGING EFFECTIVE

Cyber Defense

Nations that share democratic values should cooperate to stop threats emerging from cyberspace

By **Dr. Hans-Georg Maaßen,** director general of the German Domestic Intelligence Service, BfV

Protecting highly sensitive information and critical infrastructure is the most important aspect of domestic security. Modern societies depend on these to function well. Data protection and round-the-clock availability of communications systems have become matters of survival in the 21st century. Cyberspace offers enormous opportunities, but it also involves real threats to domestic security. Cyberspace is full of threats to data security, electronic systems and personal privacy.

Germany's domestic intelligence service, BfV, has been tasked with the collection and analysis of data related to threats to the security of the state and intelligence activities carried out on behalf of foreign powers, regardless of whether they are based on human sources or surveillance images and electronic intercepts. The BfVserves as an early warning system for the federal government and parliament. The information it gathers is used to compile situation reports and assist in executive decision-making.

Data protection in cyberspace

A year ago, cyber attacks — or perhaps cyber war — would have received most of our attention. Today, Edward Snowden, who worked at the United States National Security Agency (NSA), betrayed state secrets and disclosed more information than the best Russian spy could have collected during the Cold War. And Snowden wasn't even a top agent with special training but simply a person with access — thanks to modern technology — to large amounts of data that no one would have been able to tap into in the past.

These disclosures have raised our threat awareness. How will we effectively protect data from being maliciously accessed by individuals "on the inside" in the future? We have a better understanding of why data protection is necessary, but those who use the Snowden case as a pretext to keep silent on real threats, such as electronic attacks from China or Russia, are turning a blind eye to a dangerous situation.

For decades, German and U.S. intelligence services have profited from close cooperation. Thanks to this cooperation, a series of terrorist attacks against Germany have been prevented.

PREVIOUS PAGE: Gerhard Schindler, left, president of the German Foreign Intelligence Service, BND; Hans-Georg Maaßen, center, director general of the German Domestic Intelligence Service, BfV; and Jörg Ziercke, president of the Federal Criminal Police Office, BKA, await the beginning of a Constitutional Court hearing in Karlsruhe on Germany's counterterrorism database.

Legal basis for signals intelligence

All intelligence services engage in strategic signals intelligence gathering — not only those from the U.S. However, U.S. signals intelligence such as the NSA's PRISM surveillance program is different because it is based on laws that allow the storing and filtering of data to the extent technically possible. U.S. intelligence agencies may collect data inside and outside the U.S. if deemed necessary, as in the case of counterterrorism efforts. Within U.S. borders, U.S. laws apply. And it makes sense for the U.S. to make use of all legal and technical means available. But how about in cyberspace? No rules yet exist for this domain.

The jurisdiction of the BfV, on the other hand, ends at the German border. The German approach is different. Germany's foreign intelligence service, the Bundesnachrichtendienst, does not store data — it only filters it. From a continuous flow of data, it takes only what is relevant for its ongoing work.

U.S. and German intelligence services have one thing in common: A legal basis is required to filter data. In both countries, it is unlawful to collect data and spy on private individuals for economic or political reasons. Depending on the facts and requirements of any given case, filtering data is lawful to fight terrorism, to protect national security and to combat proliferation and international organized crime.

The U.S. and Germany adhere to the rule of law, and this also applies to their intelligence services. They may not exceed their powers and collect and store data without legal authorization. At the BfV we observe the law, and oversight of intelligence services is provided by such authorities as the Parliamentary Control Committee, the German Bundestag's G-10 Commission and independent courts. The U.S. system is similar in this respect. From our perspective, there is no doubt that our American colleagues are operating within the law.

The same cannot be said for all states engaged in strategic signals intelligence activities. Other states also have access to network nodes on land, or international broadband cables, or have submarines that can tap into these deep-sea cables. These states may have no

Owing to its political and economic strength, Germany has long been a preferred target of foreign intelligence services, both in the real and virtual worlds.

legal basis for filtering data, nor any scruples about filtering, collecting and storing data to promote their own economic interests.

Cyber attack challenge

Apart from signals intelligence, cyber attacks have become an ever more urgent problem. Electronic attacks by intelligence services present a great threat potential in terms of quantity and quality. Cyber attacks can be carried out via the Internet or by manipulating hardware. Owing to its political and economic strength, Germany has long been a preferred target of foreign intelligence services, both in the real and virtual worlds. The large number of cyber attacks on federal agencies confirms this.

Cyber attacks are no longer simply Trojan horses or virus-infected emails but have developed into customized viruses that apply social engineering to target victims with precision. The attacker knows exactly who holds an important position and who might open and read an email with a certain subject line. Some intelligence work is required to identify this type of virus or Trojan horse.

Cyber attacks most often seek to weaken Germany's foreign and security policy, as well as German and European fiscal policy. Industrial espionage focuses on the German economy, and the states behind these efforts are usually those that routinely use intelligence services to promote their own economy. The number of attacks against the German private sector is unknown because companies that have been victims of cyber attacks tend to remain silent.

Extremists and all kinds of terrorists also take an interest in cyberspace. They use it for agitation, propaganda and recruitment. Cyber wars are directed against a state and its vital infrastructure but also against extremist opponents. In most cases, the attackers' capabilities have been restricted by their limited knowledge, allowing only low-level attacks. But if they are sufficiently skilled, extremists would happily cause greater damage.

Cyber threats come from different vectors of the extremist spectrum. It will be interesting to see whether cyber guerrilla attacks will become the preferred option of militant resistance for left-wing extremists in this century. A couple of years ago, "jihadists" called for the establishment of an "Institute for Electronic Jihad" and emphasized the importance of Supervisory Control and Data Acquisition attacks on control systems for power and water supplies, gas grids, electronic airport and railway systems, and computerized stock exchanges and banking.

The threat is evolving with the same rapidity as cyberspace is developing. Therefore, we need to cooperate and share information with foreign partners whose interests and values we share. □

This article is based on a lecture at the 10th International Law Conference of the Konrad Adenauer Foundation in Bonn, Germany, on October 16, 2013.

Striving for cyber excellence

Centre of Excellence leads NATO's efforts in cyber research and training

By Liis Vihul, NATO Cooperative Cyber Defence Centre of Excellence

In the midst of defense spending cuts, cyber security stands out as an exception to the prevailing cutbacks. States are boosting investments in this area, not only to improve their own resilience to hostile cyber operations, but also to develop offensive capabilities in support of their national and foreign security policy objectives. In light of the growing investment in and overall attention toward cyber security, the Tallinn, Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is attracting attention from NATO Allies to whom membership is open, and beyond.

Since the establishment of the first NATO Centre of Excellence (COE) in 2005, 18 COEs have mushroomed on the Euro-Atlantic map. Motivated by the prospect of a permanent NATO presence in their region, all seven Central and Eastern European states that acceded to NATO in 2004, including Estonia, already operate or are in the process of setting up a COE.[1] All COEs are idiosyncratic by virtue of the fact that they are designed to complement and enhance NATO capabilities in specific areas ranging from military medicine to energy security. Somewhat prophetically, Estonia saw its opportunity in cyber defense and presented NATO with a proposal to establish a cyber-oriented COE a few years before 2007, when the state became a victim of a large-scale cyber attack that thrust cyber security and defense to the forefront of political agendas.

Estonian Foreign Minister Urmas Paet, left, and U.S. Secretary of State John Kerry celebrate the signing of the U.S. Estonia Partnership Statement in December 2013. The document reaffirms the countries' commitment to a secure Internet. THE ASSOCIATED PRESS

CCDCOE: SIX YEARS LATER

Officially founded in 2008, the CCDCOE is currently a partnership of 11 states. In addition to Estonia's tricolor flag, the colors of Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the United States have been raised in the CCDCOE flag court. The Czech Republic, France and the United Kingdom will soon become member states, and Greece and Turkey are similarly undergoing the membership process. As such, and considering that COE membership is only open to NATO nations, the Tallinn COE unites many of the most prominent cyber states of the Alliance. Despite being ineligible for full membership, non-NATO nations may become contributing participants. Decisions are made on a case-by-case basis, and talks have already begun with Austria, Finland and Sweden.

Contrary to popular belief, the approximately 40-person CCDCOE is not an operational entity. Instead, it is oriented toward research and training and facilitating numerous academic, semi-academic and training events each year. Its work is divided into three categories: law and policy, technology and strategy. The center has a number of success stories that have earned it international visibility and credibility. These include the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, the inception of an annual conference tradition with high-level speakers and worldwide participants, and the ability to convene nearly 300 information security professionals annually for the live-fire cyber defense exercise dubbed Locked Shields.

THE TALLINN MANUAL

The question of how international law governs hostile cyber operations was embraced by numerous scholars as a direct result of the 2007 cyber attacks on Estonia and those against Georgia during its armed conflict with Russia the next year. The threat of highly disruptive cyber operations had evolved from a hypothetical scenario to a real world phenomenon. The unique characteristics of cyberspace and operations in this environment raise new and difficult issues for legal scholars. These issues include the speed with which events can unfold and consequences can manifest themselves, and the engagement of states not directly involved as originators and targets (either as simple transit states or those whose territory is used, knowingly or not, to carry out the operations, for example, by setting up a command and control server for a botnet attack). Other issues include the difficulties of determining the originators of attacks, the intangibility of data, and the use of cyberspace – an environment primarily employed for civilian purposes and governed by civilian entities – for military functions.

To untangle these complex legal matters, in 2009 the CCDCOE convened an international group of 20 noteworthy academics and practitioners. They undertook the task of producing a legal manual to explain how international law applies to the most severe cyber operations, allowing for self defense as well as those carried out during an armed conflict. Their work was published as the *Tallinn Manual* in 2013.

Yet, recognizing that states struggle every day with cyber operations that do not reach the armed attack threshold entitling them to act in self-defense, the CCDCOE has launched a follow-on endeavor titled "Tallinn 2.0." This project focuses on how international law regulates hostile cyber operations of lesser gravity that, nonetheless, cause states significant harm. That could include severe financial loss and the inaccessibility of vital online services. The project will also take an in-depth look at the obligations that international law places on states and how these apply in the cyber context, such as the duty not to knowingly allow one's territory to be used for acts that violate the rights of other states, and the prohibition of intervention into the affairs of other states. Once the project concludes in early 2016, the second expanded edition of the *Tallinn Manual* will be published. The manual will then cover the entire spectrum of international law applicable to state cyber operations in times of peace and war.

The center, in cooperation with the U.S. Naval War College and the NATO School Oberammergau, also contributes to the education of legal professionals by offering a profound course based on the *Tallinn Manual*. Taught by many of its key authors and information technology (IT) experts from the center who explain how cyber operations are carried out from a technical perspective, the International Law of Cyber Operations course runs twice a year and is open to all interested individuals.[2] It is vital for states that engage in cyber operations to educate their legal advisors. Other states should understand that so long as their cyber infrastructure is vulnerable to manipulation, once an attack materializes the need to comprehend the international legal implications of that situation arises. Therefore, training legal professionals on cyber matters is critical even in states where ambitions in cyberspace are limited. In today's security environment, states that rely upon cyber infrastructure must consider themselves susceptible to attack and prepare to handle them within the confines of international law.

In light of the growing investment in and overall attention toward cyber security, the Tallinn, Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is attracting attention from NATO Allies to whom membership is open, and beyond.

COURSES AND EXERCISES

In addition to the International Law of Cyber Operations course, the center has developed an impressive portfolio of technical courses.[3] These delve into matters such as monitoring network traffic and logging security events, malware reverse engineering, and understanding how IT systems are attacked and how those attacks can be mitigated. Considering the high demand for these courses, attendance priority is given to students from the center's sponsoring nations. If vacant seats remain, they are offered to NATO nations and Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.

Each June, the CCDCOE organizes a major international cyber security conference called CyCon. Designed to inspire interdisciplinary discussion, the conference brings together more than 400 strategy, law, ethics and IT experts from the civilian and military sectors. Sessions run in two tracks and feature distinguished speakers (Estonian President Toomas Hendrik Ilves, known for his IT savviness and drive for technological developments, traditionally opens the event). CyCon provides a unique opportunity for professional exchanges and networking. In 2014, the theme of the conference in June was "active defense."[4]

Locked Shields, the center's real-time network defense exercise, is perhaps the most anticipated event of the year among participating security professionals. Twelve blue teams, each given access to identical, poorly configured networks shortly before the exercise commences, compete to determine who can best defend their network against cyber attacks by the red team. Just as in a sports competition, the exercise's three days are filled with excitement and competition, frustration and disappointment. But above all, Locked Shields is a unique learning opportunity for participants, requiring defenders to handle cyber attacks and maintain the functionality of the assigned networks under time pressure. The attackers, on the other hand, must discover alternative ways to target systems if the defenders repair vulnerabilities that were initially planned to be exploited (a skill that can be used when assessing the resilience of information systems against true hostile attacks). Moreover, Locked Shields tests the skills of legal advisors who analyze the ongoing cyber attacks in the context of the exercise's fictional scenario.

The militarization of cyberspace is a direct and inevitable consequence of societies' increasing reliance on information technology. It would be illogical to assume that states would not take advantage of cyberspace possibilities so long as they contribute to the accomplishment of national goals. As such, the notion of "cyber" is an unavoidable item also on NATO's collective security and defense agenda. The CCDCOE supports the Alliance by producing high-level research and training in a number of disciplines related to cyber security. As investments in cyber capabilities grow, so too will the role that the CCDCOE plays in helping to understand this domain. □

1. However, it is important to note that all COEs operate outside NATO's financial and command structure. For more on COEs, see Col. Andrew Bernard, "NATO Confronts Terrorism," *per Concordiam*, Volume 4, Number 3, pgs. 24-27, as well as NATO website at http://www.nato.int/cps/en/natolive/topics_68372.htm
2. For more information, including the dates of the courses, please visit http://ccdcoe.org/352.html
3. For a list of the course offerings and dates, please visit http://ccdcoe.org/236.html
4. For more information, please visit http://ccdcoe.org/cycon/2.html

THE COMPLEXITIES OF CENTRAL ASIAN

CYBER SECURITY

Turkmen officials receive laptop computers at a ceremony in Ashgabat in July 2013. Turkmenistan has recently allowed its citizens greater access to the Internet. AFP/ GETTY IMAGES

THE FIGHT AGAINST INTERNET CRIME MUST NOT NEGLECT DEMOCRATIC PRINCIPLES

By Nuria Kutnaeva, independent researcher, Kyrgyz Republic

After obtaining independence in 1991, Kazakhstan, the Kyrgyz Republic, Tajikistan, Turkmenistan and Uzbekistan — all facing completely new challenges and threats to their national securities — each chose different paths for political, social and economic development. Border security, religious extremism, drug trafficking, corruption and political turbulence have been longstanding problems in Central Asian states, but a new challenge surfaced in the last decade: crime involving high-technology and the Internet.

Cyber security is closely connected to the spread of the Internet, which is growing throughout Central Asia, despite varying connection speeds. In terms of Internet speed, Kazakhstan was ranked 58th out of 188 countries in February 2014, Tajikistan was 66th, the Kyrgyz Republic 81st and Uzbekistan 171st,[1] according to Ookla, a company that tests broadband speeds every 30 days. The average download speed in the European Union was rated as much faster.

In 2010, Kazakhstan had the highest rate of infected computers and spam traffic among the five Central Asian states (85 percent).[2] And in 2013, 92 percent of Kazakh organizations experienced at least one cyber attack.[3] This was likely due to the large number of Internet users and Kazakhstan's attractive financial state. Kazakhstan was followed by Uzbekistan with 8 percent and the Kyrgyz Republic with 4 percent of infected computers. Tajikistan (1 percent) and Turkmenistan (2 percent) had the lowest percentage of infected and spammed computers.[4]

CYBER CRIME IN CENTRAL ASIA

Cyber crime falls into three major categories in Central Asia: hooliganism, hacktivism and cyber fraud. Cyber hooliganism implies "muscle-flexing" — done by young, talented hackers[5] who want to prove to colleagues how easily they can disrupt a system. On July 19, 2010, a 14-year-old boy from Russia and his friends hacked into the website of the National Space Agency of Kazakhstan by creating a user account with administrator rights. The boy argued that the developers did not sufficiently protect the portal. "What we did is, of course, illegal," the boy said in justification. "But on the Kazakhstani website, we created a topic where we indicated where its vulnerability is."[6]

Since the Internet is a symbol of globalization, hackers become comfortable operating internationally. The Central Asian states suspect they are victims of foreign hackers because defaced[7] or cracked websites are sometimes left with images of foreign flags and inscriptions. However, the origin is unknown. Cyber security specialist Oleg Demidov of the PIR Center in Moscow points out that hackers from around the world often redirect attacks to hide their identity or to pin the blame on others.[8]

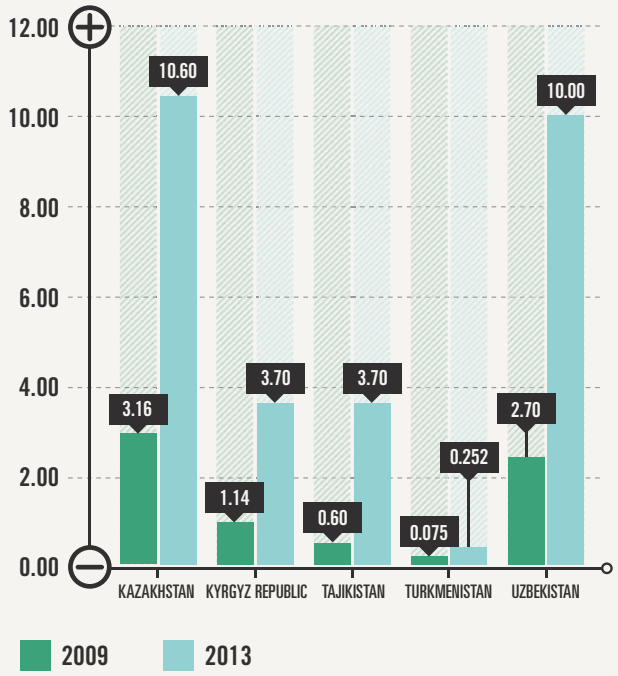
For example, in 2012-2013, several Kyrgyz government sites were vandalized by hackers believed to be from Turkey and Estonia. In 2012, a hacker from Turkey changed the passwords to many Kazakh websites.[9] In 2013, a Malaysian or Indonesian team hacked nine Kazakh legal websites. They left a message calling for the liberation of Palestine.[10]

Competition and revenge are often motivators. For example, in 2011 a Kazakh website selling cars was hit with severe distributed denial-of-service (DDoS) attacks. Owners of the site concluded that revenge was the motive because site administrators had declared war against fraudsters who had tried to sell cheap cars through their site.[11]

Hacktivism, the act of hacking or breaking into a computer system for political or social reasons, occurs frequently in Central Asia. As Ty McCormick, editor at *Foreign Policy* magazine, puts it: "If there's one thing that unites hacktivists across multiple generations, its dedication to the idea that information on the Internet should be free — a first principle that has not infrequently put them at odds with corporations and governments the world over."[12]

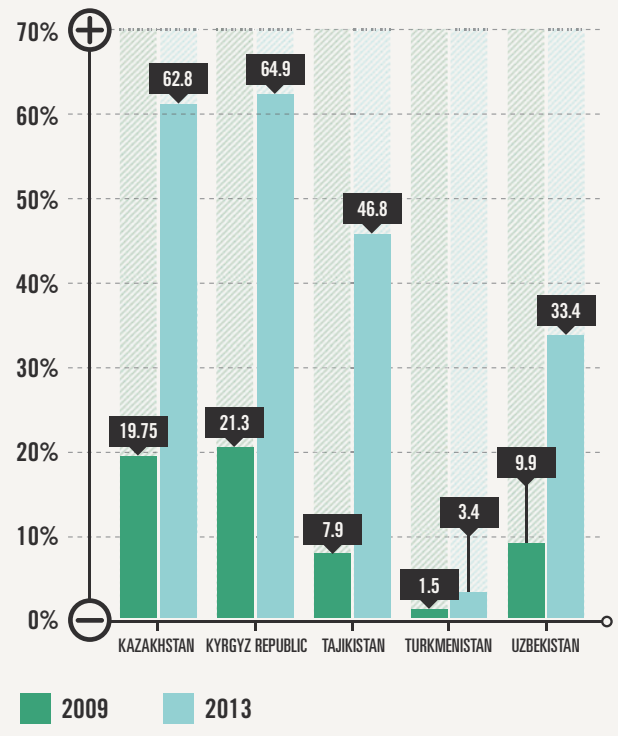
Hacktivists in Central Asia are frequently individuals or groups of information technology (IT) specialists whose main motivation is political: They want to bring an issue to the attention of their government. An Uzbek case is illustrative. In early 2013, there were two defacing attacks on the official website of the national television and radio broadcasting company of Uzbekistan, MTRK. Uzbek hackers, calling themselves

GRAPH 1. ***Number of Internet users (in millions)***



Sources: Profit.kz, ZAKON.kz, *Vecherniy Bishkek*, Internet World Stats

GRAPH 2. ***Proportion of Internet users to a country's population (percentage)***



Sources: *Demoscope Weekly*, Kaspersky Lab

PER CONCORDIAM ILLUSTRATION

"Clone-Security," made the following public statement: "This is a political action, called 'Anti-lying' ['Antilagman']. This company disseminates false information to the people. The people are not satisfied with the transmissions of the national television and radio broadcasting company. For example, the events associated with the closure of the [cellular company] MTS are not covered by MTRK. At one point, millions of people were left without communications. But no information was available. Website Olam.uz constantly talked about MTS, but stopped today. The events on the Kyrgyz-Uzbek border and the tragedy in Sokh happened — and no information from MTRK. And even non-governmental channels are under strict control."[13]

The same hacking team was responsible for defacing the Ministry of Healthcare's website in 2012; they disagreed with the government's policy on forced sterilization of women. The defaced website had an inscription: "Stop sterilizing our moms. Clone-Security."[14]

This group also has foreign policy ambitions. In February 2013, it launched attacks against Kyrgyz government and public websites. Cyber criminals left the inscription: "Clone Security: We are against racism," with the Uzbekistan flag in the background. Human rights violations against ethnic Uzbeks in the Kyrgyz Republic served as the impetus for the attack.[15]

Cyber fraud is cyber crime committed in the financial sphere. For example, in 2009, a 20-year-old Kazakh IT specialist hacked into the computer system of a Kazakh bank and transferred $1 million to his bank account. He fled to Moscow, where Russian police arrested him after he attempted to withdraw the money.[16]

Governmental institutions are not exempt from fraudsters, nor are non-financial businesses. In a case of cyber extortion, on March 9, 2012, the owner of a Kyrgyz entertainment website suffered several days of DDoS attacks. A hacker sent a blackmail message warning that the attacks would continue if the owner didn't pay.[17] In Tajikistan in December 2013, the court convicted three cyber criminals who converted international calls into internal calls and stole the rate difference.[18]

SILENCING OPPOSITION

Sometimes Central Asian governments block access to pro-opposition websites by organizing DDoS attacks against them, producing a considerable challenge to Central Asian societies. Most revealingly, in February 2005 two major Internet providers in the Kyrgyz Republic found themselves under DDoS attack. The Kyrgyz government blocked sites that presented an alternative to government versions of current politics. A site specializing in Central Asian issues, periodically under DDoS attacks, received a letter demanding they stop reporting on the situation in the Kyrgyz Republic.

The first Kyrgyz revolution happened on March 24, 2005. Two weeks later, the site administration received an

email from a Ukrainian confessing to organizing the DDoS attacks. He explained his motives this way:

In early February 2005, a man identifying himself as a Kyrgyz patriot contacted the Ukrainians, saying that parliamentary elections were upcoming and that several websites were writing about the authorities' malevolence and slandering the president and his family. He asked the Ukrainians if they could block selected websites during the elections. "Now we see what happened in Kyrgyzstan — the madness of the crowd, looting, bloodshed. ... We think that it is also a consequence of the fact that people did not have access to truthful information. We consider ourselves responsible for those riots that took place in Kyrgyzstan," the hacker admitted. "We have only now realized the full impact of our actions in suppressing information. We are ready to come to Bishkek, speak at a press conference, tell everything we know and return the money to the Kyrgyz people."[19]

Kazakhtelecom, Kazakhstan's biggest telecommunications provider, controls about 70 percent of the country's broadcast market. In 2010, Radio Free Europe/Radio Liberty reported that some Kazakh nongovernmental organization websites were blocked.[20] As of January 2014, several pro-opposition websites were still denied in Kazakhstan. Authorities used the same method to block the website of the portal "Republic" (http://www.respublika-kz.info/).[21] In February 2009, opposition-minded websites such as zona.kz, geo.kz, and respublika.kz suffered massive DDoS-attacks. Kazakh government officials called on Google to withdraw some of the Internet content from their search results. In 2012, there were four requests to delete 40 items, and 75 percent of these requests were fulfilled.[22] In the first half of 2013, there were three requests to delete 209 items from the Internet, and Google fulfilled 67 percent of these requests.[23]

Likewise, in Tajikistan in 2012, 30 websites known to post material critical of the current authorities of Tajikistan were blocked. A number of Russian news sites could not be accessed as well.[24] On the eve of presidential elections in November 2013, Tajik authorities blocked the site of the Tajik news agency Ozodagon, its Russian version on catoday.org, and the video-hosting site YouTube.[25]

Uzbekistan and Turkmenistan possess the most restrictive policies on public access to the Internet. According to OpenNet, a multinational project that monitors and reports on Internet filtering and surveillance, both states hold the highest level of Internet censorship.[26] Blocking and dropping connection speeds for certain sites — the reason behind low Internet speeds in Uzbekistan — are common practices that the Uzbek government uses to target the opposition. Authorities ordered Internet service providers to block several hundred websites in Uzbekistan.[27] In Turkmenistan, the situation is even worse; there is only one Internet service provider, TurkmenTelekom.[28] In Ashgabat, the capital of Turkmenistan, fewer than 10 Internet cafes operate. Users are required to show passports, and identifying information is recorded by Internet cafe administrators.[29]

GOVERNMENT AGENCIES CONFRONT CYBER CHALLENGES

Special units inside ministries of internal affairs pay close attention to cyber crimes. For example, the "K" Department established in the Ministry of Internal Affairs of Kazakhstan in April 2003[30] contends with a wide range of crimes connected with computer and Internet technology, including cyber bullying, counterfeit DVDs,[31] spread of information promoting extremism, terrorism, cruelty and violence, and child pornography. In 2006, Kazakh authorities established the

REUTERS

REUTERS

1. A Kyrgyz woman in traditional dress speaks on a mobile phone. The people of Central Asian countries are rapidly embracing new communications technologies, necessitating a greater emphasis on cyber security.

2. Turkmen troops guard an Internet cafe in Ashgabat. Internet use in Turkmenistan is highly controlled, and all online activity is recorded by Internet cafe administrators.

AGENCE FRANCE-PRESSE

Children use computers in Ashgabat, capital of Turkmenistan. President Gurbanguly Berdymukhamedov has broadened the country's use of the Internet since his inauguration in 2007.

National Contact Point to fight IT crime and to exchange information with the Commonwealth of Independent States and foreign partners.[32]

In the Kyrgyz Republic, a group focusing on cyber threats was established inside the Ninth Main Directorate of the Ministry of Internal Affairs in 2009. Its main objective is to search for the online presence of extremist organizations, such as Hisb-ut-Tahrir.[33] In Tajikistan, cyber criminals were recently caught by the Directorate for Combating Organized Crime.[34]

Other governmental entities specializing in communications and technologies are also responsible for meeting cyber threats. This is the case in Uzbekistan, where the Computer Emergency Response Team (UZ-CERT) was started in 2005. And in September 2013, the Information Security Center was launched within the State Committee of Communication, Information System Development and Telecommunication Technologies.[35] In Tajikistan, the government communications service is very powerful and reportedly blocked dozens of sites in 2012 and 2013.

RESPONDING TO CYBER THREATS

Realizing that defending against cyber threats demands cooperation with other international stakeholders, regional leaders have raised issues of information security within the framework of regional organizations. At the summit of the Shanghai Cooperation Organization (SCO) in 2006, heads of member states signed the Declaration on International Information Security. In 2009, participants in the SCO summit in Yekaterinburg, Russia, adopted the Yekaterinburg Declaration, which underscores the urgent need to respond to cyber threats. In the SCO, information security was deemed as important as national sovereignty, national security, and social and economic stability.

At the latest SCO summit, in Bishkek in 2013, Kazakh President Nursultan Nazarbayev stated that his country supported the improvement of activities within the SCO Regional Anti-Terrorist Structure (RATS). We "welcome the first meeting of experts on cyberterrorism held in June of this year in Tashkent."[36] To counter information threats, it was decided to establish from SCO member states an expert group on international information security.[37]

In 2010, the Collective Security Treaty Organization (CSTO) adopted the Regulation on Cooperation in the Field of Information Security. The purpose is to create an institutional and legal framework for cooperation among the members of the organization. CSTO performs a range of operations called "Countering Criminals in Information." Its main objective is to combat cyber crime in member states and to counteract prohibited information on the Internet relating to extremism, terrorism and information that can cause political damage to states' interests. For example, during operations in 2009-2010, more than 2,000 websites were identified as inciting ethnic and religious hatred, and more than 600 sites were suspended.[38] During the latest operation, conducted in 2013 in the southern Kyrgyz Republic, about a dozen sites were accused of recruiting terrorists and inciting interethnic dissention.[39]

In September 2011, SCO states that included Russia, China, Tajikistan and Uzbekistan submitted a draft resolution to the United Nations General Assembly on information security.[40] The International Code of Conduct for Information Security proposed the regulation of state actions in cyberspace. Rules also called for UN member states to cooperate in combating criminal, terrorist, and extremist activities with the use of information resources, as well as any activity that "undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[41]

The rules specify that it is unacceptable to use information and communication technologies in a manner contrary to international security. The document sends three interesting messages. First, it declares that a threat with an unknown origin needs to be addressed. This threat may come from nonstate actors or other states. In fact, the rules identify "three evils": terrorism, secession and extremism, in line with the ability of other countries via information technologies "to carry out

hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies."[42] Second, the document confirms the right of every state to control and monitor Internet technologies on their territories: "to reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage."[43] Third, it stipulates that cooperation between state and private companies is essential to combat cyber threats.

CONCLUSION

In the past decade, aside from economic, social and political challenges, Central Asian states had to contend with a threat no one expected back in 1991. Internet use has grown so fast in recent years that government authorities could not accommodate their responses to it adequately. Therefore, they reached for solutions based on familiar practices in the political and social spheres — by blocking Internet providers, obstructing Websites and tampering with Internet connection speeds.

At the moment — luckily enough — Central Asian states are confronted with threats only from the lowest levels of cyber crime — hooliganism, hacktivism and cyber fraud. However, in such a turbulent region, threats of cyber terrorism and cyber warfare should not be underestimated. Therefore, Central Asian governments must take active steps to protect their own critical information infrastructure.

Finally, declaratory statements and intentions to cooperate in cyberspace are made within the framework of Central Asian regional organizations. Identifying sites with extremist and terrorist content in each other's national domains is a great idea. However, it is a big question whether or not more in-depth cooperation is possible. It requires trust, and there should be a joint understanding of information security concepts. Hopefully, over time, understanding will grow on this issue and Central Asian states will move in a good democratic direction. □

1. No figures are given for Turkmenistan. Household Download Index, Ookla Net Index, January 15, 2014, http://www.netindex.com/download/allcountries/
2. Ekaterina Isakova, Hackers choose Kazakhstan, Kursiv.kz, October 21, 2010, http://www.kursiv.kz/news/details/hitech-weekly/xakery-vybirayut-kazaxstan/
3. Kazakhstan IT-specialists underestimate the seriousness of cyber threats. October 28, 2013. Profit.kz <http://profit.kz/news/10147/Kazahstanskie-IT-specialisti-nedoocenivaut-sereznost-kiberugroz/>
4. Ekaterina Isakova. Hackers choose Kazakhstan, Kursiv.kz, October 21, 2010, http://www.kursiv.kz/news/details/hitech-weekly/xakery-vybirayut-kazaxstan/
5. For the purposes of this article, we understand the general term "hacking" to be all illegal actions of access and intrusion to information resources without consent of their owners or administrators.
6. Kazakhstan: The hacker who cracked the site of Kazkosmos turned out to be a Russian schoolboy. March 15, 2012, International News Agency Fergana. http://www.ferganannews.com/news.php?id=18339
7. "Defacing" is changing the main page of the website without changing system files.
8. A personal correspondence between Oleg Demidov and the author. January 17, 2014.
9. Kazakh sites are attacked by Turkish hackers. May 16, 2012, Express-K, http://profit.kz/news/8526/Kazahstanskie-sajti-podvergautsya-atake-tureckih-hakerov/
10. Kazakh sites hacked from Southeast Asia, December 4, 2013, Profit.kz. http://profit.kz/news/11236/Kazahstanskie-sajti-vzlomani-hakerami-iz-Ugo-Vostochnoj-Azii/
11. Governmental sites of Kazakhstan are poorly protected from DDoS-attacks. December 4, 2012, Total.kz. http://profit.kz/news/9236/Gossajti-RK-slabo-zaschischeni-ot-DDoS-atak/
12. Ty McCormick. Hacktivism. *Foreign Policy*. May/June 2013, Issue 200, p. 24-25.
13. In Uzbekistan, the site MTRK was hacked. Ozodlik, 30 January 2013. http://www.ozodlik.org/content/article/24888716.html
14. Ibid.
15. Askat Turusbekov. Sites of Kyrgyz security agencies were hacked. Kabar, February 21, 2013. http://kabar.kg/incident/full/50072
16. Darura Zhalyn, A Hole in the Bank, *Businessweek*, June 12, 2009, http://profit.kz/articles/908/Dirka-v-banke/
17. Hacker attacks on websites of government agencies and the media in the Kyrgyz Republic (history). Tazabek, May 5, 2013 http://www.w.tazabek.kg/news:350162/
18. Tajikistan, for the first time, condemned the group of "hackers." Top News, December 28, 2013. http://www.topnews.tj/2013/12/28/v-tadzhikistane-vpervyie-osudili-gruppu-hakerov/
19. "Kyrgyz" hackers ready to arrive in Bishkek, require security guarantees - letter Central Asia. January 4, 2005. http://www.centrasia.ru/newsA.php?st=1112320800
20. NGO Says 14 Websites Being Blocked In Kazakhstan. Radio Free Europe/Radio Liberty. January 27, 2010, http://www.rferl.org/content/NGO_Says_14_Websites_Being_Blocked_In_Kazakhstan/1941642.html
21. Zarina Kozybayeva. What is lacking in the Internet in CA . May 7, 2010. Deutsche Welle. http://dw.de/p/NEDQ.
22. Google Report on the availability of services and data. January-June 2012 http://www.google.com/transparencyreport/removals/government/countries/?p=2012-06; July-December 2012. http://www.google.com/transparencyreport/removals/government/countries/?p=2012-12
23. Google Report on the availability of services and data. January-June 2013, http://www.google.com/transparencyreport/removals/government/countries/
24. Galim Faskhutdinov. Internet in Tajikistan is not developed, but the authorities are afraid of it. Deutsche Welle. December 5, 2012, http://dw.de/p/16vc8
25. Mehrangez Tursunzoda. In Tajikistan, the sites Ozodagon and YouTube are blocked. «ASIA-Plus». November 5, 2013. http://news.tj/ru/news/v-tadzhikistane-zablokirovali-saity-ozodagon-i-youtube
26. OpenNet Initiative. Country profiles: Uzbekistan, Turkmenistan. https://opennet.net/research/profiles
27. Uzbekistan: unlock some independent sites. Internet censorship has malfunctioned again? October 27, 2013. http://www.ferganannews.com/news/21412
28. Neither Here Nor There: Turkmenistan's Digital Doldrums. OpenNet Initiative. https://opennet.net/neither-here-nor-there-turkmenistan percentE2 percent80 percent99s-digital-doldrums
29. Personal interview with an Ashgabat inhabitant (on a confidential basis). January 11, 2014.
30. Oksana Koksegenova, Hackers threaten Kazakhstan, April 5, 2007, Kursiv.
31. Polina Krestovskaya. Watch out. Everything is recorded. Almanews.kz. April 27, 2009, http://profit.kz/articles/837/Akkuratno-Vse-zapisivaetsya/
32. Oksana Koksegenova, Hackers threaten Kazakhstan, April 5, 2007, Kursiv.
33. Jyldyzbek Ibraliev. Kyrgyz law enforcement agencies established a unit to fight cyber crime. January 12, 2009. Information Agency «24.kg», http://www.24.kg/community/2009/01/12/102859.html
34. In Tajikistan, for the first time condemned the group of "hackers." Top News, December 28, 2013. http://www.topnews.tj/2013/12/28/v-tadzhikistane-vpervyie-osudili-gruppu-hakerov/
35. The problems of information security are discussed. State Committee for Communications, Information and Telecommunication Technologies of the Republic of Uzbekistan. October 31, 2013, http://ccitt.uz/ru/press/aci_news/2013/10/932/. See also Resolution of the Cabinet of Ministers of September 16, 2013, No. 250, "On measures of organization the Center for Development of the 'E-government' and the Center for Information Security under the State Committee for Communication, Information and Communication Technologies of the Republic of Uzbekistan." http://www.pravo.uz/resources/anons/monitoring/files/pos_250.pdf
36. Kazakhstan supports the expansion of the functions of the Executive Committee of the SCO RATS by cyber terrorism and cyber crime – President. KAZINFORM. September 13, 2013. http://www.inform.kz/rus/article/2589151
37. CO RATS Council decides to establish a group to combat terrorism on the Internet. Novosti-Kazakhstan. September 20, 2013. http://newskaz.ru/politics/20130920/5567047.html
38. More than 2,000 extremist websites were detected in Russia for two years – Bordyuzha, RIA Novosti. December 21, 2010, http://ria.ru/defense_safety/20101221/311598350.html # ixzz2qugWwWn1
39. CSTO found in the southern Kyrgyz Republic sites to recruit terrorists. Rosbalt, March 28, 2013, http://www.rosbalt.ru/exussr/2013/03/28/1111069.html
40. Letter dated September 12, 2011, from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the secretary-general. 66th session, Item 93 of the provisional agenda, Developments in the field of information and telecommunications in the context of international security A/66/359, September 14, 2011, Developments in the field of information and telecommunications in the context of international security, http://daccess-ods.un.org/TMP/9878256.91699982.html
41. Ibid.
42. Ibid.
43. Ibid.

COMBINED ENDEAVOR

U.S. EUCOM C4/CYBER EXERCISE ENHANCES INTEROPERABILITY

By Robert L. Watson
Chief of the Combined Interoperability Branch, U.S. European Command

Photos by EUCOM

IN 2014, the United States European Command (EUCOM) celebrates the 20-year anniversary of Combined Endeavor, the premier interoperability and cyber defense exercise between NATO and Partnership for Peace (PfP) nations. In September 2013, more than 1,200 people from 40 nations and transnational organizations gathered in Grafenwöhr, Germany, to test their interoperability and cyber defense skills in a collaborative environment.

During the past two decades, this exercise has become the bellwether of interoperability training for NATO and PfP nations and now has become so for cyber security as well. It began with 10 countries seeking to achieve multiple layers of interoperability at the technical and systems level and,

Participants from 40 nations take part in Combined Endeavor 2013 in Grafenwöhr, Germany.

even more importantly, at the human level. The U.S. Department of Defense defines interoperability as "the ability of systems, units, or forces to provide data, information, material and services to and accept the same from other systems, units, or forces, and to use the data, information, material, and services exchanged to enable them to operate effectively together."[1] Combined Endeavor began with this premise.

The exercise has changed so much during the past 20 years it is barely recognizable. The learning experience leverages the collective knowledge available only in an environment of this sort. The Cyber Operations Center and Cyber Defense Seminars by leading industry experts, not to mention a Combined Joint Command and Control Center, are some of the highlights of this unique exercise. At Combined Endeavor 2013, an exercise network similar to that of the International Security Assistance Force (ISAF) in Afghanistan was built within two weeks. Although the interoperability and cyber security skills experienced in this exercise cannot be replicated, other major U.S. commands have used Combined Endeavor as a model to build similar exercises with different partners.

Sustaining the interoperability and cyber defense gains from the past 20 years will not be easy, given the challenge of austerity in manpower and financial resources. Budgets are tight, and 2014 looks to be a difficult year for fiscal stability on the heels of the global financial crisis. In 2013, the U.S. experienced a partial government shutdown and widespread budget cuts. In Europe, crushing debt issues have burdened Greece, Iceland, Ireland, Italy, Portugal and Spain.[2] While opportunities for fruitful collaboration may seem great, opportunities may also be fleeting.

Slovenian soldiers operate information systems during Combined Endeavor in Grafenwöhr, Germany.

TRANS-ATLANTIC AUSTERITY

NATO projects that defense budgetary spending will continue to contract. Most NATO nations will not come close to the Alliance's 2-percent-of-GDP target for defense spending in 2014, nor probably in the near future.[3] Even the U.S. is feeling the pressure. The 2013 Budget Control Act mandates billions of dollars in spending cuts during the next five years and reduces manpower to levels not seen in 20 years. With these budgetary pressures, maintaining interoperability within NATO and with coalition partners will be increasingly difficult.

This is significant because the threats from nontraditional vectors, such as cyber, continue to increase rapidly. Many lessons in interoperability are born of a collective desire to improve the ability to share information seamlessly and transparently. During the past 20 years, there have been remarkable gains in interoperability and partnerships. The ISAF coalition is a shining example of the ability to forge interoperability in spite of austerity.

REFLECTION ON OPPORTUNITIES

Within the context of austerity, it is important to understand the great opportunities that the past two decades have provided from both a European and a trans-Atlantic perspective. U.S. President Bill Clinton's 1994 United Nations address provided foreshadowing: "Our struggle today, in a world more high-tech, more fast-moving, more chaotically diverse than ever, is the age-old fight between hope and fear."[4] In 1994, the peace dividend of the Cold War proved substantive as the U.S and Russia signed the Kremlin accords, effectively ending the intentional aiming of nuclear missiles at each other and providing for the dismantling of the nuclear arsenal in Ukraine.[5] That same year, Finland and Sweden decided to join the European Union, and the Russian Army completed its withdrawal from Estonia and Latvia.[6] Meanwhile, in the Pacific, China connected to the Internet for the first time.[7] Unfortunately, the Balkan wars were still raging following the breakup of Yugoslavia.

In January 1994, NATO launched PfP to aid countries seeking cooperative military and peacekeeping relations with the Alliance. On July 7, 1994, in Warsaw, Poland, President Clinton announced an American commitment to provide assistance to new democratic countries in line with PfP goals. This led to the creation of the Warsaw Initiative Program, managed by the U.S. departments of

State and Defense to improve relations and military interoperability between NATO and countries committed to democratic principles.[8] The Warsaw Initiative Fund paved the way for generations of partnerships by enabling developing countries to participate in opportunities such as Combined Endeavor and a host of other creative and innovative programs to achieve mutual defense goals.

WHAT A DIFFERENCE 20 YEARS CAN MAKE

Twenty years later, it is difficult to remember how much harder it was to share information among coalition members. Radios have been eclipsed by lightning quick, accurate data communications across multiple domains. Combined Endeavor 2013 highlighted several notable firsts in interoperability resulting from many years of effort and risk-taking. For example, the French Army successfully fired artillery using a U.S. fire support system.

This also marked the first year of a persistent and consistent approach to improving collective cyber security capabilities. An entire cyber security cell was established to test the network's strength on multiple fronts. In the 2012 Joint Operational Access Concept, Adm. Michael Mullen, then chairman of the U.S. Joint Chiefs of Staff, described core military competencies necessary for successful operations: "complementary multi-domain power projection" and the "ability to maintain joint assured access to the global commons and cyberspace should they become contested."[9]

Indeed, some European nations, such as Georgia and Estonia, have experienced firsthand aggression in cyberspace. Cyber Endeavor addresses the complexities of the cyber domain and focuses on it, not just in the capstone exercise at Grafenwöhr, but also through successful regional cyber security seminars across Europe. The seminars aim to take advantage of gaps in capabilities and capacities and improve the collective cyber security posture of key partners in Europe.

A COLLABORATIVE APPROACH

Patience and perseverance are required to ensure interoperability gains are not lost. Understandably, no single nation can solve every dilemma and resources are finite, but, opportunities for collaboration must be seized in spite of austerity. U.S. Army Europe's Joint Multinational Readiness Center hosts an exceptional facility at Grafenwöhr that has taken this collaborative approach to high levels in mission rehearsal exercises for European partners. Other notable examples are the Cooperative Cyber Defence Centre of Excellence in Estonia and the Command and Control Centre of Excellence in the Netherlands. NATO and partner nations must continue to take every opportunity to exercise and maintain interoperability. It is critical to capitalize on these efforts, to expand upon the lessons learned and solidify interoperability between partner nations.

ASSURED ACCESS

It is imperative that interoperability provide assured access to information and data. Only through assured access can national leadership attain strategic flexibility. Interoperability solutions must be tested, tailored and scaled to meet operational requirements. More importantly, they must be synchronized across multidomain requirements of command and control, cyber and spectrum. Combined Endeavor provides an excellent venue to test solutions in all these domains. Assured access mandates an ability to provide defense in depth. Mutual trans-Atlantic interests have been firmly cemented in the past 20 years, and Allied cooperation has never been more important. Intersecting national interests create opportunities to strengthen mutual defense goals and objectives, as well as to develop common strategies to achieve goals that might be unattainable unilaterally.

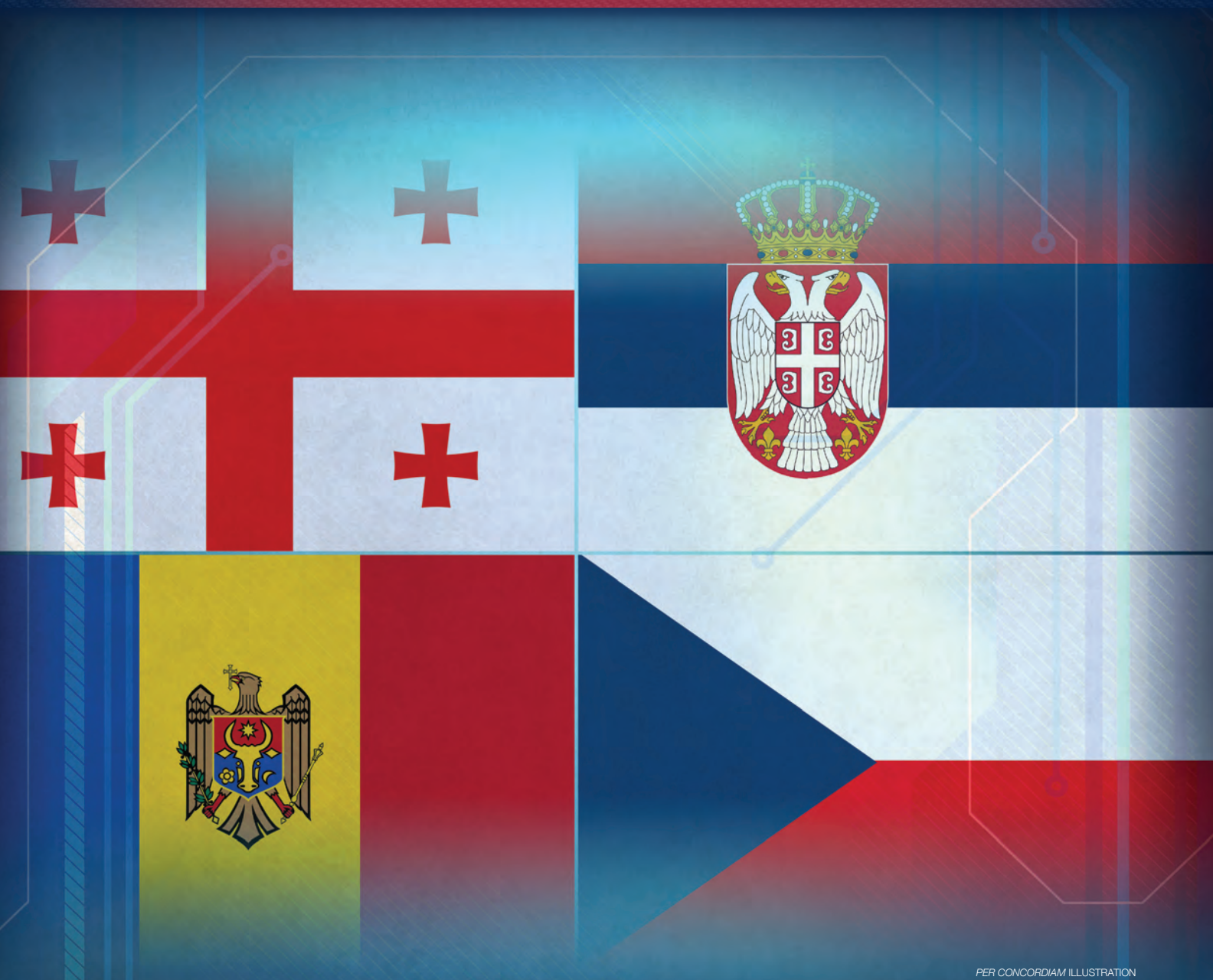
The role of defense in cyber security cannot be overstated. In 2009, Cyber Endeavor was created to build the cyber defense capability of partner nations, and compliment Combined Endeavor. In recent years, the growth of Cyber Endeavor, in concert with Combined Endeavor, has been impressive because almost every Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system has some network capabilities. Cyber Endeavor provides EUCOM and coalition partners an invaluable opportunity to collaborate on cyber defense issues and build cyber defense partnerships with NATO, partner nations, academia and industry. Subsequently, the goal is to strengthen the collective international cyber defense posture and to improve force readiness for deployment with secure C4ISR systems in support of multinational crisis response.

Finally, a collaborative approach to interoperability and cyber security is imperative to address risks and vulnerabilities that will only increase. Over the next year Combined Endeavor will evolve from using a centralized approach to a decentralized approach. Specifically, EUCOM will integrate the Mission Partner Environment and cyber security threads into the Command's Regional Exercise Portfolio. It is therefore imperative that complacency is avoided and interoperability is fostered at every opportunity. Decision-makers and leaders must not allow difficult situations and austerity to drive defense readiness, especially in the communications and cyber domain. □

1. Chairman of the Joint Chiefs of Staff Instruction 6212.01F, March 21, 2012, p. 49, http://jitc.fhu.disa.mil/jitc_dri/pdfs/cjcsi_6212_01f.pdf
2. "The Eurozone in Crisis," Council on Foreign Relations, Cristopher Alessi, April 3, 2013, http://www.cfr.org/world/eurozone-crisis/p22055
3. "NATO and The Challenges of Austerity," F. Stephen Larrabee et al, Rand Corp., 2012, http://www.rand.org/pubs/monographs/MG1196.html#key-findings
4. Address by President Bill Clinton to the 49th UN General Assembly, September 24, 1994, http://www.state.gov/p/io/potusunga/207377.htm
5. "In Disarmament Breakthroughs, Clinton, Yeltsin Sign Nuclear Accords," Terrence Hunt, AP News Archive, January 14, 1994, http://www.apnewsarchive.com/1994/In-Disarmament-Breakthroughs-Clinton-Yeltsin-Sign-Nuclear-Accords/id-c47d24f57ae53350868e17ea094a17e0
6. "Anniversary of the Withdrawal of Russian Troops from Estonia," http://estonia.eu/about-estonia/history/withdrawal-of-russian-troops-from-estonia.html
7. "China Celebrates 10 Years of Being Connected to the Internet," Stephen Lawson, 17 May 2004, http://www.pcworld.idg.com.au/article/128099/china_celebrates_10_years_being_connected_internet/
8. U.S. Assistance to the Partnership for Peace, US GAO, July 2001, Washington, D.C., http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-01-734/pdf/GAOREPORTS-GAO-01-734.pdf
9. Joint Operational Access Concept, DoD, Version 1.0, Washington, D.C. January 17, 2012, http://www.defense.gov/pubs/pdfs/joac_Jan%202012_signed.pdf

REGIONAL CYBER SECURITY

The Cases of Georgia, the Czech Republic, Moldova and Serbia



PER CONCORDIAM ILLUSTRATION

GEORGIA

By POLICE LT. GIORGI TIELIDZE, senior advisor,
State Security and Crisis Management Council,
Ministry of Internal Affairs of Georgia

Georgia learned a hard lesson about the need for a national cyber security strategy in 2008, when massive cyber attacks were carried out against national critical informational infrastructure, including the banking sector. The nature of those attacks approached the level of "cyber war" in the sense that the attacks were well-organized attempts to isolate Georgia globally and occurred just as the Russian Federation was engaged in military hostilities against the country.

As a result, the government of Georgia analyzed the grave consequences of that cyber campaign and declared that protecting cyberspace was just as important as protecting the country's sovereignty and territorial integrity.[1] In drafting its National Cyber Security Strategy, the government of Georgia used a slightly different approach from that of Estonia. Unlike Georgia, Estonia had significant cyber security measures in place when the country's networks were simultaneously attacked in 2007, affecting government agencies, banking, media and telecommunications. In retrospect, Estonia was well-prepared for individual cyber attacks but lacked sufficient capacity to counter large-scale and coordinated cyber attacks.[2]

These examples suggest that cyber security is mainly derived from a risk-based approach to information security issues. Governments should first identify and assess their previous experience with information security incidents, risks and challenges to detect possible cyber gaps and vulnerabilities upon which they can focus their specific strategic security visions.

WHAT IS CYBER STRATEGY?

Cyber security strategy and policy establish basic approaches, guiding principles and leading priorities for a nation. These types of documents are general, and their provisions should be reinforced by the passage of specific legal acts (e.g., laws, bylaws, decrees). Cyber security strategies and policies should be formulated systematically to cover a majority of problems and provide adequate countermeasures necessary for addressing those problems. A systematic approach to cyber security strategies and policies should consist of the following pillars:

a) Identifying and analyzing cyber security needs;
b) Defining the capabilities necessary for elimination of cyber security threats;
c) Researching relevant international best practices;
d) Drafting the strategy itself;
e) Devising an action plan that defines the precise measures necessary for executing strategic goals, their timelines, and the governmental agencies responsible for implementing those measures;
f) Carrying out the required measures in practice;
g) Identifying the systems necessary to monitor the progress achieved within the framework of the strategy/policy.

CAPACITIES TO CONFRONT CYBER THREATS

While defining national cyber security strategy, policy planners must identify the available state resources necessary to counter challenges. This step is a prerequisite to identifying relevant strategic priorities and is a cornerstone for all information security strategies and policies. It is pointless to define security measures that cannot be realized with available resources.

When the government of Georgia began drafting its new cyber security strategy, participants of the National Security Council (NSC) Working Group considered the country's limited cyber capacities and decided on a "minimalistic approach" to cyber security. It should be stressed that before the 2008 attacks, Georgia had no experience in building and maintaining effective information security systems. Thus at the initial stage, it was decided to tackle basic problems such as defining minimum information security standards and specifying critical information infrastructure. Policy planners decided not to impose significant financial costs on the public and private sectors, taking into account the development level of the country.

A cyber security strategy working group under the NSC decided upon a Georgian National Cyber Security Strategy that would address basic strategic cyber priorities within two years (2013-2015). Upon completion of these goals, Georgia will shift its cyber policy from a basic approach to a developing model.

RESEARCHING BEST PRACTICES

Cyber security planners should consider international standards and practices while elaborating on relevant strategies. Guidelines provided by world-renowned IT agencies are sufficient, including Microsoft Guidelines for Developing a National Cyber Security Strategy. It is also imperative to research best practices of foreign states that have already fused cyber recommendations into their relevant security policies. Policy planners should ensure that target countries have similar characteristics to their states. It would be useless to follow the examples of states with absolutely different security landscapes, economies and backgrounds.

Georgia's NSC Working Group chose to follow the Estonian example. Both countries are former Soviet republics, have identified similar security concerns, possess limited resources and share a common legacy of defending against massive, coordinated cyber attacks.[3] The NSC also actively cooperated with foreign stakeholders such as Council of Europe (Cybercrime Convention Committee)[4] and the International Telecommunications Union (ITU),[5] which provided feedback and recommendations.

DRAFTING A STRATEGY

Composing the actual strategy is the most important step because it accumulates the results from all the previous stages. A single governmental agency should coordinate the process of elaborating a cyber security strategy. This agency should identify all relevant public and private stakeholders and ensure their participation. The coordinating state body should also divide tasks among other governmental agencies competent in cyber security. Initially, the lead agency should draft a general framework of the strategy and share it with relevant agencies for comment and suggestion. The private sector must be engaged along with the public sector since it, too, owns or operates much of the critical informational infrastructure.[6]

In Georgia, the lead cyber security policy body was the NSC. It coordinated tasks among relevant public institutions (including the Data Exchange Agency, the Ministry of Internal Affairs and the Ministry of Defense) and submitted its draft policy framework to those agencies. Written comments and hearings followed. Furthermore, the NSC Working group actively involved private stakeholders (such as Internet service providers, banking representatives and mobile phone companies). At first, the government of Georgia and ISPs needed to agree on methods of handling cyber incidents consistent with international standards for public-private cooperation. Private stakeholders argued that deep and comprehensive obligatory cooperation would have imposed unjustifiable costs on them and consequently would have hampered cyber-related business development in Georgia. The government concurred, at least temporarily, and agreed to conclude a memorandum of understanding between ISPs and law enforcement agencies that establishes basic principles on cooperation in a manner that wouldn't harm Internet business development in Georgia.[7] Moreover, the NSC held several meetings with civil society representatives to reflect appropriate private interests from human rights perspectives.[8]

ELABORATION OF AN ACTION PLAN

A cyber security strategy without an adequate action plan (AP) cannot be realized. An AP defines precise time frames for achieving priorities and specifies responsible bodies for implementing cyber security measures within those periods.

Policy planners need to assess the operational capacities of the state bodies tasked with carrying out required cyber security measures. Strategists, particularly in developing countries, should not focus on the official functions of public agencies, but rather on the actual assets possessed by them. Those assets include modern technology, qualified staffers and a rich institutional memory.

Furthermore, an AP should establish clear performance indicators, both quantitative and qualitative, to assess when strategic priorities are met. Quite often, APs contain complex activities that necessitate a more detailed approach. In such a case, it's better to write additional ad hoc action plans to avoid overloading the cyber security strategy.

While drafting the Georgian Cyber Security Strategy, the NSC Working Group carefully evaluated the institutional capacities of all governmental stakeholders.[9] It decided that a majority of the AP strategic priorities would be carried out by the Ministry of Internal Affairs of Georgia and the Ministry of Justice Data Exchange Agency, taking into account their relatively advanced experience in informational security.[10]

CARRYING OUT REQUIRED MEASURES

Upon approval of the strategy, implementation begins. Countries in transition should start by adopting a relevant legal framework, which constitutes the foundation for further activities. As soon as laws are passed, institutional changes occur in relevant public agencies, which mean establishing or reorganizing cyber units to correspond to the requirements of the strategy. Along with legal and institutional development, capacity building of relevant cyber security bodies must continue. Improving technology and training is critical to realize strategic priorities.

After the Georgian Cyber Security Strategy was approved by presidential ordinance in May 2013, relevant legislative and institutional changes followed. In November 2013, a list of critical informational infrastructure was designated, for which the state would provide special protection. Furthermore, minimal security standards for critical informational infrastructure were amended as prescribed by the strategy. Moreover, Georgia engaged international partners to help develop cyber capacities operationally.

EFFECTIVE MONITORING

Policy planners should create an effective system for monitoring the progress prescribed by a cyber security strategy, both at the midway point and toward the end. Early monitoring is critical to fulfill cyber security policy requirements since it works as an alarm in case ongoing processes are not working as planned.

More precisely, national security policy bodies should have the capacity to control how relevant stakeholders are performing their duties, offering necessary instructions in case certain agencies fail to meet obligations. Monitors need an operational evaluation system to provide regular status reports on measures and actions.[11]

Georgia pursued such monitoring. All responsible agencies are obliged to report to the NSC Working Group about the latest cyber developments. Based on this information, the NSC provides instructions and schedules for carrying out other activities.

CONCLUSION

Development of effective cyber security strategies and policies is based on a well-organized elaboration process that should include all the above mentioned stages. All relevant public and private stakeholders should be involved in this process. Cyber security directly affects their legitimate interests as well.

Furthermore, policy planners need to heed international best practices to see if they correspond to the needs of their own country. While establishing the relevance of a foreign state's experience, the following criteria can be used: common legacy, similar economic situation and shared perception of national security threats. At the same time, policy planners should calculate the expense of such strategies to avoid unjustifiable costs to public and private entities.

Finally, the effectiveness of a cyber security strategy depends on its implementation. Implementation should be centrally coordinated and monitored by the highest security policy agency.

CYBER SECURITY STRATEGY AND POLICY ESTABLISH BASIC APPROACHES, GUIDING PRINCIPLES AND LEADING PRIORITIES FOR A NATION.

1. Cyber Security Strategy of Georgia for 2013-2015, p. 2 (available in Georgian only) accessed on January 17, 2014: http://www.nsc.gov.ge/files/files/legislations/kanonqvem-debare%20normatiuli%20aqtebi/cyber%20security%2017%20may.pdf
2. Cyber Security Strategy of Estonia, p. 6, accessed on January 19, 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf
3. e.g Georgian and Estonian National Security Strategies and Cyber Security Strategies.
4. Regional Seminar on Strategic Cybercrime Priorities, Council of Europe Cybercrime Convention Committee; accessed on January 17, 2014: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_Project_EaP/2523_Strategic%20Priorities_Tbilisi_V4_19june12FIN.pdf
5. ITU Cybersecurity Mission to Georgia, p. 14-16, International Telecommunication Union; accessed on January 17, 2014: http://www.itu.int/ITU-D/cyb/app/docs/Salta_101101/Session4/Probert_Presentation.pdf
6. Developing a National Strategy for Cybersecurity, p.17 Microsoft Corporation, accessed on January 17, 2014: http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf
7. Codexter Cyber Terrorism Country Profile – Georgia, p. 5; accessed on January 17, 2014: http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Georgia.pdf
8. Office of NSC Presents Draft Cyber Security Strategy for Public; Official Webpage of the National Security Council of Georgia, accessed on January 17, 2014: http://www.nsc.gov.ge/eng/news.php?id=6170
9. ENISA National Security Strategies – Practical Guide on Development and Execution, p. 31; accessed on January 17, 2014: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide
10. See Action Plan of the Cyber Security Strategy of Georgia.
11. Supra, ENISA National Security Strategies p.18.

CZECH REPUBLIC

By DANIEL BAGGE
National Cyber Security Center, Czech Republic

Ensuring the cyber security of a state is one of the key challenges of our times. The absence of geographic and physical limitations in cyberspace is the driving force behind the need for a new approach toward security. Although the cyber domain complements other domains, such as air, sea, land and space, it is also a domain in itself. Within this new domain, we cannot rely on capacities designed for better-known domains. The omnipresence of cyber threats requires intense international cooperation based on the composition of current international bodies. Nations must adopt new approaches, forge new partnerships and broaden cooperation among institutions. We must dispose of the security toolbox we used in the past: Bullets and guns are useless in the face of a cyber threat.

To forge new partnerships internationally, share capabilities and enhance security cooperation, an entirely new and comprehensive approach toward cyber security must be adopted at the national level. Only through a well-designed and whole-of-government approach can a viable model be built to promote cyber security and enhance national security. The main task for every state is to create a cyber security environment based on technical and theoretical capabilities, a legal framework and interagency cooperation.

This article presents the steps taken by the Czech government and security entities to advance cyber security nationally, regionally and internationally. The Czech Republic, as a medium-size Central European country, has an obligation to protect its citizens and secure cyberspace to allow the free exchange of information and undisrupted flow of information and commerce. The state must also protect critical infrastructure vital not only to itself, but to its neighbors, for example, in the energy sector. Also, as a member of the European Union and NATO, we have obligations to our allies and partners to enhance cyber security internationally.

NATIONAL CYBER SECURITY CENTRE

Cyber security is part of the Czech Republic's security environment. Cyber attacks are becoming more sophisticated, dynamic and complex. No longer is the Internet used merely by criminals for their direct economic benefit. The sphere of attacks has widened to include industrial espionage, cyber terrorism and vandalism and probing critical infrastructure. Attackers concentrate increasingly on elements of critical infrastructure, such as power plants, pipelines, intellectual property and health care information systems.

Aware of the growing scale of cyber threats to national security, the Czech government announced the creation of the National Cyber Security Centre (NCSC) within the National Security Authority on October 19, 2011.

The NCSC establishes the foundation for a coordinated whole-of-government approach and aims to bring all cyber security-related policies under one roof. It is responsible for national security in the cyber domain, critical infrastructure protection, legislative measures concerning cyber security, international cooperation, a Computer Emergency Response Team (CERT) and setting standards. The NCSC is not a law enforcement agency, so cyber crime is not the primary agenda; however, cooperation with law enforcement and the intelligence community is one of its roles.

LEGAL FRAMEWORK

Ensuring that the entire cyber domain follows the technical guidance of the NCSC required new legislation. The first step is defining critical infrastructure. It includes not only government networks, but private telecommunication networks and information systems and the industrial control systems of dams, power plants and other vital industrial and economically important sectors.

Efforts to adopt a legislative act were framed by consultations with an interagency working group consisting of representatives from the Ministry of Interior, Ministry of Defense, the Czech Telecommunications Office, the General Directorate of the Fire Rescue Service and intelligence services. The law sets out certain obligations, depending on whether the subject is critical or important, and gives the NCSC authority to inspect whether obligations are fulfilled.

NATIONAL COOPERATION

The second platform vital for a viable cyber security strategy is national cooperation, and is sometimes referred to as interagency cooperation. In fact, these two terms are not exact. The first refers to a mindset and an NCSC-centric approach. The governing body sets standards and campaigns for cooperation from entities involved in cyber security. Interagency cooperation is more horizontal, as other agencies and entities complement one another's efforts.

For example, national cooperation could mean a government agency follows NCSC guidelines, but interagency cooperation could mean the NCSC provides the agency with valuable intelligence about attempted cyber intrusions.

INTERNATIONAL COOPERATION

Cyberspace has no geographical borders or limitations. That fact increases the importance of international cooperation. The chronic lack of attribution in the cyber domain calls for strong cooperation among allies and the creation of new partnerships. Cyber is not just a domain that expands the existing area of potential conflict and allows hacktivists, organized crime and terrorist networks to thrive. Cyber is not just a digital highway used for attacks. It also is a means for criminals to launder money and exchange tactics. Also, the computerized interdependency between industry and consumers constitutes the battlefield of industrial and political espionage against the interests of your country.

CYBER SECURITY IS PART OF THE CZECH REPUBLIC'S SECURITY ENVIRONMENT.

All these threats cannot be handled by only one security entity. The very foundations of the cyber realm call for enhancing bilateral and multilateral cooperation at the agency, national and international level. Cooperation does not mean only the exchange of technical expertise but also shaping policies, creating awareness and coordinating efforts. Training programs and exchange of best practices among policy makers, politicians and government officers are essential for mutual understanding. Without agreement on basic terms and definitions, it is impossible to seek common goals.

Once international cooperation is established with neighboring countries and international partners, the security entity must not falsely assume its job is complete. Simulations and exercises among technical and decision-making bodies should be routine, and policies should be updated by the exchange of expertise and training methods.

One often overlooked way of improving cyber security is promoting "digital hygiene": educational campaigns to inform the public about threats and best practices in cyberspace. Breaches in security often begin between the keyboard and the chair. These campaigns can also be developed in collaboration with international partners, such as the European Union Agency for Network and Information Security or the Organization for Security and Co-operation in Europe.

SIX PRIORITIES

The Czech NCSC has established six cyber security priorities. They start with legislation to create a legal framework that defines the competence of public authorities and the rights and obligations of operators in the cyber security field.

International cooperation and communication is the second priority. Preparedness exercises and simulations should be organized nationally and internationally with multinational partners. Some of these events should include private-sector actors endangered by cyber threats.

A third priority is national cooperation: Large-scale interagency cooperation, as well as cooperation between public and private sectors, is vital. At the same time, cooperation with academia and outside experts should be established to develop cyber security capabilities.

Mapping out the risk to critical information infrastructure represents the fourth priority. Mapping helps raise awareness about the growing number of systems that can become cyber targets. An analysis evaluates the importance and significance of such systems, as well as their role within the functioning of the state. Risk assessment then helps minimize damage after a potential incident and set up key systems' protection for maintaining cyber security.

A fifth priority is building a specialized workplace for NCSC/CERT. NCSC is supposed to build and maintain a mutual early warning system, as well as connect this system into already existing international early warning systems for cyber threats. The CERT is tasked with monitoring cyberspace and detecting attacks. Such a workplace is highly skilled and fully integrated with similar institutions outside the Czech Republic.

A final priority is raising cyber security awareness, not just among leaders and specialists, but also the public at large.

CONCLUSION

The Czech Republic recognizes the complexity of cyber threats and is adopting measures to ensure cyber security in three layers — critical infrastructure, governmental networks and public computers. To reach all three layers, a whole-of-government approach is necessary, combined with cooperation from the private sector and the public.

Isolated efforts that fail to achieve all of the six priorities won't accomplish the strategic goal of securing cyberspace. Only combined and coordinated efforts will create a comprehensive cyber security framework that protects the Czech Republic and its international partners.

MOLDOVA

By **NATALIA SPINU**
Head of the Cyber Security Center
CERT-GOV-MD, Republic of Moldova

Today, cyber security is one of the world's most widely discussed topics, capturing the attention of national leaders at the majority of international security events. Consisting of a multitude of actions and controls, cyber security is seen as the guarantee of national, economic and even personal security. The Internet and information technology are transforming the global economy and creating new opportunities for society and government. Moldova's citizens, businesses and government are readily embracing the many advantages that these technologies offer.

The IT business revolution has resulted in traditional services increasingly becoming available online. In the name of convenience, everyday activities such as banking, shopping and accessing government services are taking place online. In keeping with this trend, Moldova's government and private sector are using the Internet and other digital technology to facilitate interaction with citizens.

Almost half of Moldovans are already online (38 percent have broadband access), and they expect online public services to be accessible 24 hours a day, seven days week, through their computers or mobile phones. But the increased use of the Internet and other digital technology increases our vulnerability to cyber threats. Criminals are using cyberspace to gain access to personal information, steal intellectual property from businesses and gain knowledge of sensitive government-held information for financial or political gain, or other malicious purposes. In the cyber world, national borders present no barrier.

As an example of how cyber security is being acknowledged and developed in a state, I would like to present the example of the Republic of Moldova, a onetime republic of the former Soviet Union. Moldova is deeply involved in various national and international projects and initiatives to create a safe and secure system for all. Since cyber security is borderless, it can be achieved only through cooperation and collaboration among states.

CYBER SECURITY HAS NO BORDERS

A successful targeted cyber attack could disrupt a state's critical services, harm the economy and potentially threaten national security. Moldova is not immune from such attacks. For example, in the last quarter of 2013, more than 10,000 attacks targeted government computers. It is unclear whether these attacks were attempted by individuals using specialized tools or by criminal organizations. Fortunately, these incursions were detected and the nefarious activity blocked. Moldova is also facing cyber threats to its critical information infrastructure. Given the interdependence of information infrastructure and sectors such as banking, transport, energy, social welfare and national defense, this is a cause for concern.

Moldova's government acknowledges the need to improve cyber security and understands that such security is directly correlated to national security in this technology-globalized era. The completion of national legislation in this area, including the establishment and enforcement of baseline security measures for national information infrastructure, is a government priority. This is one of the main pillars of a cyber security system.

CYBER CHALLENGES

One of the main disadvantages of the digital era is its dependence on systems and networks. Security issues are omnipresent. When it comes to cyber security, we acknowledge

that it is important for citizens to have confidence in state and private institutions. Therefore, Moldova's cyber security response must meet the challenging nature of growing and evolving cyber threats.

In 2010, Moldova launched the Governance e-Transformation process. This strategic program provides a unified vision to modernize and improve the efficiency of public services through IT governance. Information assurance — confidence in the security, integrity and availability of information systems — is therefore essential. A logical development would include implementing new systems, together with new protection measures. The fast-paced development process in the last decade unfortunately did not include enough controls to assure comprehensive cyber security.

MOLDOVA IS DEEPLY INVOLVED IN VARIOUS NATIONAL AND INTERNATIONAL PROJECTS AND INITIATIVES TO CREATE A SAFE AND SECURE SYSTEM FOR ALL.

Moldova is not alone in facing these challenges: It is inextricably linked with global IT development and emerging cyber threats.

Keeping information assets secure in today's interconnected computing environment is a challenge that becomes more difficult with each new "e" product and each new intruder tool. There is no single solution for securing information assets; instead, a comprehensive approach ensuring a multilayered security strategy and policies is required. One of the layers that governments are including in their strategies today is a computer security incident response team.

CERT-GOV-MD

Prevention, protection and detection methods must properly address existing risks. The lack of a security culture is one the biggest challenges for decision-makers and users. Developing and implementing a comprehensive set of minimum requirements across the whole of government and society is necessary to ensure cyber security. Even small changes to education, procedures and policy can raise the overall security level.

At the government level, several initiatives came to life. One of these is the establishment of a Computer Emergency Response Team, known as Cyber Security Center CERT-GOV-MD, created in partnership with NATO as a part of the Center for Special Telecommunications in the State Chancellery. CERT-GOV-MD will build on existing technical, cyber security and information assurance capabilities of the Center of Special Telecommunications to provide continuous protection of government systems and information against advanced and persistent threats.

CERT-GOV-MD is a unique entity for national data systems and public authorities. CERT-GOV-MD receives and processes information on existing or potential cyber threats, offers recommendations on the safe use of online data and provides assistance to Moldova's public administration in preventing and mitigating cyber incidents. Cooperating with various institutions, both national and international, CERT-GOV-MD is fully functional.

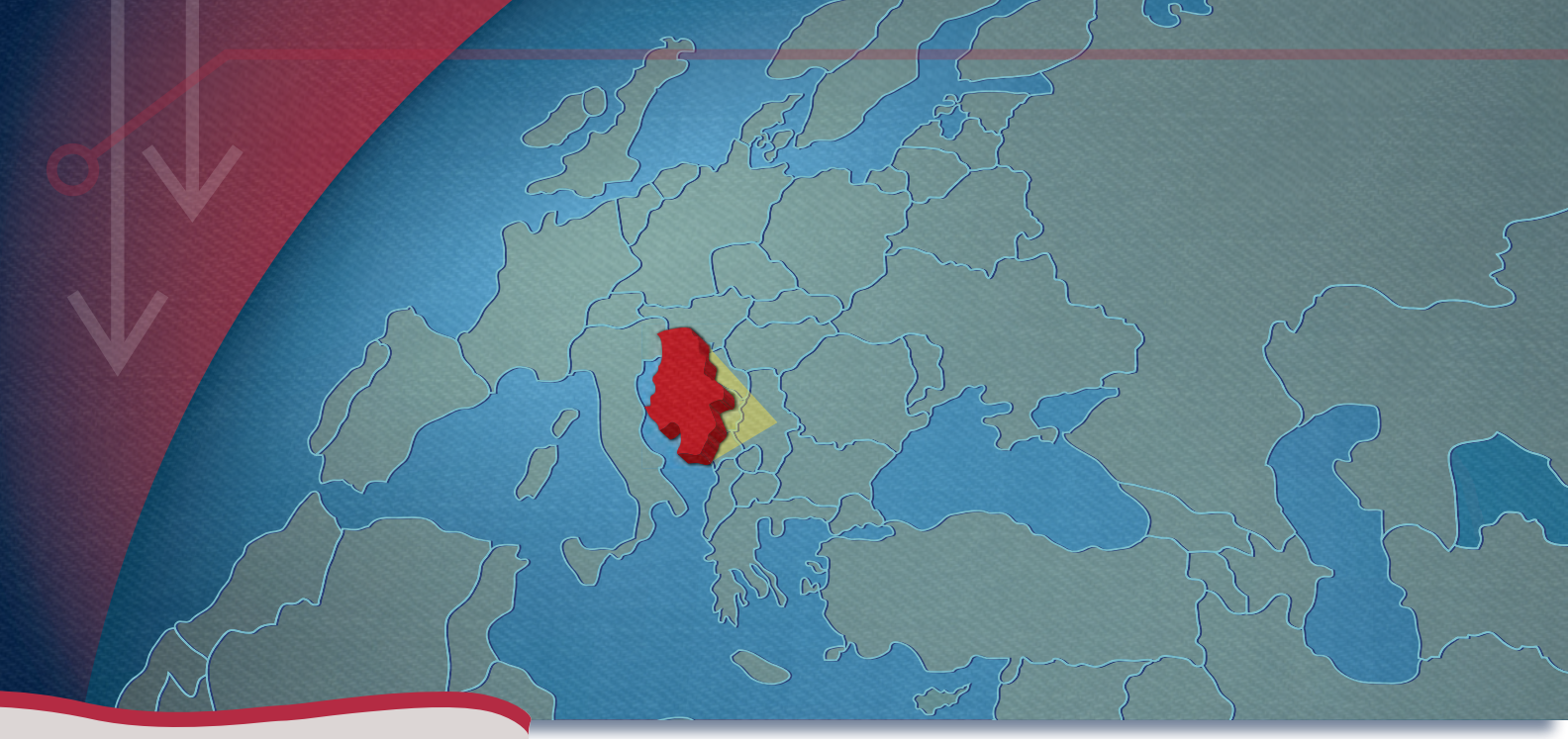
Still, the human factor is always the weakest link in the system. It is encouraging that in many countries IT security is a mandatory part of education. Young specialists are aware of new technologies and risks associated with IT and, therefore, it is the new generation that tends to drive necessary change. Moldova is striving for such educational upgrades. One of the action plans suggests creating minimum cyber security training and education requirements for public servants. This is very challenging, because the different age groups are prone to look at this issue differently. Also, changes have to be made incrementally to improve long-term retention. Cooperative international action and the sharing of best practices would improve cyber security for everyone.

The plans listed above are part of a complex strategy. The creation of CERT-GOV-MD, as well as practical training and legislative initiatives, are steps Moldova is taking to address threats. It's encouraging that in the few years since the creation of CERT-GOV-MD, the number of projects per year and people involved rise continuously. The effects of this cooperative effort across the whole of government are positive and provide tangible results by improving cyber security for everyone.

CONCLUSION

As cyber attacks grow in number and sophistication, the threat is viewed as a problem in both national and international security contexts. Yet assessments of how real the threats are, where the dangers lie, who is best suited to respond to them, and what kind of international measures and strategies are appropriate to protect information societies from malicious actors — in short, how best to safeguard long-term stability and peaceful use of cyberspace — vary widely.

The evolution of cyber threats means it is imperative that security is placed at the forefront of any organization. Unfortunately, individuals and organizations tend to underestimate the scope of the cyber security threat. It is important to enhance a public-private-civilian dialogue that will likely offer ideas and options to identify technical and policy solutions for building resilience in information systems. The Moldovan government is ultimately responsible for protecting its own systems and helping critical national infrastructure providers ensure its citizens can access government and other essential services. By becoming a leader in cyber security, Moldova can be a trendsetter in the digital world.



SERBIA

By **ZVONIMIR IVANOVIĆ**
University of Criminalistics and Police Studies, Belgrade

Modern innovations in communications technology have changed the world, but the same technology that has made modern society more productive has also been exploited by terrorists and criminals, creating new security and law enforcement challenges. As Serbia has transitioned into a 21st-century European democracy, it has strived to reform its legal system and law enforcement structures to manage the challenges presented by modern cyber crime.

Following the breakup of Yugoslavia, Serbia faced practical problems — a period of meandering legal theory and faltering reforms — but has finally achieved its goals. First, it is necessary to point out some irregularities in the Serbian legal system. Although Serbia has ratified certain Council of Europe Conventions,[1] no existing law adequately covers cyber crime with regard to information and communications technology (ICT). However, many secondary laws regulate certain aspects in detail. The responsibilities of some government agencies and ministries to enforce cyber crime laws do not correspond with their powers, and the partitioning of the Serbian legal system creates difficulties for those who must enforce the laws.

In July 2005, a law was passed creating a special prosecutor's office for cyber crime within the Office of the High Prosecutor, and establishing a special council of the court under the jurisdiction of the High Court of Belgrade.

But the Serbian legal system did not cover ICT and cyber crime until 2006, when it became necessary under obligations of the Cybercrime Convention of the Council of Europe (CETS 185). Although the former Union of Serbia and Montenegro signed CETS 185 (and the following protocol, CETS 189) in 2005, Serbian legislation did not cover cyber crime until the following year, when it was only partially covered by the Serbian Criminal Code.[2] Since then, the Serbian legal system has been frequently and thoroughly modified, a process to which a working group — formed under CETS 185 and 189 and implemented as part of the Council of Europe led Cybercrime@IPA SEE[3] project — contributed greatly.

In 2008, the High-Tech Crime Unit (HTCU), a special department for combating cyber crime, was established within the Ministry of Internal Affairs' Service for Combating Organized Crime. The HTCU is composed of two sections — a section for combating electronic crime and a section for combating intellectual property crime (copyright infringement and forgery). The HTCU has jurisdiction over pretrial proceedings for criminal acts involving cyber crime and crimes executed using computers and computer networks.

The Ministry of Internal Affairs is responsible for investigating (under the public prosecutor) criminal acts involving distribution of illegal content on the Internet and infringement of intellectual property rights. The HTCU can conduct investigations into crimes against computer systems as well as all crimes that involve technology. Digital forensics collection and analysis is not conducted by the HTCU, but entrusted to special services under the Ministry of Internal Affairs.

HTCU cooperates with foreign cyber crime

specialists via direct officer-to-officer communication through various international police organizations, such as Europol and Interpol and the Southeast European Law Enforcement Center, and through 24/7 networks and points of contact established by CETS 185.

Changes in the criminal code[4] in August 2009 made the Serbian legal system more, but not fully,[5] compliant with CETS 185 and 189.

A law on the organization and jurisdiction of government agencies in combating cyber crime[6] was passed in December 2009 to delineate jurisdictional responsibilities in cyber crime enforcement. Article 3 states that it governs investigation, indictment and prosecution of criminal acts such as: breaching computer data security; computerized offenses against intellectual and physical property and commerce; and offenses against human rights, including child pornography.

TRACKING ILLICIT MONEY

The law on the confiscation of property of criminal offenders has general provisions designed to stop the flow of illicit money and to search for, seize and confiscate criminal proceeds. It is possible to conduct a financial investigation and confiscate assets, regardless of the type of crime.

POLICE ACTIONS

To initiate criminal proceedings, evidence of a crime is required. As part of a criminal investigation, police officers conduct searches to collect evidence and other physical items or information useful for criminal proceedings, or to apprehend or prevent the escape of suspected perpetrators.[7]

The Law on Special Measures for the Prevention of Criminal Offenses Against the Sexual Freedom of Minors (Mary's Law) prescribes special measures for those who sexually abuse children and governs record keeping of people convicted of these crimes.[8] It includes stipulations on sexual abuse of minors through cyber crime. It also commissions government agencies within the Ministry of Justice to enforce criminal sanctions to include tracking, informing of movement, and storing sexual offender records.

CONCLUSION

Serbia's approach to cyber crime is scientifically and practically founded. Serbia has learned from its mistakes in this strategically important field. The path was very difficult but also fruitful. The Serbian legal system has experienced minor strains, but now has taken solid procedural, organizational and functional measures to meet the challenges posed by cyber crime. There is no perfect system, but Serbia's holistic approach represents a good start and is providing results.

Creating and managing this system is not possible without the help of international partners, and their efforts are acknowledged. All parts of the system were built to develop capacities to answer the challenges of new technologies and their misuse in the form of cyber crime. □

THERE IS NO PERFECT SYSTEM, BUT SERBIA'S HOLISTIC APPROACH REPRESENTS A GOOD START AND IS PROVIDING RESULTS.

If an offense was committed using the Internet and meets these general provisions, a financial investigation will be conducted as well. The prosecutor initiates such an investigation, which is conducted by the Financial Investigation Unit (FIU) in the Ministry of Internal Affairs. Institutional roles are as follows:

- Ministry of Finance – Administration for the Prevention of Money Laundering collects and analyzes data on suspicious transactions;
- Ministry of Internal Affairs – The FIU conducts investigations to identify and locate assets obtained through crime;
- Ministry of Justice – The Department for Organized Financial Crime leads pretrial proceedings to identify cyber crime and other offenses carried out using computers and computer networks, prosecutes offenders, conducts court proceedings, and manages seized property.

1. Before all Council of Europe Conventions – CETS: No. 185. and No.189.
2. Official Messenger of the Republic of Serbia no. 85/2005.
3. Official information about the project can be found at: http://search.yahoo.com/r/_ylt=A0oG7nw5J9lSQmMAEfpXNyoA;_ylu=X3oDMTBybnZlZnRlBHNlYwNzcgRwb3MDMQRjb2xvA2FjMgR2dGlkAw--/SIG=14s71c2eq/EXP=1389991865/**http%3a//www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%2520project%2520balkan/Mar11_Belgrade_Money_flows/Belgrade_A.Seger.pdf, last accessed January 17, 2014.
4. Official Messenger of the Republic of Serbia, no. 72/2009.
5. This means that there are still some inconsistences' regarding implementation of Cybercrime Convention.
6. Official Messenger of the Republic of Serbia, no.104/09.
7. Ivanović, Z. and Žarković, M. "Scientific approach to building teams for seizure of digital evidence," pp. 399-413 in Thematic proceedings of international significance, Vol I, Academy of Criminalistics and Police Studies, 2013, Ed. Goran Milošević, p.400.
8. Official Messenger of the Republic of Serbia, no. 32/13.

DEFENDING the Internet

A four-course program at the NATO School prepares graduates to identify and foil cyber attacks

By Maj. Rob Meanley, director of academic operations, NATO School

Since its founding in 1953, the NATO School Oberammergau (NSO) in Germany has graduated more than 210,000 officers, noncommissioned officers and civilians from 88 nations. Recognized as the global leader in multinational education, NSO conducts operational-level training in support of NATO's strategy to enhance operational capability.

In this capacity, NSO promotes the framework for NATO organization, plans, policies, operations, procedures and instruction in the employment of, and defense against, selected weapons systems. In partnership with U.S. European Command and NATO, the NSO underpins all allied operations, strategy, plans and doctrine throughout the European theater and other partner nations.

Through NSO, NATO assures the Alliance's collective capability to neutralize security challenges, including cyber attacks, the proliferation of weapons of mass destruction, terrorism, energy vulnerabilities and other threats to the security of NATO's nearly 900 million citizens. As such, NSO's charter is to focus strategically on countering these ever-evolving challenges — not the least of which is the cyber warfare arena.

Cyber security certificate program

Considering that cyber threats are projected to increase exponentially during NATO's shift from an operational to contingency planning mindset, NSO has collaborated with the U.S. Naval Postgraduate School (NPS) in Monterey, California, to offer a cyber security curriculum. Beginning with a basic (intro-level) foundation, each course complements previous material, culminating with in-depth network traffic analysis and evaluations. Upon completing the rigorous, four-course program, graduates earn an NSO-NPS Cyber Security Program Certificate.

Although NSO recommends that students take all four courses in logical progression to ensure the highest comprehension and cyber security skills development, students should pursue courses in any order as seats become available through their national points of contact.

Individual course highlights

Each course lasts 10 weeks and is offered twice per year. Each begins with one week of in-residence instruction at NSO in Germany, followed by eight weeks of facilitated distance learning, culminating with a final week in residence for student evaluation and graduation. The course list includes:

- M6-108 Network Security Course, the introductory course, is offered in collaboration with the U.S. Partnership Training and Education Center in Monterey. This course forms the bedrock of the program, which prepares graduates to comprehend the bits-in-transit aspect of network security. Foundational topics include defining networks, exploring routers, routing and access-control-list basics, traffic analysis, perimeter defense, e-authentication and virtual private network protocols.
- M6-109 Network Vulnerability Assessment Course complements and expounds upon M6-108 fundamentals. It aims to arm graduates with methodologies and techniques required for vulnerability assessments and follow-on mitigation. These methodologies are reviewed in-depth and are applied from the vantage point of hackers attempting to analyze and exploit common vulnerabilities. The course also uses lab exercises to solidify understanding of security threats, weaknesses and emerging methods of exploitation.
- M6-110 Cyber Incident Handling and Disaster Recovery Planning Course logically follows M6-109, stressing comprehension of the nature and scope of cyber-security-incident handling services, such as policy, planning, operations and technology issues. Students gain insight into intrusion/incident detection, minimizing loss of service, service continuity, and forensic analysis and service/data restoration. Ultimately, students learn how to mitigate and respond to natural disasters, denial of service, malicious code, malicious misuse of hardware and firmware, unauthorized access, data compromise and inappropriate use of network equipment.
- M6-111 Network Traffic Analysis Course completes the four-course cyber security program. By design, this course is the most robust. It not only supplements previous academics, it integrates real-time practical analysis and evaluation — the ultimate challenge. Students are expected to master operation of protocol/traffic analyzing equipment while simultaneously reviewing, analyzing and evaluating either "live" or prerecorded network traffic for indications and/or forensic evidence of potential, impending or realized configuration errors or malicious attacks.

Key allies and partners can expect powerful strategic and operational cyber security training programs, whether through NSO or the Marshall Center, to shape future engagements well into the future.

Conclusion

Whether NSO's popular cyber security courses are pursued individually or part of the recommended complete package, graduates glean invaluable cyber-awareness acumen in a critically functional area. As cyber threats continue to evolve, NSO will counter them by fortifying and adapting its strategies.

Meanwhile, the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany, is planning to launch its own tailored cyber security program in the summer of 2014 with possible plans to collaborate with NSO.

Key allies and partners can expect powerful strategic and operational cyber security training programs, whether through NSO or the Marshall Center, to shape future engagements well into the future. □

ONLINE *in* africa

"Our leaders need a reorientation, not tomorrow but today."

– TIM AKANO, CEO, New Horizons Nigeria[1]

The rising popularity of computers and mobile phones demands greater Internet protection

By DR. ERIC YOUNG, Marshall Center

As the e-revolution sweeps across Africa, cyber security has become a major emerging challenge. The continent's significant Internet-penetration growth rates are challenging the notion of a global digital divide. Economies are growing, social structures are changing, and political systems are transforming. Maasai ranchers can check cattle market prices on their mobile phones, and Africa's new high-speed undersea cables are leading an entrepreneurial boom in Kenya and Ghana. Rwanda's Vision 2020 is a youth-led, knowledge-based economy, and the Nigerian government recently launched a "Single Window Trade Portal" to facilitate trade and standardize services. However, with dramatic growth and change come challenges and threats to security from cyber crime, intellectual property theft, espionage and cyber attacks. To ensure that Africa fully benefits from the e-revolution, the continent's governments must take cyber security seriously, and nations worldwide can learn from Africa's approach.

Bedouins use a laptop computer in the Sahara in Tunisia. Mobile Internet use in Africa is among the highest in the world.

AGENCE FRANCE-PRESSE

AFRICA'S E-REVOLUTION

In the past few years, 11 new undersea fiber-optic cable systems surrounding Africa were completed, thanks to international and local investment.[2] This has brought faster and cheaper broadband connectivity to the continent. Economic growth, urbanization and a rapidly growing youth population have followed and created new economic opportunities. Cyber cafes have opened in war-torn Somalia; engineers in Kenya, Rwanda and South Africa are building new software for worldwide markets; and e-commerce is taking off from Algeria to Zimbabwe.

The numbers are impressive: Six out of the world's 10 fastest growing economies are in Sub-Saharan Africa, which has contributed to the creation of the second largest mobile phone market in the world. Smartphones outsell computers 4 to 1 in Africa, and it is estimated that Africa will have 1 billion mobile phones by 2016. Mobile Internet usage is among the highest in the world, and annual growth in the use of social media exceeds 150 percent.[3] There are more than 90 tech hubs, innovation labs, and e-incubators in more than 20 African countries. In addition to the economic and social impact, the political impact has been profound. The software platform, Ushahidi, emerged from and shaped the post-electoral violence in Kenya in 2008, @GhanaDecides educated voters prior to the 2012 elections, and social media had a profound role in the Arab Spring throughout North Africa in 2010.

Africa's e-revolution has not been without its challenges. Access to broadband remains uneven, focused mostly on the Anglophone countries and coastal urban hubs. Africa remains a "dumping ground" for second-hand, second-generation mobile devices and personal computers that are more vulnerable to attack and likely already to contain malicious code. An estimated 80 percent of the personal computers in Africa are already infected with viruses and other malicious software.[4] Mobile phone service has been used by some to advocate violence, and states have used it to limit freedoms and human rights. Yet on balance, all facets of life in Africa, from food security to health care access, employment opportunities to democratic freedoms, have benefited from the e-revolution.

THREATS TO AFRICA

To date, Africa has experienced a honeymoon in cyberspace. Most cyber attacks have been relatively unsophisticated with little impact. Cyber crime, off-the-shelf malware, phishing, or email-based advance-fee scams (commonly known as Nigerian 419 scams or in Nigeria as *yahoo-yahoo*) are referred to as *bafere* by Ugandans, and Ghanaians call it *sakawa*. Average citizens are routinely victims of cyber attacks, and only recently have cyber attacks had a major economic impact. The availability of more affordable Internet service and the increase of e-commerce have led to a rise in cyber crime. Likewise, the substantial growth in cellular telecommunications has led to more cyber attacks on smartphones. In 2012, South Africa, the most advanced e-commerce market on the continent, also ranked as the world's second most targeted country for phishing attacks. In October 2013, a variant of the "Dexter" malware program cost South African banks millions of dollars when it was inserted into point-of-sale devices at fast-food chains. In Nigeria, from 2010 to 2012 there was a 60 percent increase in attacks against government websites, which included attacks against the Central Bank of Nigeria, the Ministry of Science and Technology, and the Economic and Financial Crimes Commission.[5]

REUTERS

Workers lay fiber optic cables near the coastal city of Mombasa, Kenya, in June 2009. Eleven undersea fiber-optic cables have been laid in Africa in the last few years, providing faster and more affordable Internet connections.

Much more opaque and difficult to quantify is the theft of intellectual property (IP), cyber espionage, the costs of cyber security, and opportunity and reputational costs associated with malicious cyber activities. As McAfee and the Center for Strategic and International Studies note, the economic impact of the theft of IP is probably several times more than the cost of cyber crime.[6] Africa is not a leader in IP, yet as the e-revolution sweeps the continent, there will be more IP emerging from Africa and the theft of IP and sensitive business information is likely to increase. And although Africa, except for South Africa, is currently not a major target of cyber espionage, the threat is real.[7]

So, too, is the likelihood that some states will develop offensive cyber capabilities, further skewing the military capabilities between the "haves" and "have-nots." Information is not available on whether an African state or nonstate actor has successfully conducted an offensive cyber attack, but the social media and online presence of terrorist groups such as al-Shabab in Somalia demonstrates the ease and cost-effectiveness of such an attack. And because cyber crime is a transnational issue, African countries and their citizens remain vulnerable to attacks from anywhere in the world.

LAYERS OF SOLUTIONS

Africa faces many cyber challenges. First, African governments have limited capabilities in writing legislation and enforcement. In Kenya, for instance, fewer than 50 percent of cyber crimes are successfully investigated to the point of achieving a conviction.[8] Governments have only begun to fund cyber security, and governments lack information technology (IT) and cyber security professionals. Laws and regulations covering mobile telephones and Internet service providers (ISPs) are in their infancy, and enforcement is often lax. Corruption is endemic and spills over into the cyber domain. At the same time, the United States and Europe do not offer particularly good examples to follow, because they are heavily dependent on the private IT security industry and often behind the curve when it comes to cyber crime. Internationally, there isn't a central repository of cyber knowledge, expertise or training where Africa-specific solutions are presented.

Several "layers" of solutions to these challenges have emerged in Africa, from increasing cyber awareness to establishing Computer Emergency Response Teams (CERTs). National strategies against cyber security and international collaboration are necessary to ensure the e-revolution continues in Africa.

Cyber awareness through education and training is vital. This includes public and corporate awareness but most importantly awareness among lawmakers about the threats and opportunities of cyber security issues. Some in government have recognized the need for public awareness. As noted by Dr. Bitange Ndemo, Kenya's permanent secretary of the Ministry of Information and Communication: "The new government's pledge to provide a laptop to every child presents an opportunity for creating cyber security awareness at an early age. …

This will lead to a new generation of technology savvy people who are conscious about the effects of cybercrime."[9] Growing awareness will lead to growing demand for cyber security in Africa, and cyber security companies and ISPs must also facilitate protection. For instance, credit cards are widely required for online software purchases, yet credit cards are luxuries many Africans do not possess. Government should work with ISPs to provide greater public and private security.

In addition to increasing awareness, national cyber capacity is key. Further government training of experts as well as policy, legal and regulatory reforms will be needed to prevent and respond to cyber security threats and incidents. Several countries have quickly hired an impressive number of cyber human-resources staff, but only South Africa and Egypt have a significant number of trained cyber security experts. In recent years, a few countries have passed laws related to cyber security, cyber crime and data protection, but many already need updating, while other countries are struggling to catch up.[10] To better control crimes committed with the use of a mobile phone, SIM card registration is increasingly a requirement. Expertise in the cyber domain is needed at all levels across the government. A positive step would be to bolster law enforcement. Ghana, South Africa and Uganda have created new cyber units within their police forces.

The creation of national CERTs indicates growing government awareness and capacity. Eleven African countries have established them,[11] and a continentwide AfricaCERT based in Ghana coordinates incident reporting and promotes cyber security education and human resource development. Some CERTs have been impressive. In 2012, the new CERT in Côte d'Ivoire investigated 1,892 incident reports and authorities made 71 arrests, leading to 51 convictions on cyber security-related crimes.[12] Yet CERTs are also evolving institutions that must themselves learn to cooperate with other CERTs and the rest of government to be fully operational.

CERTs are only part of a comprehensive national cyber security strategy. Indeed, it can be a vital tool to ensure that scarce government resources are being appropriated to the cyber realm. South Africa emerged as a leader in cyber strategy on the continent, developing a national cyber security strategy in 2010 and inaugurating a National Cyber Security Advisory Council in 2013. Uganda also has a national cyber security strategy, and Kenya is developing a national cyber security master plan. In national strategies, it is important, as the South African and Ugandan strategies demonstrate, to take a whole-of-government approach, which ensures that the strategy is effective and will build national cyber capability, not just the power of one ministry or the capabilities of the government.

In addition to national strategies, regional and international approaches have improved cyber security in Africa. Regional economic communities have sought to collaborate on cyber security — the most active being the Southern Africa Development Community and the East African Community. For the past four years, the African Union has been considering an African Union Convention on Cyber Security that includes sections on electronic commerce, personal data protection and cyber crime with a special focus on racism, xenophobia and child pornography. But the draft convention has not been well-received among defense ministries in Africa. Critics are concerned the convention would curb Internet freedom. At the same time, leaving cyber security to the private sector in Africa is not a feasible, because profit-seeking, corruption and a weak legal framework do not correlate with national security requirements. Academia, think tanks and nongovernmental organizations will undoubtedly play important roles but they lack the financial resources to take the lead.

CONCLUSIONS

Africa's e-revolution will continue. Many Africans benefit from increased global connectivity. Africa's emerging cyber entrepreneurs must be embraced, both by the global community and by their governments. Uniquely African approaches, research and solutions are important for any cyber security strategy to take hold. But this growth, and indeed Africa's economic growth in general, will depend on improving cyber security. Continued prosperity in Africa will help pay the high costs of cyber security. Cyber security is not something that governments should simply outsource to the private sector or nongovernmental organizations. Countries must form partnerships, share best practices, build technical capabilities and offer legal guidance to one another. When it comes to cyberspace, everyone will sink or swim together. □

1. As quoted in Cristina Gallardo, "African Union Set to Get Tougher on Cybercrime," Allafrica.com, December 30, 2013, available at http://allafrica.com/stories/201312301604.html?aa_source=sptlgt-grid
2. For a summary, see Lucif Kharouri, "Africa: A New Safe Haven for Cybercriminals?" Trend Micro Research paper, 2013, pp. 3-4. Available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ice-419.pdf
3. Jonathan Kalan, "African youth hungry for connectivity," *AfricaRenewal,* May 2013. See more at: http://www.un.org/africarenewal/magazine/may-2013/african-youth-hungry-connectivity#sthash.rIejOhul.dpuf
4. B. Rowe, D. Reeves, D. Wood and F. Braun, "The Role of Internet Service Providers in Cyber Security," Institute for Homeland Security Solutions, June 2011, at http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf
5. "Cyber Attacks At Nigerian Government Websites Increased By 60% In 2012," TechLoy, January 17, 2013. Available at http://techloy.com/2013/01/17/nigerian-government-websites-cyber-attack-report/
6. McAfee, "The Economic Impact of Cybercrime and Cyberespionage," McAfee Report, July 2013.
7. South Africa appears to have been the only target of the suspected Chinese People's Liberation Army Unit 61398 offensive cyber group. See Mandiant Intelligence Center Report, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, p. 22. Available at http://intelreport.mandiant.com/
8. "Roundup: African governments seek to collaborate on cyber security," *Global Times,* May 28, 2013, available at http://www.globaltimes.cn/content/784802.shtml
9. Ibid.
10. See Kharouri, "Africa: A New Safe Haven," p. 8.
11. These include Burkina Faso, Cameroon, Côte d'Ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, South Africa, Sudan and Tunisia. Burundi and Uganda are in the process of creating national CERTs.
12. Rebecaa Wanjiku, "Africa Increases Cybersecurity Efforts," IT World, June 21, 2013 available at http://www.itworld.com/security/362093/africa-increases-cybersecurity-efforts

THE CYBER BATTLEFIELD

Russia has been at the vanguard of militarizing cyberspace

By **MAJ. DANIEL SINGLETON,** U.S. Army

VEER

In April 2007, the Estonian government moved a bronze statue of a Soviet soldier from a prominent place in the Tallinn city center to a military cemetery. The statue was controversial because it commemorated the "liberation" of Estonia by the Soviet Union. Ethnic Russians rioted against the decision and within a day of the statue's relocation, Russian-language websites began calling for armed revolution. During the next few weeks, the situation escalated. Massive cyber attacks originating from Russian servers were launched against Estonia's government and civilian infrastructure. These were mostly distributed denial of service (DDoS) attacks that clog Internet servers and render them inaccessible but do no permanent damage. Because Estonia is probably the most "wired" country in the world, the attacks impacted nearly every area of life and business. And these were relatively simple attacks.

Former U.S. counterterrorism chief Richard Clarke suggests in his book *Cyber War* that China has planted logic bombs[1] in the U.S. electric grid — essentially the equivalent of "dozens of Chinese government agents running around the country strapping C4 explosive charges to those big, ugly high-tension transmission-line towers and to some of those unmanned step-down electric substation transformers that dot the landscape."[2] He argues that Chinese cyber attacks dominate the news only because the Russians are better at covering their tracks.[3]

This article is a case study of cyber war from a Russian perspective: how the Russians view it, how they wage it, and what kind of international agreements they might be open to as the world confronts the challenges of applying international law to this new form of warfare.

The West generally views "cyber war" as activity that brings about the effects ordinarily caused by war but within the framework of the Internet, intranets, and all communication networks and devices connected to them. A related but broader term is "information war," which is the fight to control information itself. However, each region uses the term differently. The West uses "war" metaphorically, in the same way we spoke of the "Cold War." Even though it is normally used in conjunction with declared hostilities and military operations, "information war" does not constitute war in and of itself. But when those in the East, including Russia, speak about information war, they literally mean war, just by nonmilitary means.[4]

Unlike information war, both East and West usually see cyber war as a form of war. It describes the use of force even if it does not use typical weapons, because it has the potential to bring about military effects. Entering a network and causing physical destruction or damage to systems is a component of cyber attack that most would recognize as the equivalent of a conventional attack. In 2010, Gen. Keith Alexander, commander of U.S. Cyber Command, affirmed America's right to respond kinetically to cyber attacks that the Pentagon determines constitute an "armed attack."[5] This principle has been dubbed "cyber equivalency" and argues for a sort of *jus ad bellum* parity in regard to the methods that may initiate a war.

Although disconcerted by Alexander's remark,[6] Russia also recognizes cyber equivalency. For example, as four Russian colonels noted in the Russian military affairs magazine, *Voennaia Mysl'*: "… the heads of the member states of the Shanghai Cooperation Organization … established that the usage of modern information technology towards military-political goals could cause global catastrophes comparable in their destructive consequences with the results caused by weapons of mass destruction."[7] Russia does not disagree with the U.S. that cyber attacks can inflict damage equivalent to kinetic attacks and may be answered by either means. When Russians draw attention to Alexander's remark, it simply illustrates their concern that their own cyber operations or those of their surrogates might be met with what they view as a disproportionate response. But the issue of war in cyberspace is far more complex.

In Russia's view, there is no global Internet. Russia's proposal for principles of Internet governance at the 2012 World Conference on International Telecommunications reads: "Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance, and to regulate the national

Summary of Legal Positions on the
LAW OF WAR IN CYBERSPACE

Russian Federation	New international law is required to delegitimize cyber war. Current law is inadequate. Source: Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*
Collective Security Treaty Organization (CSTO)	While the CSTO has no official position, its leaders have likened cyberspace to anarchy that threatens the security of its member countries. Source: Joshua Kucera, "With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers"
European Union	Current international law should apply in cyberspace, but further dialogue and development of norms is necessary. Source: European Commission
North Atlantic Treaty Organization (NATO)	The law of war is difficult to apply in cyberspace because cyber attacks are unlikely to cause significant destruction, and the identity of the attacker is hard to determine. Source: NATO Council of Canada
United States of America	Cyber war already falls under the same laws as its kinetic counterpart. No new law is needed. Source: Elena Chernenko, "Russia warns against NATO document legitimizing cyberwars"

Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic."[8] In this view, cyberspace is not an international asset, but comparable to national airspace, land or any other physical space.[9] As such, each state has sovereignty over the Internet within its borders. This broad concept of domination of the Internet by individual states is necessary for the Russian military's plans for operating within it. Col. S.I. Bazylev, et al., explains why:

> *"The activity of the Russian Federation Armed Forces in information space is mainly aimed at restraining and preventing military conflicts in information space. In practice, this means the necessity of rigorous observation in the course of military activities in information space of generally accepted norms and principles of international rights, such as respect for state sovereignty, non-interference in the internal affairs of other states, abstention from the use or threat of force, and the right of individual and collective self-defense."*[10]

Sovereignty is key to Russia's position. The country wants power over its space, including its information space. Russia is concerned about three gray areas in cyber war: preparation of the battlefield with information weapons, such as the alleged Chinese logic bombs in the U.S. power grid; cyber espionage; and propaganda.

Russia is especially concerned with the proliferation of logic bombs, one of the most dangerous forms of cyber attack, since hackers attempt to penetrate the sites of the Russian president, Duma and Federation Council a combined 10,000 times every day.[11] This could explain, in part, why Russia has called for a ban on logic bombs, as well as "trapdoors," which are access points built into software that allow easy access to attack at a later date. This makes sense in a strictly military context but banning information weapons is unenforceable because they are not subject to inspection. It is much more difficult to hide a 32-meter-long SS-18 Satan missile from inspectors than a 5-centimeter thumb drive. Such a ban would also be convenient for countries planning to continue stealing technology rather than developing it themselves.

Espionage is not sabotage, but at some point even cyber espionage could become cyber war. Espionage has long been considered acceptable under international law. Russia is within its rights to prohibit cyber espionage, or any kind of espionage, within its own borders. But Gen. Vladislav Sherstyuk, director of the Institute of Problems of Information Security at Moscow State University and former deputy secretary of the Russian Security Council, has proposed a treaty making cyber espionage illegal internationally.[12] It is interesting that a world leader in espionage would seek to ban it. Some suspect this means the Russians are confident in their ability not to get caught.

The difference between espionage and sabotage seems clear at first glance, but the methods and effects of cyber espionage have shifted the paradigm. Most agree that a single spy entering a country and collecting intelligence does not constitute an armed attack. But consider the nonstop flow of cyber attacks the Pentagon and other U.S. government agencies must divert precious resources to stopping every day, which could be compared to millions of spies sent by a government that does not care if you stop some or even most of them. This massive espionage has even been described as "death by a thousand cuts."[13] If the 1 million attacks the Pentagon must defend its networks against daily[14] does not yet rise to that level, surely at some point it must. Countries and individuals who engage in this form of espionage should consider the ramifications, particularly when it appears even more magnified to the targeted country when combined with other cyber espionage being attempted by numerous actors.

Espionage may appear more threatening than propaganda to Western eyes, but Russia has made a national defense issue out of the latter, calling for the "defense of [the] public information-psychological sphere from negative content."[15] During a recent speech in Moscow, Deputy Prime Minister Dmitry Rogozin called social networks part of a cyber war against Russia. "These sites allowed for government opponents to identify each other and organize themselves," he said. "Through this, they increase the number of people who receive special content that is undermining the authority of the state and the values of the established state."[16]

Russia blames Western propaganda enabled by cyberspace for the color revolutions of the early 2000s that led to the fall of Russia-friendly governments in several former Soviet states. The editor of the Russian journal *Geopolitika,* Leonid Savin, wrote:

> *"As history has shown, the governments of foreign states are often behind these structures (social sites), as was the case with the Rose revolution in Georgia and the Orange revolution in Ukraine. The U.S. government and various funds financed organizations that initiated disorder and acts of protest, prepared activists, secured media support, and even brought political pressure on the governments of countries, demanding they initiate 'democratic reforms.' "*[17]

Judging by the effects, we must acknowledge propaganda to be a form of warfare. It is simply a form of warfare that the U.S. has decided to allow because it considers restricting freedom of speech a greater evil and because it is confident of winning in the marketplace of ideas. This constitutes an irresolvable difference between the Western and Eastern conceptions of the value of freedom of speech. Keeping the Russian interpretation of propaganda as a form of war in mind, however, should help us see why the U.S. quest to nurture Western-style democracy since the end of the Cold War has elicited a more hostile response from post-Soviet Russia than we might otherwise have expected.[18]

Supporters of the Pirate Party rally in St. Petersburg against Internet censorship. The Russian government, which views online freedom differently from the West, believes that it has sovereignty over cyber networks within its borders.

Russians have gone beyond propaganda

in waging cyber war but it is unclear who bears responsibility. After the DDoS attacks against Estonia in 2007, a leader in Russia's state-funded Nashi youth movement and assistant in the Russian Duma, Konstantin Goloskokov, took credit but insisted he acted alone.[19] By contrast, the attacks against Georgia in 2008 appeared more coordinated.

The Russian-Georgian War, which included cyber attacks from both sides, began when Georgia attacked Russian troops who had occupied the breakaway Georgian territory of South Ossetia as peacekeepers. *Inside Cyber Warfare* author Jeffrey Carr writes that Georgia used cyber war first, attacking Ossetian websites, and Russia responded.[20] If Carr's version of events is correct, why does Russia continue to deny that it conducted cyber attacks against Georgia? From a legal standpoint, it seems the Russian government should have few concerns since these cyber operations occurred in the context of a shooting war and had little negative impact on civilians.

In all likelihood, Russia continues to deny responsibility for three reasons. The first reason is to protect itself from legal scrutiny, deserved or otherwise. The attackers defaced some commercial sites with no conceivable military objective.[21] A second reason could be to hide Russian capabilities and tactics. The cyber attacks against Georgia, in addition to relatively unsophisticated DDoS attacks, included more advanced attacks such as injections of the programming language SQL[22] and cross-site scripting (XSS).[23] If Russia had assumed responsibility for either attack, it would be acknowledging a military capability[24] and a willingness to use it.

A third, and likely primary, reason is to retain plausible deniability in the future. Russia relies on strategic ambiguity in the area of cyber. The physical evidence in the cyber attacks on Georgia is so unclear that most writers on the topic are quick to hedge, asserting, like Naval War College professor Michael Schmitt, that "there was no conclusive evidence that the Russian government conducted the attacks or was otherwise involved therein."[25] The government of Russia does not conduct cyber attacks itself.[26] Instead, it has trained, supported and funded a number of hacktivist groups, like the now-defunct Nashi, that know what they are expected to do and that they will not be punished for it.

Russia's emphasis on state sovereignty protects this capability. Carr writes: "The Kremlin will negotiate on military capabilities that they haven't used, but will not negotiate on their civilian hacker assets that they have used. In fact, the latter is considered an internal criminal matter not open to international negotiation at all."[27] So when a state claims to be the victim of a cyber attack originating in Russia, Russia can say that it has never conducted a cyber attack of its own, so it cannot be blamed. Absent physical proof of the attack originating from within the Kremlin, it is difficult to hold the government legally responsible for everything done in Russia with a computer. As Katharina Ziolkowski of the German Ministry of Defense observes, "taking into account the supposed indirect and quiet use of 'proxies,' e.g. patriotic hackers (hacktivists), by certain States, invoking State responsibility for cyber activities will very seldom meet the legal requirements as currently set by international jurisdiction and scholarly writings, i.e. the test of an 'effective' or 'overall' control of the State over the activities of the non-State actors."[28]

In her paper "Ten Rules for Cyber Security"[29] Enekin Tikk, project coordinator for the *Tallinn Manual*, addresses the issue of state responsibility for aggression originating from its territory by hashing out the "Responsibility Rule," proposed earlier by Schmitt,[30] and by adding a related "Cooperation Rule."

- RESPONSIBILITY RULE — The fact that a cyber attack has been launched from an information system located in a state's territory is evidence that the act is attributable to that state.[31]
- COOPERATION RULE — The fact that a cyber attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state.[32]

In other words, if a computer within state A launches a cyber attack against state B, state A bears a presumption of guilt, the responsibility rule, and must demonstrate its innocence by assisting state B in finding the real culprit. The official U.S. position is more ambiguous.

Georgians visit a military cemetery in Tbilisi in August 2013 during a ceremony in memory of the 2008 war with Russia. The war marked the use of cyber attack as part of a wider military strategy.

AFP/GETTY IMAGES

THE *TALLINN MANUAL*

The *Tallinn Manual on the International Law Applicable to Cyber Warfare,* written at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence by an independent international group of experts, is the result of a three-year effort to examine how extant international law norms apply to this "new" form of warfare. The *Tallinn Manual* pays particular attention to the *jus ad bellum,* the international law governing the resort to force by states as an instrument of their national policy, and the *jus in bello,* the international law regulating the conduct of armed conflict (also labeled the law of war, the law of armed conflict or international humanitarian law). Related bodies of international law, such as the law of state responsibility and the law of the sea, are dealt within the context of these topics.

Source: NATO CCDCOE

U.S. Department of State Legal Advisor Harold Koh has said that states will be held responsible for cyber attacks when they are conducted by individuals under that state's instructions, directions, or control.

"If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful."[33]

"Control" could be interpreted broadly enough in the case of an authoritarian state or one with renowned policing capability.

Russia is especially concerned with the ambiguity, probably for fear that the U.S. will respond kinetically to cyber attacks originating in Russia. Savin writes: "Although governments declare that any cyber attack is deserving of a reactive response, it is necessary to draw the boundary where legal pursuit begins. The insistence that some attack is purposeful might be wrong."[34]

While hesitant to accept the responsibility rule, Russia has created the framework for the cooperation rule by signing an agreement[35] to create a communications link with the U.S. so that each party can inform the other of cyber activities in their information space that could be construed by the other as an attack. This could serve as a model to help prevent the further weaponization of cyberspace.

Conclusion and Recommendations

Russia is realizing that reliance on organized crime for the bulk of its cyber offensive capability is untenable in the long run. Internet service providers and other private entities are beginning to do the police work that Russia would not or could not do.[36]

We should also note that Russians are increasingly becoming victims as well. Not content with stealing from foreign interests, some cyber criminals are targeting Russians and thus directly challenging the state's authority and inadvertently providing common ground with the U.S. and Europe in the area of state sovereignty.[37] The U.S., Russia and the *Tallinn Manual* all concur: "States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[38] International law could be written in such a way as to address mutual concerns about the Internet's vulnerability and encourage solutions for reducing it, including separating lawful military targets as much as possible from civilian infrastructure.

Russia must also be reassured that "responsibility" does not mean that if someone in Russia launches a cyber attack against a NATO country, it will automatically be considered an armed Russian attack, or that "cooperation" gives the attacked country an automatic right to examine the entirety of Russian cyberspace. The responsibility and cooperation rules can be interpreted broadly so as to let the international community decide case by case whether a country is doing its best to prevent international cyber attacks from within its borders and allow neutral parties to do the inspecting. Adopting some form of these rules, either unilaterally or with NATO, could force Russia's hand against organized crime and give hard-pressed Russian politicians a measure of political cover, while reducing the possibility of an

international misunderstanding that could lead to the outbreak of kinetic war.

At the same time, the international community should encourage Russia not to mistake responsibility for absolute control. As Swedish Foreign Affairs Minister Carl Bildt remarked at the 2013 Stockholm Internet Forum, Russian law now allows the state to "block websites without judicial oversight or transparency."[39] Even if Russia's motives are benign, the potential for abuse and violation of human rights is grave.

Finally, to reduce the potential for miscalculation, the bar should be lowered for self-defense against cyber attacks, provided the attacker's identity is certain. With most states now capable of conducting a cyber attack, a high standard for the use of force to respond to a cyber attack merely encourages aggressor states and nonstate actors to push the envelope. Of course, it is vital to positively identify the attacker, as difficult as that often is, before retaliating. With potential victims authorized to use force against cyber attacks that fall short of what legally constitutes an "armed attack," potential attackers will think twice, uncertain of whether they will face repercussions for their actions. □

1. A logic bomb is a piece of code emplaced into a victim's computer via the Internet. When emplaced into certain networks, such as the U.S. electric grid, it can inflict damage equal to or greater than a conventional explosive.
2. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 198.
3. Ibid., 63.
4. Chinese thought goes even further, viewing war as a constant and the military as but a single aspect of it. Sun Tzu, for example, viewed the state as in constant conflict, competition or tension with other powers. Occasionally the conflict involves military means, but it is always there.
5. An "armed attack" is the use of military force against a state on a scale that justifies that state to resort to self-defense. It may be contrasted with the "use of force," which is a smaller-scale hostile act, such as an embargo, that does not trigger a state's self-defense rights, and nonmilitary hostile acts, which are matters of criminal or civil law, not war.
6. А.В. Савин, *Сетецентричная и Сетевая Война: Введение в Концепцию* (Москва: Евразийское Движение, 2011), 102.
7. С.И. Базылев, др., "Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве: Принципы, Правила, Меры Доверия." *Военная Мысль* 6 (июнь 2012): 25. http://www.ebiblioteka.ru/browse/doc/27601462 (accessed May 20, 2013).
8. Russian Federation, "Proposals for the Work of the Conference, Revision 1 to Document 27-E," WCIT Leaks, November 17, 2012. http://files.wcitleaks.org/public/S12-WCIT12-C-0027!R1!MSW-E.pdf (accessed June 19, 2013).
9. The U.S. military also considers cyber as a "domain," along with land, sea, air and space. David Perera, "Lynn: Cyberspace same as land, sea, air and space," FierceGovernmentIT, May 25, 2010. http://www.fiercegovernmentit.com/story/lynn-cyberspace-same-land-sea-air-and-space/2010-05-25#ixzz2s5YT9DjY (accessed February 1, 2014).
10. Базылев, "Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве," 27.
11. Иван Егоров, "Отобьем Кибератаки," Российская Газета 161 (июль 17, 2012): 2. http://www.ebiblioteka.ru/browse/doc/27406360 (accessed June 20, 2013).
12. Clarke, *Cyber War,* 229.
13 Sean Watts, "Low-Intensity Computer Network Attack and Self-Defense" in Raul A. Pedrozo and Daria P. Wollschlaeger, eds., *International Law and the Changing Character of War.* (Newport, RI: Naval War College, 2011), 72.
14. В. Гаврилов, "Взгляды Министерства Обороны США на Обеспечение Национальной Безопасности в Кибернетическом Пространстве," *Зарубежное Военное Обозрение* 7 (июль 2012): 3. http://www.ebiblioteka.ru/browse/doc/27608955 (accessed May 20, 2013).
15. I. N. Dylevsky, et al., "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect," *Military Thought* 1, vol. 16 (2007): 5. http://www.ebiblioteka.ru/browse/doc/24406039 (accessed May 22, 2013).
16. "Social networks part of cyber-war against Russia – Rogozin," Russia Today, June 7, 2013. http://rt.com/politics/part-cyber-war-rogozin-russia-354/ (accessed June 10, 2013).
17. Савин, *Сетецентричная и Сетевая Война,* 112.
18. Dylevsky, "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect," 3.
19. Carr, Jeffrey, *Inside Cyber Warfare,* O'Reilly Media Inc., 2011, pg. 118.
20. Ibid., 18.
21. One of the *Tallinn Manual* authors, Professor Thomas Wingfield, notes that, even with no conceivable military objective in some of these attacks, they would not rise to the level of the "use of force" because there was no "real" damage done. Conversation with Wingfield.
22. SQL injections involve inserting code into databases to steal information from them, manipulate them or even assume administrator access over them.
23. XSS involves inserting malicious code into JavaScript routines, usually found in third-party advertising on websites, which is then activated whenever an unsuspecting user clicks on the link.
24. Such an admission would not guarantee that this represents the limits of Russia's cyber attack capability. They did not need to use their entire arsenal against small countries like Estonia and Georgia.
25. Schmitt, Michael N., "Cyber Operations and the Jus in Bello: Key Issues" (March 2, 2011), U.S. Naval War College *International Law Studies,* 2011, pg. 90.
26. If Russia's cyber war capability is anything like its cyber espionage capability, it has far more in its arsenal than is commonly known. The successor agencies to FAPSI (Federal Agency of Government Communication and Information), the Russian equivalent of the U.S. NSA, run a school in Voronezh that sanctions hackers. Clarke, Cyber War, 63.
27. Carr, *Inside Cyber Warfare,* 170.
28. Katharina Ziolkowski, "Ius ad Bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force" in Czosseck, C., R., Ottis, and K. Ziolkowski, eds. 2012 4th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2012), 306.
29. Eneken Tikk, "Ten Rules for Cyber Security," *Survival: Global Politics and Strategy* 53, iss. 3 (2011): 129. http://dx.doi.org/10.1080/00396338.2011.571016 (accessed May 28, 2013).
30. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37, (1998-99): 913.
31. Tikk, "Ten Rules," 122.
32. Ibid., 123.
33. Harold H. Koh, "Koh's Remarks on International Law in Cyberspace, September 2012," Council on Foreign Relations, September 8, 2012. http://www.cfr.org/cybersecurity/kohs-remarks-international-law-cyberspace-september-2012/p29098 (accessed June 19, 2013).
34. Савин, *Сетецентричная и Сетевая Война,* 101.
35. Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security," *The Washington Post,* June 17, 2013.
36. John Leyden, "Russian Cops Lack Kit to Fight Cybercrooks, Says Brit Security Buff," Register (London), June 6, 2013. http://www.theregister.co.uk/2013/06/06/private_sector_leading_russian_cybercrime_cleanup/ (accessed June 10, 2013).
37. This was the heart of the Russian Communications Ministry's proposal at Dubai. The problem was that it authorized strict control of content and not merely infrastructure.
38. Schmitt, Michael, N., "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal,* 2012, pg. 31.
39. Carl Bildt, speech at Stockholm Internet Forum 2013, May 22, 2013.

CYBER SECURITY STUDIES

at the MARSHALL CENTER

A Comprehensive Nontechnical Program for Government and Cyber Professionals

By **DR. ROBERT B. BRANNON,** dean, Marshall Center

EXECUTIVE SUMMARY

Meeting the escalating demands of digital infrastructure requires the right technology and public policy. In today's interconnected world, organizations must actively defend against transnational threats in cyberspace. Decision-makers must be familiar with cyber security best practices to protect governmental and private activities. PCSS invites top experts from government, industry and academia to share their experiences and knowledge to provide participants the principles and state-of-the-art practices and strategies for the future.

The curriculum focuses on strategic objectives, techniques, policies and best practices that secure and defend the availability, integrity, authentication, confidentiality and nonrepudiation of information and information systems across cyber domains. PCSS provides participants with transnational cyber skills and prepares individuals for positions as senior-level cyber security leaders throughout government.

Sessions address strategy, policy and legal practices from multiple viewpoints and focus on comprehensive methods to advance cyber security and mitigate cyber vulnerabilities. Participants will also learn about active defense, incident response preparation and risk analysis. The content is targeted at ensuring the privacy, reliability and integrity of information systems.

There is a great deal of interest these days in all things "cyber." Despite a flurry of activity in several critical areas, the field of education and training has lagged, especially at the strategic, or policy, level. The Marshall Center's Program in Cyber Security Studies (PCSS) is designed to meet the specific needs of senior government officials who strive to improve their professional knowledge of transnational cyber security challenges. The program is taught by world leaders in cyber security and is tailored for senior officials with responsibilities for developing or influencing cyber legislation, policies or practices. PCSS is a nontechnical course that is ideal for diplomats, legislators, ministerial staff, policymakers, military and law enforcement officers. The program is unclassified, conducted in English, and open only to serving government officials.

The George C. Marshall European Center for Security Studies (GCMC) in Garmisch-Partenkirchen, Germany, is a unique German-American partnership institution that focuses on the most important transnational security issues, including cyber security, extremism, civil security, region-specific challenges, and interagency and interdisciplinary responses and cooperation. Guided by the legacy and ideals of the Marshall Plan, the Marshall Center promotes Euro-Atlantic values through security education. The GCMC conducts resident and nonresident courses throughout Europe and Eurasia. The Marshall Center supports both governments and boasts an international faculty and staff from 10 partner nations.

WHAT IS CYBERSPACE?

Cyberspace is the transnational domain of information technology infrastructures and interdependent networks. This includes the Internet, telecommunications networks, computer systems and embedded processors in critical industries.[1] Common usage of the term also refers to the virtual environment of information and interactions between people.

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, commerce is not compromised, and infrastructure is not infiltrated.

Protecting cyberspace requires strong vision and leadership, as well as 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 enhancing national security, the global economy and individual free expression.

Threats to cyberspace pose one of the foremost economic and national security challenges of the 21st century for national security professionals. A growing array of state and nonstate actors are targeting citizens,

commerce, critical infrastructure and governments. These transnational actors compromise, steal, alter or destroy information.

PROGRAM OVERVIEW

The Marshall Center Program on Cyber Security Studies is led by Professor Phil Lark and his deputy, Col. Gottfried Salchner of the Austrian Army. They have developed a comprehensive program incorporating a whole-of-government approach. Elements of PCSS are included in all Marshall Center programs, including the Program on Terrorism Security Studies (PTSS), the Seminar on Transatlantic Civil Security (STACS), and the program on Counternarcotics and Illicit Trafficking (CNIT). The PCSS program seeks to increase partnership possibilities with cyber security organizations. Interested organizations should contact the GCMC for further information.

The PCSS prepares leaders for making informed decisions on cyber security, strategy, resourcing, policy and planning and is designed for senior and midlevel civil servants from throughout the whole of government who are involved in the development of cyber and information technology and legislation, planning, investigations and government oversight. Diplomats, policy practitioners, cyber security management, law enforcement and military officers are invited. Participation is extended to, but not limited to:

- Ministry of Interior
- Ministry of Justice
- Ministry of Banking and Finance
- Ministry of Emergency Situations
- Ministry of Foreign Affairs
- Ministry of Defense civilians and military officers
- Law enforcement officials
- Ministry of Communications and Information

The program emphasizes:

Privacy versus security and liberty versus control
The PCSS addresses the friction between individual privacy and collective security.

The private and commercial nature of the Internet
No single entity — academic, corporate, governmental, or nonprofit — administers the Internet. Most of the technical infrastructure is privately owned. The network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks.

Action, leadership and ethics
Participants in the PCSS join a corps of educated, professionally connected and disciplined leaders who can address cyber security's complex challenges. This network cultivates a proactive and cooperative approach to meeting present and future transnational cyber security challenges.

Competing angles of analysis
In international affairs, there are multiple approaches to solving problems and meeting transnational security challenges, including cyber security. Competing priorities, public-private friction, legal issues, national and corporate interests, and professional ethics must be kept in mind.

The program focuses on:

The environment, institutions and challenges
PCSS offers a comprehensive cyber program that encourages "intellectual cyber interoperability." The program promotes:

- Understanding of the transnational cyber environment, including national approaches in the United States, Germany, the European Union, NATO and other international organizations
- International collaboration and information sharing
- Cyber strategy and policy development
- Detecting and combating cyber crime
- Cyber policy applications in countering terrorism
- Cyber aspects of critical infrastructure protection
- The role of the private sector in information and cyber technology
- Identifying measures for cooperation in detecting and mitigating cyber incidents

The program features:

- This three-day intensive cyber education program for parliamentarians and senior leaders covers the critical strategy, policy, and legal and private sector issues of cyber security at the executive level. This program enables the sharing of perspectives, experiences and best practices on current and relevant cyber security issues. It facilitates a network of key government officials in positions of influence from throughout the world with a common understanding of cyber security challenges.

- A PCSS resident course conducted at the Marshall Center starts with a two-week session that focuses on strategic objectives, techniques, policies and best practices that secure the availability, integrity, authentication, confidentiality, and nonrepudiation of information and systems across cyber domains. The course length may grow in future iterations and will include distance learning via GlobalNET. This core resident course provides:
  - Deeper understanding of cyber security challenges at the executive and functional levels
  - Networking opportunities for civil servants and cyber practitioners to forge strong transnational and cooperative relationships

NONRESIDENT OFFERINGS

These are regionally focused events supporting Central and Southeast Europe, the Black Sea, Eurasia and Central Asia. Each workshop supports the needs and requests of partners and connects regional leaders with leading cyber experts and German and American teams. GCMC nonresident events are flexible and respond to emerging requirements nationally and regionally.

Distance Learning
Participants registered for the resident program undergo an Internet portion of the course before arriving at the GCMC. Reference materials, policy documents, selected lectures and panels are available online at the Marshall Center's GlobalNET Web pages. PCSS alumni may continue their professional development through GCMC distance learning webinars and other online hosted events.

Cyber-Weekly Newsletter
The GCMC's cyber security newsletter is available to GCMC alumni every week. This newsletter highlights cyber-related news and emerging challenges in a variety of areas, including:

- New vulnerabilities and threats
- Academia and professional articles
- Cyber trends
- Legislation, policy and regulations
- Technologies and standards
- Investigations, law enforcement and litigation
- Research and development
- Best practices
- Cyber events
- Key leaders and cyber personalities

Internships
The George C. Marshall Center Student Internship Program is an unpaid internship offering U.S. and EU citizens who are enrolled as undergraduate and graduate students a chance to participate and support the GCMC Program on Cyber Security Studies. These internships provide professional development through hands-on experience in an academic setting and insight into the daily operations of an international security studies center.

English Language Refresher Course-Cyber Security Language (CSL)
Commencing in 2014, CSL is designed for both military and civilian cyber professionals who want to improve their topic-specific English language skills before attending the PCSS resident course. The five-week course helps non-native English speakers participate fully in PCSS and enhances their professional development, as well as their engagement with fellow participants, GCMC faculty, and the cyber community as a whole.

Cyber Library at the Marshall Center with Internet via GlobalNET

Alumni Program
The GCMC has more than 10,000 alumni in nearly 140 partner nations. The alumni include senior policymakers and military officers, as well as career civil servants from dozens of ministries. Our specific alumni programs include:

- Distinguished alumni events
  Conversations with senior leaders
- Community of interest events
  Cyber-specific networking and education
- Regional alumni workshops
  Southeast Europe, Black Sea/Eurasia, Central Asia and worldwide
- In-region networking
  Partnerships with embassies, ministries and alumni associations

THE RESIDENT COURSE

The resident course focuses on ways to address evolving challenges in the cyber domain but still adhere to fundamental democratic values. It helps participants appreciate the nature and magnitude of today's threats and develop a common understanding of the lexicon, best practices and current initiatives within the public and private cyber sectors. Moreover, the program allows participants to establish a professional network with other cyber-focused government officials. Initially, the GCMC will offer a two-week resident program beginning in December 2014. There is enthusiastic potential to expand and grow the resident program, especially as we seek to establish new partnerships and adapt the curriculum to current and relevant challenges. The objectives of the program include:

- Developing a mutual understanding of country-specific approaches to cyber security
- Enhancing participants' ability to comprehend, analyze and evaluate defense and cyber security issues and transnational challenges
- Cultivating an ability to think critically and strategically on cyber matters
- Strengthening the foundation for cooperative approaches to shared cyber security challenges

PARTICIPANT OUTCOMES AND EXPECTATIONS

The Marshall Center does not offer textbook solutions to challenges. Participants can expect to develop a better understanding of the main cyber security issues influencing national, regional and international security, the factors shaping national cyber security strategies, and the imperatives of cooperative security in an interdependent world. Corresponding benefits of participation include:

WHOLE-OF-GOVERNMENT APPROACHES TO:

Internet Governance	Privacy and Security
Cyber Statecraft Development	Protection of Intellectual Property
Cyber Capacity Building	Combating Terrorism & Cyber Crime
Internet Freedom	Public/Private Partnership

- Increased awareness of the magnitude of the challenges in cyber security
- Improved coordination between intergovernmental/international organizations, international processes and private enterprises
- Long-term international support to regional challenges
- Proactive coordinated international support
- Practical information sharing and professional networking
- Exchanging best practices
- Greater local ownership of the issues, problems and solutions

THE CURRICULUM

The course curriculum emphasizes the essential skills of the cyber professional, including strategy and policy development, collaboration, planning, critical thinking, strategic leadership, and crisis and risk management skills. It consists of lectures, panels, video teleconferences, seminars, exercises and case studies. The modules consist of plenary lectures attended by all participants, small group seminars (approximately 12-15 participants) led by Marshall Center resident faculty and adjunct international experts, and readings that focus on relevant and current literature.

PCSS begins by building a foundation for understanding cyber security. GCMC professors orient participants on the operational definitions, conventions and institutional frameworks of the cyber security field. These initial lectures cover norms and responsible state behavior in cyberspace, international laws and organizations, and the cyber security policies of the U.S., Germany, the EU and NATO. This expands into current trends and issues such as privacy versus security, and discussion of national and transnational threats and challenges.

PCSS then moves into complex issues of cyber strategy and risk analysis through case studies of governmental and corporate cyber policy development. Participants examine best practices on how to protect high-value assets and critical infrastructure, and how highly adaptive nonstate entities, such as organized crime networks and terrorist groups, influence policy. This prepares participants for the PCSS capstone exercise in which they develop a personalized cyber strategy on a topic of their choice.

Additionally, PCSS seminars expand on cyber attribution, and focus on public-private collaboration and the contrasts between both sectors' emergency response teams. PCSS professors guide participants through contingency planning for natural disasters and other events, reinforcing data protection, and understanding the growth of data centers. The curriculum concludes with cyber policy ethics and guidelines on how to acquire and develop the next generation of cyber professionals, and futurists from the private sector share their visions of emerging possibilities, challenges and solutions in cyber security.

In summary, PCSS participants receive presentations from prominent government officials, private industry experts and internationally renowned scholars. The curriculum provides a framework of professional development and networking for cyber security experts and professionals as they pursue their careers. Graduates of PCSS do not learn what to think, but how to think about complex national and transnational cyber challenges.

Specific cyber security topics addressed in the PCSS and other GCMC resident and nonresident programs include a wide variety of cyber security themes. The German-American partnership at the GCMC offers rich, constructive and useful programs to best prepare government leaders for complex challenges.

The Program on Cyber Security Studies complements other GCMC transnational security programs that focus on countering transnational threats such as terrorism, insurgent and criminal networks, organized crime, illicit trafficking and civil security challenges. All transnational threats include a cyber domain. □

1. National Security Presidential Directive 54/Homeland Security Presidential Directive 23.

HOW TO APPLY

For additional information about PCSS, contact the program leadership at cyber@marshallcenter.org. For application information, contact the Marshall Center registrar at registar@marshallcenter.org, your ministry point of contact, or the U.S. Embassy or German Embassy in your capital city.

FREE *to* WORK

EUROPE BENEFITS WHEN LABOR CAN MOVE FREELY ACROSS EU MEMBER STATES

By *per Concordiam* Staff

Newspaper reporters and television cameramen patrolled British airports, train stations and bus depots on January 1, 2014, looking for the "tidal wave" of new migrants. An influx of migrants was expected because transitional work restrictions on Bulgarian and Romanian citizens had expired the day before, seven years after those countries joined the European Union, allowing their residents to work anywhere in the EU.

Even though that feared tsunami didn't arrive, many Europeans are concerned that liberalization of labor markets for immigrants from the EU's eastern members will interrupt the progress made by Western European countries still struggling through economic recoveries. In the Netherlands, Germany and the United Kingdom, media outlets and politicians clamor for protecting labor markets and social welfare systems from immigrants.

ISTOCK

"100 Romanians and Bulgarians take a job in Britain every day, official figures show," blared an August 2013 headline in the online version of London's *Daily Mail*. Others warn of "benefits tourism" — immigrants coming not to work but to collect generous social welfare benefits.

Eastern European leaders continue to confront what they view as popular misconceptions about job competition in Western Europe. "We will not accept being treated as second-rate citizens," Romanian Prime Minister Victor Ponta said in November 2013 in response to rumblings in the UK media.

Fundamental EU right

The free movement of all member-country citizens has been enshrined as one of the cornerstones of EU integration and of the EU's Single Market. Labor mobility was guaranteed in the 1957 Treaty of Rome that established the European Economic Community, the common market that evolved into the EU. At any one time, more than 14 million people work, study and retire in member states other than their own, the EU reports.

In 2004, when eight formerly communist Eastern European countries entered the EU, only the UK, Sweden and Ireland allowed immediate unrestricted labor migration. UK government officials estimated 13,000 immigrants per year would come. But at the peak, before the economic crisis, more than 100,000 came each year from Poland alone, causing substantial social concern and, some argue, labor displacement. Many of these laborers returned home to work in Poland's relatively robust economy. Nevertheless, according to the 2011 census, more than half a million Polish citizens lived in the UK, nearly 10 times the 2001 population.


AFP/GETTY IMAGES

British wine merchant Richard Fox, at his shop in Bucharest in December 2013, welcomes Bulgarians and Romanians who want to work in his home country. He and thousands of other Europeans have settled in Bulgaria and Romania.

On joining the EU in 2007, Bulgarian and Romanian citizens endured transitional labor restrictions imposed by Austria, Belgium, France, Germany, Luxembourg, Malta, the Netherlands, Spain and the UK. Many of these countries demanded an adjustment period they argued would benefit the host and source countries alike. From the beginning, Bulgarian and Romanian citizens have been able to travel freely throughout the EU and could work in a self-employed or temporary capacity. As of July 2012, the UK Office for National Statistics said that about 150,000 Bulgarians and Romanians were living in the UK; the EU said that more than 3 million already live throughout the EU.

Immigration's benefits

Despite social problems caused in some communities by any large migration — strains on housing, education and other infrastructure — studies show that opening labor markets in 2004 was beneficial to host countries, including the UK. In the book *Borderless Economics*, author Robert Guest calls migration a "productivity multiplier" because it spreads ideas, inspires innovation and allows skills to flow where they are most needed. Migration is the most efficient way to allocate human capital.

As the EU has pointed out, mobility "addresses skills gaps and labour shortages and tends not to take jobs away from host country workers." An October 2013 report from the Centre for European Reform (CER) concluded that Eastern European immigrants have had virtually no impact on native unemployment rates in Britain (except a negligible impact at the lowest levels of the jobs

AT ANY ONE TIME, MORE THAN 14 MILLION PEOPLE WORK, STUDY AND RETIRE IN MEMBER STATES OTHER THAN THEIR OWN.

market) and often stimulate increases in overall wages, thanks to higher productivity. Rather than losing jobs to immigrants who tolerate lower wages, many jobless Britons suffered from a lack of "basic employability skills, incentives and motivation," according to a 2008 UK Department for Work and Pensions (DWP) report.

Construction workers build new houses in Bristol, England. The British construction industry provided plentiful employment for immigrants from Eastern Europe.

In 2004, European economies were thriving, and jobs for immigrants were plentiful, particularly in the construction and service sectors. The UK and other longtime EU members suffered severe shortages of skilled workers and were looking to the new eastern members to fill the void. Meanwhile, Eastern European countries had many highly educated workers unable to find good jobs in their post-communist economies. But the UK and other "rich" countries now face higher unemployment and budget austerity, raising concerns that such migration is no longer affordable.

Much of the uncertainty is based on the belief that floods of new immigrants overtax host counties' social welfare systems. German Bundestag member Hans-Peter Uhl told Reuters in December 2013: "We have the free movement of labor in Europe, and that is the main idea. It is important for us and we should keep this idea, but freedom of movement does not mean free access to our German social welfare system for everyone." British Prime Minister David Cameron introduced measures to prevent new arrivals from qualifying for unemployment benefits and placed restrictions on other social benefits. In defiance of EU rules, the Dutch cities of Rotterdam and The Hague announced intentions to deny identification numbers to Bulgarians and Romanians who can't prove they're working.

The data do not support these fears. A study commissioned by the Dutch Ministry of Social Affairs found that Eastern European immigrants not only take jobs most native Dutch don't want, but also "pay more taxes than they claim in benefits," *The Economist* reported. The CER report found the same thing in Britain, calling "benefits tourism" a falsehood. CER said EU immigrants are "more likely to be in work than Britons" and "far less likely to take up benefits than the British population." According to a January 2014 *New Europe* article, the UK DWP registers only 60,000 benefits claimants out of about 2.3 million EU immigrants to Britain.

AFP/GETTY IMAGES

Romanian students in Bucharest react to comments by European politicians and media outlets portraying them as benefits scroungers in December 2013.

Conclusion

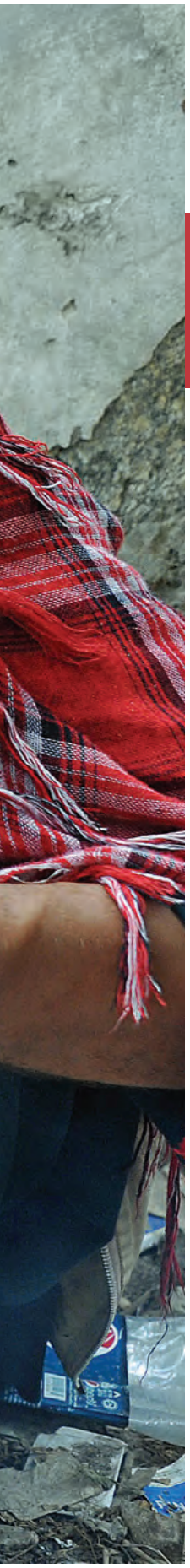
In the end, the worst fears of labor migration critics may amount to little more than hyperbole and political posturing. Bulgarians and Romanians have been able to travel freely throughout the EU since 2007 and have been free to work in most EU countries. Experts suggest the vast majority who want to work abroad have already relocated. Mihai Fertig, who operates a bus service between Bucharest and several Western European cities, told Euronews television that he expected only a 10 percent increase in bookings in 2014.

Romanians in particular have little reason to "flood" the UK or Germany. Romanians have more linguistic and cultural affinity with Italy and Spain, and Romania's economy is not doing badly, *The Economist* says. The country's rapidly growing wages, low unemployment and lower cost of living have reduced the desire to emigrate. In an interview with BBC Radio that aired in January 2014, Andreas Cser, who runs a jobs placement service for Romanians, said interest in British employment has waned and job seekers favor positions better aligned to their skills.

A study released by the European Commission in October 2013 shows that across the EU, the vast majority of economic migrants move to another country to work, not take benefits. The free movement of labor benefits both source and host countries, economically and socially. Studies suggest that migrants tend to be entrepreneurs and risk-takers equipped with the courage necessary to leave home and start anew in a foreign land. As the CER report said: "EU immigrants are a boon, not a burden." □

Young Afghans smoke opium in Jalalabad. Addiction is rife in Afghanistan with repercussions for domestic stability.

AFP/GETTY IMAGES



TAKING ON NARCOTRAFFICKING

Border security and demand reduction could alleviate the scourge of Afghan heroin

By *per Concordiam* Staff

It's been called the doomsday scenario for Afghan heroin: As Afghan military and police forces assume greater responsibility for their own national security, opium production will skyrocket with dire consequences for security in the region and the world.

But evidence is accumulating that a sustained explosion probably won't occur, if only because the youthful populations that have driven demand for Afghan drugs are exhausting their capacity to consume ever increasing amounts of opium and its derivative heroin.

"Some may contend that sustainable counternarcotics efforts in Afghanistan are doomed," said a joint 2013 United States-Russia study called "Afghan Narcotrafficking: A Joint Threat Assessment." "This report, however, takes issue with a simplistic hands-off view that Afghanistan is quickly becoming … an intractable problem."

The doomsday scenario is just one of several misconceptions experts have identified in outlining a strategy for suppressing narcotrafficking that, in its Afghan incarnation, blights the health of millions, nourishes corruption and finances terrorism. Reflecting on more than a decade of multinational peacekeeping operations in Afghanistan, experts are challenging other planks in the anti-opium campaign.

They place less faith in a single-minded focus on eradicating poppy fields, arguing that the destruction of crops in one province tends to shift production to other provinces. They question the belief that rivalries among Central Asian states preclude cooperation on stopping drugs. And they are investigating whether licensing Afghan farmers to produce legal opium for medicinal use, an experiment that has worked well in Turkey, would help build stability.

NO DOOMSDAY

Although opium production in Afghanistan shows few signs of abating, the recent growth appears to be unsustainable. The experience of Russia suggests a reason why.

As the largest single market for Afghan heroin, Russia is wracked by addiction and diseases such as HIV linked to the use of infected needles. Heroin became cheap and plentiful just as Russia experienced an economic boom fueled by sales of oil and gas. The United Nations Office on Drugs and Crime (UNODC) estimates Russian opiate users at 1.7 million, more than 1.6 percent of the country's population, and the number of addicts has risen by about 80,000 a year.

"It fell upon us like an avalanche," said Dr. Ekaterina Stepanova, a Russian expert who lent her research to the Afghan narcotrafficking report.

But avalanches usually subside, and that is what could happen in Russia based on the experience of Western Europe, another large destination for Afghan heroin. Use of the drug there has stabilized or declined as the user population ages and fewer young people take up the habit.

That means demand for Afghan heroin could reach a ceiling with repercussions for the producers and traffickers operating in and around Afghanistan. Instead of being almost exclusively a consumer nation, Russia could become more of a transit nation for the drug.

QUESTIONING ERADICATION

Russia has pressed hard for eradicating poppy fields from the air, a technique used in places such as South America to eliminate coca crops, the main ingredient of cocaine.

But experts such as Vanda Felbab-Brown of the Brookings Institution insist that destroying fields—and thus the livelihoods of thousands of poor Afghans—tends to strengthen the bonds between farmers and extremists.

She called eradication the "single worst policy," and insists groups such as the Taliban cynically adopt the cause of illicit opium to turn themselves into "potent political forces" among the roughly 20 percent of Afghans who sustain themselves through poppy cultivation. Poppies, the seeds of which are also used for food, have been planted for centuries in the region. "It throws populations into the hands of the militants," Felbab-Brown said during the 5th International Symposium on Terrorism and Transnational Crime held in Turkey in December 2013.

Opium also finances those same extremists. By taxing farmers—generally considered a form of extortion—the Taliban have raised millions of dollars to wage violent campaigns against Afghan and multinational security forces.

One Afghan smallholder named Khan Bacha in the eastern province of Nangarhar told The Associated Press that extremists have demanded payment of a "religious tax" in the form of opium.

"They say we are going for jihad," Bacha said in the November 2013 article. "It is the 'God money' we give."

GUARDING BORDERS

Abandoning eradication as a primary strategy shifts the emphasis to interdicting opium after harvest. Much of the focus has been on the so-called northern route that crosses primarily Tajikistan and Kazakhstan on its way to the Russian market and beyond.

An even more prolific pathway, called the Balkan Route, begins in western Afghanistan, veers south of the Caspian Sea and uses Turkey as a land bridge to European markets.

Turkey prides itself on leading the world in bulk heroin seizures, but notes that tens of thousands of its citizens continue to make a living through the illicit trade. "Drugs and corruption go hand in hand," said Dr. Behsat Ekici, an eastern Turkish police official with firsthand knowledge of the Balkan Route.

It's little surprise that Turkey, with ethnic ties to most of the Central Asian republics, has helped lead the way in training Kazakhs, Tajiks, Afghans and Kyrgyz in counternarcotic techniques and border security.

The Turkish International Academy against Drugs and Crime has joined NATO, Russia and the UNODC to train more than 2,000 counternarcotics officers from Central Asia and


REUTERS

Afghan policemen burn over 20 tons of narcotics seized by Afghan Security Forces in Kabul in November 2013.

Afghanistan. In addition, the Central Asian Counternarcotics Initiative has set up anti-drug task forces throughout Central Asia to seize opium and heroin passing mostly through regional transit points.

"The resulting counternarcotics network would link both the main narcotics source country, Afghanistan, with the key transit countries in Eurasia, many of which are also becoming large consumers of Afghan-based narcotics in their own right," *World Politics Review* noted in a 2012 article.

Such a counternarcotics network is needed now more than ever: Despite measures to increase effectiveness by Afghan police, military and customs officials, they still struggle to keep pace with the rise in Afghan opium production.

LICENSING OPIUM?

Turkey could provide yet another useful example to serve a global counternarcotics strategy.

The Turkish government and the U.N. oversee legal cultivation of about 35,000 hectares of poppies divided among 13 provinces. The crop services not just the legitimate market for medicine but also a demand for poppy seeds for baked goods.

Turkey recognizes that opium is one of the easiest crops to grow on marginally productive land. Up to 100,000 farmers — and by extension another 500,000 of their relatives — benefit financially from the program, the U.N. said in a report.

Most of that output is processed at the Turkish-run Afyon Alkaloids Plant and exported abroad. The U.S. pharmaceutical market is the biggest customer.

Many suggest the model is exportable to Afghanistan, where poppies are entrenched in the culture and used as tribal medicine.

But any movement toward legalization should proceed cautiously. India, which also runs a legal opium operation to supply international pharmaceutical companies, suffers from the fact that an unknown percentage of the production is siphoned off for illicit uses.

"Even if instituted, the licensing scheme would not be a panacea, and some serious problems posed by large-scale opium cultivation would persist," Felbab-Brown wrote. "Because licensing absorbing only a part of the illicit economy could easily generate new problems, including ethnic and tribal tension, licensing should only be undertaken once the Taliban insurgency has been defeated, other obstacles to licensing have been overcome, and licensing could be implemented on a country-wide scale."

> Destroying fields — and thus the livelihoods of thousands of poor Afghans — tends to strengthen the bonds between farmers and extremists.

CONCLUSION

Suppressing the drug trade in and around Afghanistan has proven elusive, but few doubt that a solution must be multinational.

Zabihullah Dayam, spokesman at the Afghan Ministry of Counter Narcotics, emphasizes that Afghanistan, which borders Pakistan and Central Asia, cannot fight drugs on its own.

"As long as we don't have a joint regional and even beyond regional cooperation and commitments, it will be difficult for the Afghan government to succeed," he told the Voice of America in 2013.

The alternative — narcotrafficking remaining one of the chief tools of regional destabilization — is a scenario rejected by a broad coalition of states encompassing the Middle East, Central Asia and Europe.

"The drug economy is more than just mafia cartels buying estates, businesses and aircrafts. They also buy officials, elections and parties. In a word, they buy power," said Antonio Maria Costa, former executive director of the UNODC. "Here is where the drug industry threatens security and development." □

Looking East

Joining the Eastern Partnership has proven valuable for EU partner nations

By *per Concordiam* Staff

The former Soviet republics of Georgia and Moldova each have taken a big leap toward European integration. On November 28, 2013, leaders of the two countries initialed Association Agreements with the European Union, committing them to a path of economic and democratic reform. The hard work of implementing those reforms is just beginning, and if Georgia and Moldova formalize the agreement in September 2014, the EU will remove some trade and travel barriers with those countries.

Moldovans rally in favor of European Union integration on Great National Assembly Square in Chisinau in November 2013.

REUTERS

The agreements were reached through the EU's Eastern Partnership (EaP), a multilateral cooperative initiative between the EU and six former Soviet republics from Eastern Europe and the South Caucasus. The EaP advances concepts such as the rule of law, human rights and democracy to improve security and open new markets to a region deemed strategically important. Within the forum of the EaP, each partner country negotiates a bilateral Association Agreement with the EU based on the country's specific progress and priorities.

"The Eastern Partnership is an EU policy aimed at bringing our eastern neighbors closer to the European Union," said EU Commissioner for Enlargement and European Neighbourhood Policy Štefan Füle. "The EU's support for democratic and economic reforms in the neighborhood helps to strengthen stability and prosperity, which brings direct benefits to the citizens, both in these countries and in the EU."

Acting-Ukrainian Prime Minister Arseny Yatseniuk attends an emergency summit of European leaders in Brussels in March 2014 to discuss Ukraine and the Russian occupation of Crimea.

Eastern Perspective

The EaP is the "eastern dimension" of the EU's European Neighbourhood Policy (ENP). The EU launched the ENP in 2004 with the aim of building prosperity and democracy in neighboring regions. In addition to the Eastern Partnership, the ENP includes the Euro-Mediterranean Partnership with countries from North Africa and the Middle East, and Black Sea Synergy to encourage regional economic cooperation in the Black Sea basin.

The EaP was initiated in 2009 to foster closer political and economic relations among the countries of the EU and Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. The idea for the EaP originated in the Polish Foreign Ministry, which partnered with Sweden to present it to the rest of the EU.

Poland has a long-held interest in improving relations with its eastern neighbors and drawing them closer to the EU, particularly Ukraine, with which it has significant historical and cultural ties. Even before its own accession to the EU, Poland pushed for increased EU engagement with the East.

According to *The Telegraph* of London, the central reason for the EaP is to encourage the eastern neighbors to "look to Brussels, not Moscow, for future leadership." Despite the desire to more deeply integrate Eastern Europe with the EU, neither membership in the EaP nor an Association Agreement guarantees a path to EU membership. Expansion fatigue has arisen in many European countries since Bulgaria and Romania were admitted in 2007. Perhaps more importantly, Russia strongly opposes further EU expansion into the former Soviet space, and some EU members see little value in "rocking the boat" of fruitful commercial ties with Moscow.

Structure and Programs

Economic integration with the EU — a fundamental purpose of the EaP — is formalized through a Deep and Comprehensive Free Trade Agreement (DCFTA). According to the EU, the DCFTA gives the partner country "enhanced access to the European market" and the tools to modernize. It also incentivizes reforms by requiring the partner country to conform to a wide range of EU standards and regulations. The EU helps finance institutional reform, democratization and economic and social development programs. Examples include the Comprehensive Institution Building Programme and the Pilot Regional Development Programme, both established in 2011.

The EU has distributed substantial bilateral aid packages to partner nations since 2010, including 596 million euros to Ukraine and 339 million euros to Moldova. Programs supported by the aid include vocational training in Armenia, environmental protection in Belarus and border security in Ukraine and Moldova.

Multilateral platforms were established to support reforms and exchange best practices on topics such as good governance, economic integration and energy security. The EU has used flagship initiatives to "give substance and focus to multilateral cooperation" in border management, small- and medium-size business support, energy efficiency, disaster response, civil society and education.


AFP/GETTY IMAGES

Moldovan Prime Minister Iurie Leancă, left, speaks with French President François Hollande at the European Union's Eastern Partnership Summit in November 2013 in Vilnius, Lithuania, where Moldova initialed an Association Agreement.


AFP/GETTY IMAGES

Acting Ukrainian Foreign Affairs Mnister Andrii Deshchytsia, right, welcomes Polish Foreign Affairs Mnister Radosław Sikorski to Kiev in March 2014.

Partnership Unraveling

Just as the EaP appeared to be bearing fruit, it faces new and substantial challenges. Ukraine, which was supposed to sign its Association Agreement (initialed in March 2012) at the November 2013 EaP Summit in Vilnius, Lithuania, declined to sign under pressure from Russia and in turn was awarded $15 billion in loans and a deep discount in natural gas prices by Moscow. Armenia also backed out of initialing its Association Agreement — fearing the loss of Russian security guarantees in the face of the country's troubled relations with Azerbaijan — and promised to join the Russian-led Eurasian Union trade bloc instead.

"What happens in the countries in Eastern Europe and the southern Caucasus matters to the EU. As the EU has expanded, these countries have become closer neighbours, and their security, stability and prosperity increasingly affect the EU's."

— Eastern Partnership policy statement

Russia sees the EaP as a threat to its regional influence, particularly in Belarus and Ukraine. Shortly after the EaP was launched, Russian Foreign Minister Sergei Lavrov accused the EU of trying to establish a "sphere of influence to pull countries away from taking sovereign decisions."

After moderating its criticism for several years, Russia took aggressive steps in November 2013 to keep EaP countries from establishing closer relations with the EU.

According to Carnegie Europe, "Russia's increasingly assertive tactics have chipped away at the ties that bind the six Eastern Partnership countries to the EU, and the entire Eastern Partnership is on the verge of unraveling."

But the EaP is not "one size fits all." As Lithuanian Foreign Ministry official Juris Poikāns pointed out, the EaP was established with the understanding that partner states have different levels of ambition regarding EU membership, making them open to different levels of engagement. Georgia and Moldova have clearly chosen closer integration than Belarus or Armenia. Azerbaijan, self-assured in its energy wealth, seeks only trade and visa agreements.

But Ukraine is crucial, with its population of more than 45 million and substantial economic capacity, not to mention an important geopolitical location. Former Kremlin official Gleb Pavlosky told Reuters in November 2013 that Russian President Vladimir Putin's dream of a Eurasian Union, built from the former Soviet states and centered on Russia, "is impossible without Ukraine." "Losing Ukraine would be a massive blow to Russia," James Nixey of Chatham House told the *Guardian* in October 2013. "Ukraine is viewed by Putin as part of Russia. He'll ask himself, how can you be a great power if this huge appendage is lopped off?"

A Ukrainian demonstrates against Russian involvement in Ukraine, holding a sign that says, "Putin, if you love us, let us go!" in front of the Russian Embassy in Kiev in December 2013. The pumpkin is the symbol of a rejected marriage.

REUTERS

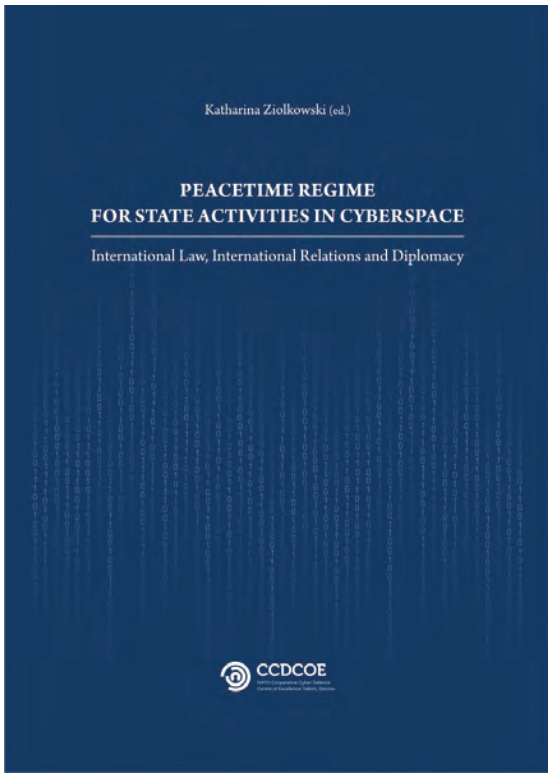
But Ukrainian opinion is split. A majority in the western and northern districts appears to favor a European path; eastern and southern districts with large ethnic Russian populations are more Moscow-oriented. The Ukrainian government's initial refusal to sign the EU Association Agreement ignited massive protests in the streets of Kiev that ended with the removal of President Viktor Yanukovych from power. An interim Ukrainian government led by the former opposition signed an Association Agreement in March 2014 as Russia annexed Ukraine's Crimean peninsula.

Enduring Partnerships

Despite opposition from Russia, EU engagement in former Soviet states will persist. Carnegie Europe concludes that the EU can best help by "offering an alternative to Russian forms of power projection," which it calls a zero-sum game.

The EU should not be seen as competing with Russia for influence and power in the EaP countries, Carnegie says, but should proceed with a "positive-sum" approach. The EU should reward eastern neighbors for making real reforms in areas such as corruption and judicial independence rather than slowing progress and impeding relations by dwelling on less critical technical, bureaucratic and administrative hurdles.

"What happens in the countries in Eastern Europe and the southern Caucasus matters to the EU," the Union says in its Eastern Partnership policy statement. "As the EU has expanded, these countries have become closer neighbours, and their security, stability and prosperity increasingly affect the EU's." □



Cyber Security in an International Context

BOOK EDITOR: Katharina Ziolkowski, NATO CCDCOE Publications, December 2013, 746 pages

REVIEWED BY: Vytautas Butrimas, chief cyber security advisor, Lithuanian Ministry of National Defense

There is a legend about former U.S. President Dwight D. Eisenhower's visit to a secret government laboratory to see the latest "super computer." In those days, computers were large, and this particular computer filled a warehouse the size of a modern IKEA store. President Eisenhower asked it: "Is there a God?" Several minutes passed while lights flashed and the machine hummed and churned inside. Finally, it presented the president with the answer: "Now there is."

Similarly, the dynamic interactions and synergies of new information and communications technologies have created a new domain called "cyberspace." This domain of electromagnetic activity, digital data processing and data transmission is invisible to the naked eye, yet it is just as vital to the health of our economies and social well-being as the air we breathe. However, the great promise of these new technologies and our growing dependence on them has exposed serious vulnerabilities that need to be addressed. One of these is malicious state-sponsored cyber activities, including cyber espionage and the use of malware to disrupt or destroy critical processes that support life and economic activity.

The recent contribution by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, a book titled *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, comes after several high-profile cyber incidents have contributed to an increasingly tense atmosphere among nations. This landmark 740-page volume features a collection of articles on technology, security policy and legal issues that could apply to state activities in cyberspace.

Policymakers, legal experts and information technology (IT) security professionals who are used to working in a Microsoft Windows, Intel, PC-based environment will find much to like. However, industrial control systems-oriented cyber security folks may be slightly disappointed. For example, searches in the book for terms that refer to the systems and devices used to remotely access and control critical infrastructure (CI) operations such as SCADA, PLC, DCS and RTU yielded no results. The cyber fragility of CI devices and systems, which provide the foundation for the safety and availability of electric distribution grids, transportation systems, and water and gas pipeline control, is not adequately understood and not properly addressed. The complexity of cyberspace requires cyber security professionals from multidisciplinary backgrounds. It is not enough to be an IT cyber security expert.

This selection suffers from an imbalance in contributors: 15 of 24 focus on legal aspects, four address international security policy, three are scientists/specialists and two examine military ramifications. The lack of a multidisciplinary approach is perhaps part of the reason malicious state-sponsored activities in cyberspace have not been adequately addressed in international forums. Diplomats who seek to develop confidence-building measures and draft cyberspace treaties through discussions and negotiations in international organizations

need to work in partnership with the technical community, not in isolation. Diplomats and policymakers alone cannot manage this issue without an understanding of technology and its potential misuse.

Critical infrastructure is a vulnerable target for cyber attack, not just from cyber criminals and politically motivated hacktivists, but also from states. Part I of the book focuses on "technical features" (and most curiously, "sociological facets"). STUXNET is mentioned, but not one author made reference to Ralph Langner, the first to analyze and draw attention to the sinister non-Windows part of STUXNET. This is like writing about the theory of relativity without referencing the works of Albert Einstein. Our understanding of the serious technical and policy implications of STUXNET came not from IT professionals, or those working for anti-virus firms specializing in Windows-based software protection, but from industrial control experts who are aware of STUXNET's second, non-Windows "warhead," namely the Siemens program logic controllers and the specialized software used to monitor and control these devices. The book underestimates the impact of this new family of malware, handicapping policymakers who must ask two critical questions when developing national cyber security strategies: What needs protecting and what are the threats?

This compilation also fails to address the link between STUXNET and the "Edward Snowden affair," revelations of massive government cyber spying and surveillance programs. To prepare hostile malware for a specific target requires a great deal of support not only from laboratory programmers but intelligence services. Snowden's leaks of information from the U.S. National Security Agency show the enormous capacity of governments to actively and passively collect intelligence. If the book better integrated STUXNET and Snowden, it would have been possible to evaluate the threat of STUXNET type attacks in the future.

The book's failure to recognize these two points leads to its third major weakness – the assumption that attribution is futile. The legal analysis gives the impression that current laws are sufficient if attribution were feasible, but failed to explore other ways of addressing the issue. For example, Jason Healey of the Atlantic Council wrote an excellent paper, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," offering an innovative proposal for dealing with attribution.

The authors could also have noted successes in assigning attribution to cyber crime. The main ingredients are a shared perception of the common threat, available technical means and, most importantly, the will and desire to cooperate. A good example is the arrest of Sven Olaf Kamphuis, alleged to have organized the biggest cyber attack in Internet history. He lived in the Netherlands but was arrested with the cooperation of Spanish law enforcement. The Snowden revelations, if true, support the argument that the technical means to investigate and assign attribution are available. When a state comes under suspicion for a cyber incident, the combination of ingredients used to defeat cyber crime is lacking. Attribution is not impossible, as many of the authors (Christian Czosseck, Mauno Pihelgas and Terry D. Gill) seem to think, but rather a political problem. However, governments do not want to apply the same methods, nor any legal caveats, that could constrain their own cyber activities.

Part II, "Rights and Obligations of States in Cyberspace," is perhaps the most ground-breaking section. It provides approaches on how states' current responsibilities in other domains could be applied to cyberspace. There is a fascinating and informative survey of current legal applications in the domains of aviation (Stefan A. Kaiser and Oliver Aretz), the environment (Thilo Marauhn), undersea cables (Wolf Heintschel von Heinegg), outer space (Martha Mejia-Kaiser), territorial sovereignty (Benedikt Pirker) and world trade (Joel P. Trachtman). Many have tried to use nuclear or chemical warfare policy as an analogy, but space law is worth reading. The section ends with a discussion of cyber espionage (Ziolkowski). Efforts should be made to avoid equating cyber spying with traditionally accepted spying. In cyberspace, the policy implications of the easy transition from cyber spying to cyber sabotage are not fully appreciated, especially relating to "preparation of the battlefield."

In a 2011 *per Concordiam* article, I concluded that because of growing and largely unaddressed security issues, the Internet as we know it is at a crossroads. In Part III, Chris C. Demchak provides a very plausible, yet troubling, prediction on where one choice for the road ahead may lead. The remaining choices unfortunately will not save the Internet "utopia" that existed from 1992 to 2007. The best we can do, in this reviewer's opinion, is to agree on some reasonable "rules of the road" that will save as much of that utopia as possible.

This collection of articles provides a strong case for putting the activities of states in cyberspace on the international agenda. It represents a significant contribution toward a wider understanding of the complex policy issues raised by our critical dependence on cyberspace. This is an ambitious, challenging, must-read volume for everyone seeking ways to manage clear and present cyberspace dangers threatening national security and economic and social well-being. This work can provide a common base from which to work together to ensure a "cyber safe" future for all. □

A downloadable, free copy of the book is available at https://www.ccdcoe.org/427.html

This review represents the opinion of the author and should not be attributed to any organization with which he is affiliated.

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 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 15-1
Dec. 4 - 19, 2014

December

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

PROGRAM ON COUNTERING NARCOTICS AND ILLICIT TRAFFICKING (CNIT)

The two-week resident program focuses on 21st-century national security threats as a result of illicit trafficking and other criminal activities.

CNIT 15-4
Apr. 9 - 24, 2015

April

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

The Marshall Center's flagship resident program, a seven-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 14-9
Sept. 29 -
Nov. 14, 2014

September

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

October

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

November

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

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 15-3
Feb. 25 -
Mar. 25, 2015

February

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

March

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

PTSS 15-7
July 9 -
Aug. 6, 2015

July

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

August

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

SEMINAR ON TRANSATLANTIC CIVIL SECURITY (STACS)

STACS provides civil security professionals involved in trans-Atlantic civil security an in-depth look at how nations can effectively address domestic security issues that have regional and international impact. The three-week seminar examines best practices for ensuring civil security and preventing, preparing for and managing the consequences of domestic, regional, and international crises and disasters. The STACS will be offered once in FY 2015.

STACS 15-6
June 3 - 24, 2015

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.

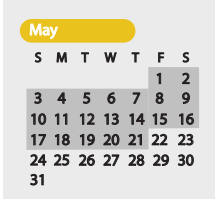
**Adapting Our Strategies to Counter Evolving Transnational Terrorist Threats from Al-Qa'ida, its Affiliates and its Advocates*

SES 14-8
Sept. 15 - 19, 2014

SEMINAR ON REGIONAL SECURITY (SRS)

The three-week seminar aims at systematically analyzing the character of the example crises, the impact of regional actors, as well as the effects of international assistance measures. SRS 15-5 will concentrate on two traditionally unstable regions, looking at actual conflicts in the regions and efforts to achieve stability.

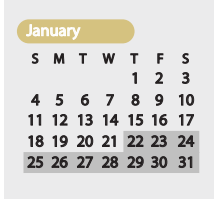
SRS 15-5
Apr. 30 -
May 21, 2015

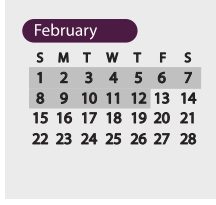


PROGRAM ON SECURITY SECTOR CAPACITY BUILDING (SSCB)

The purpose of this three-week course for midlevel and senior security-sector professionals is to assist partner and allied countries, as well as states recovering from internal conflict, to reform and build successful and enduring security institutions and agencies.

SSCB 15-2
Jan. 22 -
Feb. 12, 2015





Alumni Programs

Dean Dwigans
Director, Alumni Programs
Tel +49-(0)8821-750-2378
dwigansd@marshallcenter.org

Alumni Relations Specialists:

Barbara Wither
Africa, Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Macedonia, Middle East, Montenegro, Romania, Serbia, Slovenia, Turkey

Languages: English, Russian, German

Tel +49-(0)8821-750-2291
witherb@marshallcenter.org

Chris O'Connor
Belarus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Moldova, North America, Poland, Russian Federation, Slovak Republic, South America, Ukraine

Languages: English, Russian, Polish

Tel +49-(0)8821-750-2706
oconnorc@marshallcenter.org

Milla Beckwith
Afghanistan, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyz Republic, Mongolia, Pakistan, Southern & Southeast Asia, Tajikistan, Turkmenistan, Uzbekistan

Languages: English, German, Russian

Tel +49-(0)8821-750-2014
ludmilla.beckwith@marshallcenter.org

Christian Eder
German Element, Germany, Austria, Switzerland, Western Europe

Languages: German, English

Tel +49-(0)8821-750-2814
christian.eder@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**

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