per
Concordiam
Journal of European Security and Defense Issues

■ **PINPOINTING THE PROBLEM**
Discovering sources of cyber attacks

■ **UNWELCOME TRENDS**
Hackers skirt the law

■ **CYBER ALLIANCE**
Business partnering with government

■ **CAUCASUS COURTS TOURISM**
Travel revival brings benefits

PLUS
Integrating European Roma
In defense of Afghan women
Quest for clean electricity

SECURING CYBERSPACE

Table *of* Contents

features

ON THE COVER

Stopping attacks on vital computer networks, both civilian and military, has become a top security goal of the European defense community. Against a backdrop of more than 1 billion Web users and tens of millions of Websites, cyber attackers have learned to wield computers as cheap, anonymous weapons, often with impunity. NATO and the European Union are making progress in identifying and punishing hackers who pose a security threat.

PER CONCORDIAM ILLUSTRATION

p. 10

An Unsettling Trend

Cyber attacks illustrate need for better defense against Internet intrusions.

16 Stopping Cyberterror

Countries must work together to fend off cyber threats from criminals.

22 Heading Off Hackers

Criminals use computer networks as cheap, anonymous weapons.

28 Strength in Unity

Public and private sectors can help each other secure cyberspace.

34 Defending Cyberspace

International law must address security threats emerging online.

38 A New Era of Accountability

International legal reform could help pinpoint sources of computer attacks.

departments

4 Director's Letter
5 Contributors
6 In This Issue
7 Letters to the Editor
8 Viewpoint
64 Book Review
66 Calendar


p.22

COOPERATION

42 An Electrifying Start
Europe aims to diversify energy supplies with proposals for wind and solar power.

46 From Hostility to Hospitality
Calm in the Caucasus could revive the region's tourist industry.

SECURITY

50 Upholding Afghan Women's Rights
ISAF mission is key to preserving women's gains in Afghanistan.

54 Touting Reform in Central Asia
Five former Soviet republics seek strength through cooperation.

58 "Hacktivists" Strike Back
Attacks on financial institutions illustrate the worldwide cyber threat.

POLICY

60 Europe's Mixing Bowl
Better integration of ethnic and religious minorities would build stability in the European Union.


p.54


p.60

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the sixth issue of *per Concordiam*, in which we address the topic of cyber security. As the world becomes more interconnected and countries become more reliant on computer technology and high-speed communications, we see growing threats to the privacy of our citizens, the integrity of our business transactions, the safety of our critical infrastructure, and even the readiness of our military forces. Traditional measures of security, such as geographic distance or standing forces capable of deterring or defeating comparable enemies, are less relevant against those who would take advantage of cyberspace for unauthorized, hostile or illegal activities.

Cyber threats are diverse: from teenage vandalism to state-sponsored espionage, from traditional organized crime to the malicious targeting of individuals, from incitement to riot (as in the early stages of the cyber attack on Estonia in 2007) to the stealthy placement of weapons to be activated in the event of war between nation-states. Those examples suggest that cyber activities are limited more by the imagination of the aggressor than by the defender's ability to detect and prevent such attacks.

Effective, lawful cyber defense faces many challenges. Internet technology makes anonymous or even false-flag operations much easier to mount. The high speed of cyber operations leaves little time for effective investigation of intrusions, consultative cooperation among targeted states, or even legal review of the available responses before immediate defensive actions must be taken. The law pertaining to cyber operations runs the gamut from domestic criminal law enforcement to international legal determinations regarding "use of force" and "armed attacks" giving rise to the right of self-defense. Finally, national cyber policies are further complicated by challenges in interministerial cooperation and the fact that the overwhelming majority of cyber targets inhabit the private sector, beyond the immediate control of most governments.

To stay ahead of cyber threats, European and Eurasian government leadership should use a "whole of nation" approach to maintain critical infrastructure protection programs that encourage cooperation between government and key private sector companies.

Despite these very real threats, advances in cyber technology will continue to accelerate. The benefits such technology affords — economic efficiency, political transparency and global integration — will require the security studies community to provide analysis and advice to address and overcome these threats. This issue of *per Concordiam* and continuing research, education and outreach programs at the Marshall Center contribute to this effort.

We look forward to your comments on cyber security issues. Your responses will be included in the next two issues of *per Concordiam*, which will cover the topics of NATO and the change occurring in North Africa and the Middle East. Please contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director

Keith W. Dayton
Director, George C. Marshall European Center for Security Studies

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

Vytautas Butrimas has been working in information technology and communications for more than 20 years, starting as a computer specialist for Prince William County, Virginia, and advancing to Vice Minister at the Ministry of Communications and Informatics, Republic of Lithuania. In 1998, he moved to the Ministry of Defense as policy and planning director. Since 2001, Mr. Butrimas has worked as deputy director of the CISS under the Ministry of Defense. In 2009, he led the task force that prepared the Cyber Defense Strategy and Implementation Plan. Mr. Butrimas is a two-time Marshall Center SES graduate.

Dr. Viacheslav Dziundziuk is a professor at the Kharkhiv Regional Institute of the National Academy of Public Administration (Ukraine). He specializes in contemporary political and geopolitical processes, information security and government reform. Dr. Dziundziuk is the author of a monograph and numerous articles, and has co-authored several books in this field. He holds a doctorate in governmental affairs and graduated in 2008 from the Program in Advanced Security Studies at the Marshall Center.

Alexander Klimburg is a fellow at the Austrian Institute for International Affairs. Since 2006, Mr. Klimburg has undertaken government national security projects for the Austrian Federal Chancellery, the Ministry of Defense and the National Security Council. He has consulted with various national governments and governmental institutions, and is the principal author of a forthcoming European Parliament study on cyber warfare. Within cyber security, his work has primarily been in the area of information security, critical information infrastructure protection, and the integration of cyber warfare, cyber terrorism and cyber crime. He is the author of advisory papers as well as a contributor to the book *Inside Cyber Warfare*. He holds degrees from the University of London's School of Oriental and African Studies and the London School of Economics.

Col. Ilmar Tamm is the director of the NATO Cooperative Cyber Defence Centre of Excellence. Col. Tamm graduated from the Finnish Military Academy in 1994, served as a signals officer and trained as a staff officer at the Estonian National Defence College. He served on the General Staff of the Estonian Defence Forces as chief of the Communication and Information Systems Department. Col. Tamm was then assigned to the Allied Land Component Command headquarters in Heidelberg and deployed to Afghanistan, where he served in International Security Assistance Force headquarters as chief of operations of the Joint CIS Control Centre. Col. Tamm's awards include the Distinguished Service Cross of the Estonian Defense Forces and the NATO Meritorious Service Medal.

Novak Djordjijevic is an officer in the Serbian Air Force assigned to a fighter squadron as a pilot. He previously worked in the Air Operations Centre and has broad experience in military air operations and civil-military air traffic matters. He is a 2003 graduate of the Program in Advanced Security Studies at the Marshall Center and received a master's degree in information systems from Belgrade University and is currently preparing a doctoral thesis. He has published two books about aviation and developed an Internet site about aviation, science and information technology.

Kenneth Geers (PhD, CISSP), Naval Criminal Investigative Service (NCIS), is a scientist and the U.S. representative to the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia. He has served as an intelligence analyst, a French and Russian linguist, and a computer programmer in support of strategic arms control initiatives.

Dr. Bret Michael is a professor of computer science and electrical engineering at the U.S. Naval Postgraduate School, having previously served in research positions at the University of California at Berkeley, Argonne National Laboratory and Institute for Defense Analyses. As an expert in distributed and high-assurance systems who is also interested in law and policy, he serves as a technical advisor to the group of experts drafting the Tallinn Manual on International Law Applicable to Cyber Conflict. He served three years as an associate editor-in-chief of *IEEE Security & Privacy* magazine and holds a doctorate in information technology from George Mason University in Virginia.

Prof. Thomas Wingfield is a professor of international law at the Marshall Center. He served as the civilian rule of law advisor to COMISAF's Counterinsurgency Advisory and Assistance Team in Afghanistan in 2009 and 2010. He is a former naval officer who has worked in the private sector, think tanks and academia, most recently at the U.S. Army Command and General Staff College. He is a former chairman of the American Bar Association's Committee on International Criminal Law and the author of *The Law of Information Conflict: National Security Law in Cyberspace*. He holds doctorate and master's degrees in international and comparative law from Georgetown University Law Center in Washington.

per Concordiam

Journal of European Security and Defense Issues

Cyber Security
Volume 2, Issue 2

MARSHALL CENTER

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The staff of this security studies institute furthers the vision of the post-World War II Marshall Plan into the 21st century. 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
George C. Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
http://tinyurl.com/per-concordiam-magazine

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

Our lives rely on computers and Internet access. A person uses a computer for everything from communicating through e-mail, chatting and photo sharing to banking, investing, shopping and planning vacations. Governments, militaries, business and national security organizations also depend on computer networks. This reliance of nations on the Internet has drawn attention to a host of security threats in cyberspace. This issue of *per Concordiam* examines the growing concern in Europe and Eurasia about cyberterrorism, cybercrime, and cyber attacks instigated by unknown intruders or hackers using malware, worms, Trojan horses, botnets and zombies against critical computer infrastructure.

This sixth issue of *per Concordiam* starts off with a viewpoint article written by Col. Ilmar Tamm, director of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. He stresses the need for new national and international defensive capabilities to confront an increase in cybercrime and cyber attacks. He argues it is time to change our collective security mind set and start integrating the cyber domain into the national security picture.

The first feature essay is "An Unsettling Trend," which provides a balanced assessment of cybersecurity issues facing the world today. Vytautas Butrimas, the deputy director of CISS in the Ministry of Defense of Lithuania and two-time Marshall Center graduate, describes recent cyber attacks and explains the value of information sharing in trying to pinpoint the source.

The next article is "Stopping Cyberterror" by Dr. Viacheslav Dziundziuk, professor at the Kharkhiv Regional Institute of the National Academy of Public Administration (Ukraine) and a 2008 graduate of the Marshall Center's Program in Advanced Security Studies. As recently as 20 years ago, the prefix "cyber" was relegated to fiction. Such words as cyberspace and cyberterrorism have since entered the modern lexicon. Unfortunately, the same can be said of cyberterrorism. New approaches and methods are required to combat this new form of terrorism. Dr. Dziundziuk discusses the evolution of cybercrime in general, and cyberterrorism in particular, and lists possible ways of countering them.

World leaders fear that cyberterrorism and cyber warfare may pose a serious threat to national security. Unfortunately, cyber attacks and defense often remain a mystery to those lacking an education in computer science or information technology. Kenneth Geers, the U.S. representative to the NATO Cooperative Cyber Defence Centre of Excellence, clearly explains the technical language in the article, "Heading off Hackers." His article simplifies the cyber threat by reducing it to basic concepts and definitions with the goal of aiding strategists working in cyber defense.

In "Strength in Unity," Alexander Klimburg of the Austrian Institute of International Affairs uses a "Whole of Nation" approach to explain the lessons he learned working in cyber security. The four lessons illustrate challenges governments are experiencing in maintaining critical infrastructure protection through cooperation with key private sector companies. Mr. Klimburg concludes that nations need to promote cross-organizational collaboration that includes non-governmental actors.

"Defending Cyberspace," written by Novak Djordjijevic, a Serbian Air Force fighter pilot and Marshall Center graduate, argues that existing computer network protection is too defensive and reactive. When an attack occurs it is almost too late. He explains that cybercriminals face small risks for large benefits, and urges the international community to take a systematic approach to stopping what he considers to be organized crime.

The final feature article, "A New Era of Accountability" is by Dr. Bret Michael, professor of computer science and electrical engineering at the U.S. Naval Postgraduate School, and Prof. Thomas Wingfield, professor of international law at the Marshall Center. They describe the domestic and international challenges of responding to crime and terrorism in cyberspace. Their article describes how anonymity, data encryption and communication platforms make attribution difficult in cyberspace and calls for solutions that take policy, law and technology into account.

The next issue of *per Concordiam* will examine NATO's New Strategic Concept, followed by an issue devoted to the change occurring in North Africa and the Middle East. We invite you and those you know to submit articles on these themes to *per Concordiam*.

We encourage your feedback and look forward to your e-mails in this ongoing dialogue on important security issues. Each issue is available online at the Marshall Center Web site:
http://tinyurl.com/per-concordiam-magazine

- *per Concordiam* editorial staff


THINKSTOCK

per Concordiam magazine addresses security issues relevant to Europe and Eurasia and aims to elicit thoughts and feedback from readers. We hope that the publication of our first five 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.

Send feedback via e-mail to:
editor@perconcordiam.org

ARTICLE SUBMISSIONS

The intent of *per Concordiam* is to be a moderated journal with the best and brightest submitted articles and papers published each quarter. We welcome articles from readers on security and defense issues in Europe and Eurasia.

First, e-mail 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, e-mail 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 approach from the region. We probably won't 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 factcheck 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).

E-mail manuscripts as Microsoft Word attachments to: editor@perconcordiam.org

Merging Cyber with National Security

Military preparation must include defense of computer networks

Col Ilmar Tamm, director of the NATO Cooperative Cyber Defence Centre of Excellence

The evolution and wide accessibility of information technology has brought about a new way to support manipulation and malicious ambitions. The world is witnessing a growing amount of politically motivated cyber incidents relevant to the security of nation-states, including their militaries. From a legal point of view, a cyber attack will invoke a military response if it reaches the threshold of an "armed attack," the equivalent of tanks crossing the border inflicting loss of life and property. Our defense forces are expected to establish deterrence and, when necessary, help the civil authorities defend against cyber threats by functioning in a nonmilitary capacity.

PER CONCORDIAM ILLUSTRATION

With cyber incidents having crossed the threshold of being just ordinary crimes, the use of the term "cyber" with "warfare" is not an "if," but a "when" and a "how" question. Cyber attacks threaten our national attempts to promote and maintain an informed society. They frequently constitute a threat to national security. They have entered the domain of warfare requiring the full attention of our defense forces. These areas are covered by instruments that need to be applied consistently to the whole spectrum of threats. To confront the new threat, we need to learn how to use our existing legal arsenal, including the Geneva Conventions, United Nations Charter and European Union information society directives. We need to understand how to refine our national security strategies to address cyber issues and extend computer security so that it supports national and global security.

We need to understand how to refine our national security strategies to address cyber issues and extend computer security so that it supports national and global security.

To better capture the essence of the cyber domain and how the military fits into it, Scott Borg, director of the U.S. Cyber Consequences Unit, has described the essential differences between cyber defense and industrial defense. According to Borg, cyber defense involves combating networked groups often not clearly connected to nation-states. The opposing force is potentially diffused in multiple jurisdictions around the world. Cyber defenders must respond with ubiquitous force, using informational power over conventional firepower.

Strategically, cyber defense is a lot less about geographical defense perimeters and outside threats. More often, the targets include internal networks and insider attacks. Targets have switched from being military-industrial to privately owned critical infrastructure. In military terms, these are soft targets, but targets of very high value. Cyber attacks are not measured primarily in injuries, death or destruction. Instead, the value of a destroyed information asset is determined by the influence it has on the functioning of a society or a nation, including the military. Nevertheless, cyber attacks could ultimately cause injuries, deaths and destruction.

Furthermore, Borg claims that we have moved from an era of deterrence-based policies to an era of resilience-based policies. I would argue that a good defense concept still produces a great amount of deterrence and conclude that we need to keep both ends in mind when crafting military response plans.

All of these factors affect how decisions are made in developing and sustaining information superiority — a term that comprises the confidentiality, integrity and availability of information in the widest possible sense. The presence of multiple stakeholders ensures that effective control over individual components of the information infrastructure is inherently dispersed. All planning occurs in the context of uncertainty about the identity of the adversary and the difficulties in recognizing patterns and distilling useful information out of noise. Reaction has a different meaning in cyberspace — only technology can keep up with technology, but decision-making remains in the hands of humans.

Asymmetric threats are about unpredictability and targeting the weakest link of the chain. Therefore, the links that have been reinforced based on experience mark just the beginning of defense efforts. Accordingly, to ensure that one's cyber defense is effective, one needs to maintain full awareness of the present danger and threat picture, which for military commanders is a Common Operational Picture, as well as maintain the ability to identify trends using experience and current observations. Consequently, even from the theoretical perspective, preparing against a cyber attack is most challenging. Once you see it coming, your adversary sees you see it coming. Repositioning the attack is significantly easier than repositioning the defense.

As Carl von Clausewitz observed in his famous book *On War*, a general in time of war is constantly bombarded by reports both true and false; by errors arising from fear or negligence or hastiness; by disobedience born of right or wrong interpretations, of ill will, of a proper or mistaken sense of duty, of laziness, or of exhaustion; and by accidents that nobody could have foreseen. In short, he is exposed to countless impressions, most of them disturbing, few of them encouraging. In a cyber conflict, this challenge is exacerbated by the fact that attacks are rather easy to launch, defense is more costly than attack, and states often choose to ignore or even nourish cyber perpetrators in their jurisdiction. Because of our way of life, we are increasingly vulnerable to these attacks without smoking guns. It is time to reset our minds and start integrating the cyber domain into our national security picture and link it with defense capability development. □

An Unsettling Trend

ATTACKS SHOW THE NEED FOR A PROACTIVE DEFENSE STRATEGY IN CYBERSPACE

Vytautas Butrimas, chief adviser, Lithuanian Ministry of National Defense

The 2010 United Nations Internet Governance Forum (IGF[1]) was held in Vilnius, Lithuania. Part of the IGF mandate is to "discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet." The IGF was meeting for the fifth time since 2005. The discussion was mostly set in the context of protecting privacy and freedom of access to the Internet.

Very little attention, however, was given to dealing with several disturbing cyber security events that occurred during the period of the IGF's five-year mandate. In 2007, for example, Estonia's Internet infrastructure was attacked to such an extent that the country was cut off from the Internet. In 2008, Georgia experienced a devastating cyber attack on its information and communications systems that resulted in the isolation of the Georgian government and people from the rest of the world. These attacks resulted in significant violations of privacy and freedom of Internet access, the very things that the IGF seemed so concerned about protecting.

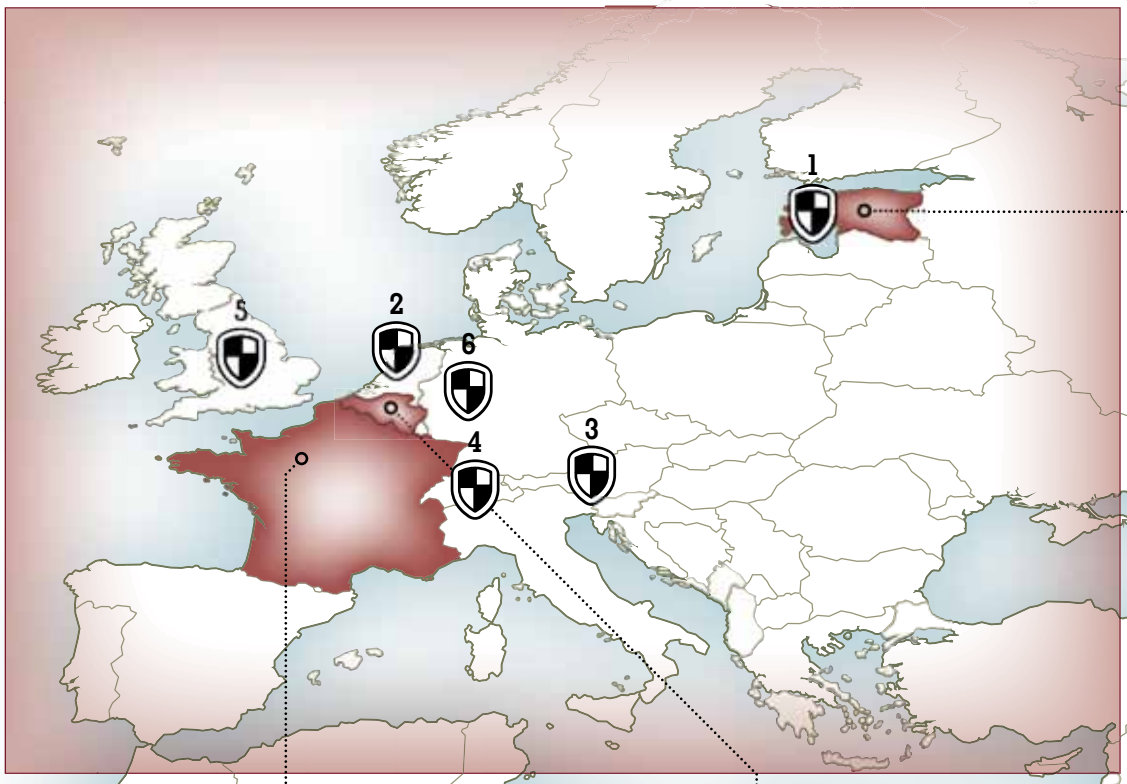
Something serious was going on in cyberspace. Unknown perpetrators were demonstrating sophisticated and effective cyber offensive capabilities against critical communications and information systems, or CCIS. Even more serious was that no one was held responsible for these attacks. This article will provide a brief appraisal of some important cyber events and trends in an effort to achieve a more balanced understanding of the cyber security issues facing the international community today.

MALWARE AND CYBER CRIME

The writing of malware (malicious computer software) and hacking[2] into computer systems is no longer an activity limited to amateurs or hobbyists looking for recognition. It has become a relatively safe and profitable criminal activity. One of the factors allowing for the development of this new growth industry of malware and botnets (robot computer network) is that the Internet or cyberspace is mostly a free and unregulated environment.

Think of it as a road or highway network. However, in this network, there are

Recent Cyber Attacks



Estonia
May 2007

Georgia
August 2008

Paris, France
Cyber attack prior to G-20 summit
December 2010

Brussels, Belgium
Major and widespread cyber attack before a large European Union summit to discuss the economy and the Middle East
March 2011

Iran
Stuxnet
Summer 2010

Sampling of Cyber Defense Agencies

1 **NATO**
Cooperative Cyber Defence Centre of Excellence
CCDCE

2 **The Netherlands**
National Infrastructure Against Cyber Crime
NICC

3 **Austria**
Austrian Program for Critical Infrastructure Protection
APCIP

4 **Switzerland**
Reporting and Analysis Centre for Information Assurance
MELANI

5 **United Kingdom**
Centre for the Protection of National Infrastructure
CPNI

6 **Germany**
National Cyber Defense Center
NCAZ

no rules of the road or police to issue "speeding tickets" or otherwise bring perpetrators to justice. Even if police existed, one would find it almost impossible to give them a description of the perpetrators. The perpetrator has long since left the crime scene, leaving no trace. This is the problem of attribution. It is very difficult to prove who did it. Perhaps the malware and botnet can be identified, but the criminal and his computer are safely hidden.

When Estonia was cyber attacked, its specialists had a gut feeling who was behind it, but finding proof was one of the first problems. The first list of attacking computers were identified in unexpected countries such as Egypt, Vietnam and Peru.[3] Most likely, these computers were part of a botnet controlled by a "herder" who had previously installed his software on poorly secured personal computers throughout the world.

Money can be made by using malware to commit fraud, break into banking systems and take control of people's credit card and banking accounts. Cyber crime is on the rise. A report by the U.S. National White Collar Crime Center noted more than 330,000 cyber crimes in 2009, an increase of 667 percent since 2001.[4]

The malware that can attack and hack into these financial systems has a value much like any commodity. A "herder," or commander, of a botnet makes use of malware to infect and control other computers. Botnets are sold and rented just like any commodity, with prices based on supply and demand.[5] A new industry has therefore emerged as one of the fastest growing sectors in the criminal world. Professional skills are required to hack into a computer and run a botnet. These skills are very much in demand not only in the cyber crime economy but also in government and private sectors.[6]

SOCIAL NETWORKING THREATS

The next trend on the rise is social networking. The Internet has provided new ways for people to stay in touch and share information. Pictures, videos and files can be shared freely, either publicly or with an authorized group. Social networking also lends itself to social activism. On Facebook, for example, there is a section labeled "causes" where interested parties can meet and organize. If you are unable to find a cause, you can search for it or create one. These causes provide possibilities for healthy democratic activism, but what if that activism is destructive?

In one published case,[7] a website called for "volunteers" to fight a cause. Those who wanted to "join the fight" only had to download the provided software and the software would do the rest. In effect, those people allowed their computers to join a botnet.

Social networking offers like-minded people a chance to act together for democracy, but it has a dark side. For example, an individual or group could use these services to raise volunteer armies of cyber warriors. The process is as simple as following written instructions or downloading someone's malware. In 2007, we started to see this in action.

CYBER ATTACKS: ESTONIA AND GEORGIA

The year 2007 marked a watershed in cyberspace. The Estonian example demonstrates that a cyber attack on a nation's infrastructure, initially fueled by a grassroots patriotic base, can later attract professional cyber criminals. It's a potent combination.

On the surface, the cyber attack seemed to be a spontaneous and patriotic Russian reaction to Estonia relocating a statue of a Russian Soldier. However, the attacks showed a degree of organization that was adequate to cripple Estonia's internal networks

TIMELINE

OF COMPUTER AND INTERNET ADVANCES AND SETBACKS


APPLE

1976:
Apple Computer founded, marking the start of the age of personal computers.


WIKIPEDIA

1981:
Microsoft Corp. offers its first computer operating system to the public.

1984:
The European Organization for Nuclear Research (CERN) begins installing a version of the Internet to link its internal computers.

and Internet links temporarily. Targeting and attack information was provided on websites to those who wanted to use their computers to enter the fray. Botnet managers that had used malware to infect unsuspecting computers directed their "zombie" computer armies to "open fire" against listed Estonian banking, government and press sites.

In August 2008, the use of linked computers to temporarily disrupt a nation's CCIS infrastructure took on a new and potentially deadlier form — the execution of a cyber attack during a traditional military operation. It combined several elements used in the Estonian attack a year earlier: grassroots patriotism channeled with the help of social networks, professional botnet herders and elements of organized crime. The result was the execution of a well-planned, well-timed and debilitating cyber attack against Georgian government and civilian CCIS. This attack succeeded in cutting off access to information about what was happening in the country. Daily business was disrupted, and people were fearful and uncertain what would happen next. In short, Georgia's ability to organize and coordinate its national defense was severely compromised.

A study of the cyber attack in Georgia also suggested the appearance of a darker trend — the possibility for physical destruction of critical CCIS components.[8] According to the study, a much more deadly attack could have been executed; however, the perpetrators chose restraint.[9] Unfortunately, the organizers of the attack learned an important lesson: It's still an attractive weapon and nobody has a clue how to deal with it.

THE ASSOCIATED PRESS

The Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, was created by NATO to enhance capability, cooperation and information-sharing among member nations and partners.

STUXNET: FIRST INTERCONTINENTAL CYBER ATTACK?

The appearance of the Stuxnet malware in 2009, and its appearance in the news in the summer of 2010, revealed a new cyber stew combining the ingredients of the cyber professional's skills. Publicly available analysis of Stuxnet indicated that this was a well-researched and sophisticated worm. The worm demonstrated it could not only temporarily neutralize a target, but destroy it physically.

One study suggests[10] that the substantial resources (cyber professionals and intelligence assets) required to deploy this worm could be supplied only by a government. One of the intended Stuxnet targets could have been Iranian nuclear facilities whose supervisory control and data acquisition systems (SCADA[11]), used to manage sensitive operations, were manufactured by Siemens.

THINKSTOCK

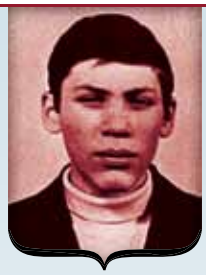
1986:
First case of successful attribution. Astronomer Clifford Stoll uncovers KGB hacking of U.S. SDI data.

ROANOKE COLLEGE

1989:
The firm McAfee Associates markets its first anti-virus software. Internet attracts its first 1,000,000 users.

THINKSTOCK

1991:
World Wide Web (www) formally established.



1994:
Russian hacker Vladimir Levin robs major corporations by breaking electronically into Citibank accounts.

It was difficult to determine if Stuxnet succeeded in performing the destructive task it was designed for. It appeared in other countries and there were no reports about damage to nuclear facilities.

One study concluded that Stuxnet was designed as a psychological weapon and as such was probably successful.[12] Imagine being able to deliver the following message to your adversary: "We don't like what you are doing with this facility, we can control it without your knowledge, and by the way, maybe you should be careful about pushing buttons." As with previous cyber events, the organizers of Stuxnet remain unknown. There may be no "smoking gun," but there is "blood in the water."[13] If Stuxnet and its variants are a new form of cyber attack, this represents a new trend and deeper problem.

BURMA'S ELECTORAL ATTACK

Burma, in the first week of November 2010, was preparing for its first national elections in 20 years. The elections received plenty of press coverage, but one event almost went unnoticed. One week before the elections, Burma CCIS infrastructure suffered a massive distributed denial-of-service[14] attack, effectively cutting Burma off from the Internet. One can only speculate on what effect this attack had on the Burmese elections. In cyber security terms, however, this attack demonstrated a disturbing escalation in cyber attack capabilities. The attack against Burma was several times more massive than the attacks against Estonia and Georgia.[15] This increase in "cyber power" constitutes a troubling trend.

CONCLUSIONS

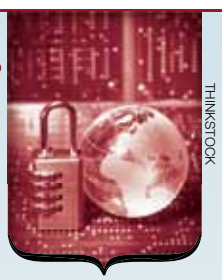
The state's dependence on CCIS and its vulnerability to disruption or destruction via malware sent from unknown locations by unknown perpetrators has created a new and attractive form of attack. Such an attack is attractive especially for governments unable to achieve a foreign policy objective using internationally acceptable means.

This Internet option provides so many levels of application that it is too tempting for a state not to use. It can be employed clandestinely through third parties with the assurance of nearly 100 percent deniability, regardless of whether the attack becomes publicly known. Harm can be limited to just short-term disruption or expanded to damage CCIS physically. The "commanders" of these arsenals are hidden but are reachable by those interested in employing their services. One can harp on the fact that there is no "smoking gun" proving government involvement but circumstantial evidence can build a good case that governments are involved to some degree.

To the extent that botnets and malware can disrupt the state's critical CCIS infrastructure, the cyber threat is a national security issue. This is recognized by nations dependent on the Internet and those seeking to take advantage of that vulnerability. In recognition of the threat, governments are beginning to cooperate in fighting cyber crime. However, many are also competing in a cyber arms race.[16]

Industry can inadvertently make it easier to mount cyber attacks. For example, Microsoft Corp. announced it had signed a Government Security Cooperation Agreement with Russia that, among other things, provided access to the Windows operating system source code.[17] The company signed the same agreement with China in 2007[18] and, this past summer, provided the Russian government with access to the code of the latest Windows operating system. One can perhaps understand the marketing and sales motives behind Microsoft's actions, but it's not hard to understand that if the code falls into the wrong hands it could be used to find weaknesses and new attack vectors for exploitation.

How can we address this new threat to national security and avoid a possible cyber arms race? For starters, government and industry need to understand their dual roles in being part of the solution and part of the problem. Restraint within the framework of a "cyber arms control treaty" could be considered. Treaties, however, need to be verifiable and enforceable to be effective. Principal stakeholders among



1995:
The Strano Network becomes one of the first "hacktivist" groups when it attacks French government computers.

1996:
Finland's Nokia launches the first cell phone with Internet connectivity.

1998:
Google establishes its first search engine.

2000:
10 million Internet domain names registered up to this point. The Love Bug "worm" from the Philippines corrupts computers worldwide.

the public and private sectors and international community need to be identified, and appropriate coordination instruments need to be applied. The objective would be the creation of an intelligence-gathering and communications network that would allow for the exchange of information leading to the identification of cyber criminals and attack organizers. This means coming up with a reliable solution to the problem of attribution. If it is possible to pin down who is attacking then perhaps those gray commanders would be forced to weigh the costs and benefits of an attack. Once the organizers of the attacks have been identified, an international instrument needs to be on hand to ensure enforcement and punishment, if necessary.

Call it an Internet police[19] force, if you will. Nations must hold service providers and individuals accountable for their actions. If they do not agree to act on information, sanctions should be applied. We must raise the price for those wishing to organize cyber attacks.

International action will take time, but a step can be taken now at the local level: creating a cyber specialist contact network composed of all sector players (government, the private sector, banking, energy, transportation, commercial interests and telecommunication). Government must lead, since it should naturally be concerned with developing a national cyber security strategy.

This league of experts representing all cyber security stakeholders could be the first national line of cyber defense. The contacts forged during meetings and consultations will increase trust among stakeholders to share information and expertise that can be tapped during a cyber emergency. Memorandums of understanding for cooperation among stakeholders would allow for a more coherent and coordinated response to incidents.

One should not wait for a crisis and respond to it *ad hoc*. In May 2007, at a joint NATO-Microsoft workshop on cyber security held in Redmond, Washington, the Estonian representative came to the podium and announced "my country is under cyber attack." After a night of phone calls to capitals, offers of help eventually came but everything was done impromptu. Since then, some progress has been made beyond the *ad hoc* approach to cyber crisis management.

Cyber security and the Internet are at a crossroads. The way we deal with cyber security today will determine not only the extent to which privacy and freedom of access will be preserved but the security of our CCIS as well. It is not enough, however, to concentrate on cyber crime or restricting terrorists use of the Internet for information or recruitment purposes. To paraphrase Sun Tzu, the enemy (as well as ourselves) must be fully understood if we are to prevail. □

1. http://www.intgovforum.org/cms/aboutigf
2. People committed to circumvention of computer security. This primarily concerns unauthorized remote computer break-ins via a communication networks such as the Internet (Black hats), but also includes those who debug or fix security problems (White hats), and the morally ambiguous Grey hats. http://en.wikipedia.org/wiki/Hacker_(computing)
3. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired magazine, Issue 150 2007-08-21. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all#ixzz0mIn5gsPQ
4. 2009 Internet Crime Report, NWCCC and US DoJ, p.15, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
5. http://www.businesscomputingworld.co.uk/botnets-for-rent-explained/ and http://www.net-security.org/secworld.php?id=4002
6. "Marc Maiffret: The quick rise of a teen hacker," http://news.cnet.com/8301-27080_3-20002317-245.html?tag=mncol
7. Gunter Ollmann, Damballa "The Opt-In Botnet Generation," p. 13., 2010. http://www.damballa.com/downloads/r_pubs/WP_Opt-In_Botnet.pdf
8. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." p. 5, 2009 U.S. Cyber consequences Unit, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf
9. Ibid. p. 5.
10. Preliminary Stuxnet report ver. 1, p. 16., The cybersecurity forum initiative, 2010 http://www.csfi.us/
11. SCADA – supervisory control and data acquisition, http://en.wikipedia.org/wiki/SCADA
12. Preliminary Stuxnet report ver. 1, p. 16., The cybersecurity forum initiative, 2010 http://www.csfi.us/
13. http://www.zdnet.com/blog/security/metasploit-and-scada-exploits-dawn-of-a-new-era/7672?tag=nl.e589
14. Distributed Denial of Service (DDOS)
15. Craig Labovitz "Attack Severs Burma Internet," November 3rd, 2010, Arbor Networks. http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/
16. Jim Wolfwed, "China aims to top U.S. in cyberspace," U.S. general, International Business Times, 13 June 2007 http://www.ibtimes.com/articles/20070613/china-internet.htm
17. Tom Espiner, ZDNet UK, 8 July, 2010 "Microsoft opens source code to Russian secret service" http://www.zdnet.co.uk/news/security/2010/07/08/microsoft-opens-source-code-to-russian-secret-service-40089481/
18. AsiaInfo Services 08-07-2007, "Microsoft signs new open source code agreement with China," www.highbeam.com/doc/1P1-142370666.html
19. "Where are the Internet police?" Data Center Times, 2009-03-03, http://www.datacentertimes.com/view_article.php?a_id=64&PHPSESSID=f134dc43445920bfdf69622e2c0b3cee


AGENCE FRANCE-PRESSE

2001:
Scottish hacker Gary McKinnon breaks into dozens of defense computers in what is called "the biggest military computer hack of all time."


THINKSTOCK

2007:
Web users exceed 1 billion mark worldwide.

2009:
Chinese computer spying operation dubbed Ghostnet discovered infiltrating machines in more than 100 countries.

2011:
"Anonymous" group hacks Sony and Bank of America servers, exposing confidential information to the public.

Stopping Cyberterror

COUNTRIES MUST WORK TOGETHER TO THWART EFFORTS OF INTERNET CRIMINALS

Dr. Viacheslav Dziundziuk, professor, Kharkhiv Regional Institute of the National Academy of Public Administration (Ukraine)

PER CONCORDIAM ILLUSTRATION

Cybercrime encompasses crimes in the so-called "virtual space." Virtual space (or cyberspace) may be defined as a computer-modeled information space containing information about individuals, subjects, facts, events, phenomena and processes presented in a mathematical, symbolic or any other form and circulating in local or global computer networks, or data contained in the memory of any physical or virtual device or any other medium specifically designed to store, process and transmit those data.[1]

In contrast to traditional types of crimes whose history goes back many centuries, such as murder or theft, cybercrime is a relatively recent phenomenon that appeared with the creation of the Internet. It bears mentioning that the very nature of the Internet is conducive to committing crimes. Its global reach, ability to transcend borders and reach a broad audience, anonymity of its users, and distribution of major network nodes and interchangeability create advantages for criminals and allow them to hide effectively from law enforcement agencies.

The first computer criminals, later called "hackers," appeared in the 1970s. It's difficult to say exactly who the first hacker was, but most sources cite John Draper as the first professional hacker. He also created the first hacker specialty — "phreakers," from "phone hacker." Among the ranks of the hackers of the time were such well-known figures as Steve Wozniak and Steve Jobs, who would later go on to found Apple Inc. *Phreakers set up the production of devices to intrude into home telephone networks. This period can be considered the beginning of the development of computer crime.*

The first widely publicized arrest of an Internet criminal occurred in 1983 in the city of Milwaukee in the United States. The case was the first recorded Internet hack, committed by six teenagers who called themselves the "414 Group" (414 was the Milwaukee area code). Over nine days they hacked into 60 computers, some of which belonged to Los Alamos National Laboratory. After the arrest, one group member testified against the others, who received suspended sentences.[2]

The very nature of the Internet is conducive to committing crimes.

In the 1980s, we began to see a major increase in computer attacks. For example, although Internet users made only six complaints of computer attacks to the CERT Internet security center in 1988 (the year the center opened), there were 132 complaints in 1989, and 252 in 1990. Cybercrime was no longer a rarity. Large hacker groups were coming on the scene, and the Internet began to be used to commit a wider range of crimes. *This was the beginning of the second phase of the development of cybercrime, characterized by new areas of specialization for Internet criminals.*

In 1984, Fred Cohen published information about the development of the first malicious self-replicating computer programs and used the term "computer virus" to describe them. He also wrote a program that demonstrated the possibility of one computer infecting another.

In 1986, a member of the group "Legion of Doom," Loyd Blankenship, known as "Mentor," was arrested. During his incarceration, he wrote the famous "The Hacker Manifesto."[3] The ideas espoused in this manifesto are considered to this day to underlie the hacker ideology and culture and are widely distributed throughout the Internet. Clearly, a quantitative rise in cybercrimes coincided with the increased popularity of hacker ideas in the computer world, which attests to the interconnection between these phenomena.

In 1994, the world learned of the Vladimir Levin case, categorized by investigators as a "transnational computer network crime." An international criminal group of 12 people using the Internet and the Sprint/Telenet data transmission network breached a protection system and attempted to make 40 transfers totaling $10.7 million from the accounts of bank clients in nine countries to accounts in the United States, Finland, Israel, Switzerland, Germany, Russia and the Netherlands.[4] This was the first major international financial crime using the Internet to become known to the general public. It demonstrated that cybercrimes can cause serious financial damage. In 1998, a 12-year-old hacker penetrated the computer system controlling the floodgates of the Theodore Roosevelt Dam in Arizona. Opening the dam's water-release gates could have inundated the U.S. cities of Tempe and Mesa, Arizona, which had a population of more than 1 million.[5] This incident gave rise to such terms as "Internet terrorism," "computer terrorism" and "cyberterrorism." It also demonstrated that the Internet itself is most vulnerable to cyber attacks, as its key components are accessible from anywhere in the world. This fact does not escape the attention of hackers.

The Internet itself is most vulnerable to cyber attacks, as its key components are accessible from anywhere in the world. This fact does not escape the attention of hackers.

THE INTERNATIONAL THREAT

The emergence of cyberterrorism and highly publicized cases of crime by international groups provide evidence that cybercrime is now transnational. This represents the beginning of the third phase in the evolution of cybercrime.

It is alarming that with the development of the Internet, serious consequences can ensue, not only from intentional cyber attacks but also from the carelessness of professionals. For example, in 1997, a mistake by an employee of Network Solutions resulted in sites with names ending in .net and .com becoming inaccessible. That is, the operation of the entire World Wide Web was disrupted owing to the carelessness of a single individual.

At the same time, cyber attacks are becoming a means to achieving political ends. A typical example is Internet stoppage in which perpetrators simultaneously log onto a site, connect to a server, send an e-mail or make postings to forums in order to limit or even deny access to the site by other users. The Internet site or server is overwhelmed by access requests, causing an interruption or complete stoppage.

The first such attack was carried out by a group calling itself the "Strano Network," protesting against the French government's nuclear and social policies. In the course of one hour, on December 21, 1995, the group attacked the sites of various government agencies. Group members from around the world were instructed to use their browsers to visit government sites simultaneously. As a result, some sites were indeed shut down for a time.[6]

The transnational aspects of cybercrime continue to manifest themselves more widely. The conflict in Kosovo can be considered the first Internet war, in which various groups of computer activists used the Internet to condemn actions of both Yugoslavia and NATO, and in doing so, intentionally impeded the operation of government computers and gained control over sites. This was followed by a "deface," a change in the site's content. At the same time, stories about the dangers and horrors of the war, as well as facts and opinions of political leaders and public figures, circulated through the Internet. This served as propaganda to a wide audience throughout the world.[7] All this is characteristic of the third phase of the development of cybercrime.

It should be noted that today practically any military or political conflict is accompanied by organized opposition on the Internet. For example, in 2005, there was a wave of cyber attacks prompted by a school history textbook issued in Japan that presented a distorted account of events in China from 1930 to 1940 by ignoring war crimes committed by Japanese forces during the occupation. Among the targets of the attacks were Japanese ministries and agencies, sites belonging to large Japanese corporations, and sites devoted to World War II. In this case, the Chinese hackers displayed a high degree of organization, as evidenced by the synchronicity and massive nature of their attacks. Considering that the state controls the Internet in China, this attack was presumably sanctioned by the government. *The use of cyber attacks for political ends may be considered the beginning of a fourth phase in the development of cybercrime.*

The China example was copied by Russian hackers who carried out several large-scale distributed denial of service attacks. Estonian government sites were attacked over a period of a few days in late April and early May of 2007. A youth movement called "Nashi"[8] claimed responsibility. And in August 2009, the U.S. publication *Aviation Week* accused Russian hackers of attacking the server for the Baku-Tbilisi-Ceyhan pipeline. The publication stated that the attacks were carried out from the same addresses as the attacks on the Estonian sites.[9]

CHARACTERISTICS OF CYBERTERRORISM

Today's terrorism is international and, in accordance with a number of international norms, is considered to be an international crime. This is certainly the case for a new manifestation of terrorism — cyberterrorism.

It bears noting that the media often use the term "cyberterrorism" incorrectly, confusing the concept by conflating the terms "hacker" and "cyberterrorist." This, however, is incorrect. Terrorism is a crime, but not every crime is terrorism. Not every hacker commits terrorist acts in cyberspace.

The term "cyberterrorism" was presumably coined in 1997. In that year, FBI special agent Mark Pollitt defined it as "the premeditated politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[10]

Renowned information security expert Dorothy Denning refers to cyberterrorism as "unlawful attacks and threats of attack against computers, networks and information stored therein … to intimidate or coerce a government or its people in furtherance of political or social objectives."[11]

Researchers Matthew Devost, Brian Houghton and Neal Pollard define information terrorism (cyberterrorism being a subcategory) as:

1. The combination of criminal use of information systems via fraud or misuse and physical violence that is characteristic of terrorism.
2. The conscious misuse of digital information systems, networks or components of those systems or networks for purposes that facilitate carrying out terrorist operations or acts.[12]

Three kinds of cyberterrorism can be identified:

1. The commission of terrorist acts using computers and computer networks (terrorism in its "pure form").
2. The use of cyberspace to further the aims of terrorist groups but not directly for the commission of acts of terrorism (on this count former CIA Director George Tenet stated that terrorist groups, including Hezbollah, Hamas, Abu Nidal and al-Qaida are very actively using computer capacities to manage their activities).[13]
3. The commission of acts in cyberspace that do not further political aims but do present a threat to national or public security.

The first kind of cyberterrorism may be defined by combining the concepts of "cyberterrorism" and "cyberspace."

From this it follows that cyberterrorism may be understood as an intentional, politically motivated attack on computer-processed information, a computer system, or a network that jeopardizes the life and well-being of people or involves other serious consequences, if such actions were committed for the purpose of disrupting public safety, intimidating the population or provoking a military conflict. This also includes intimidating the population or government authorities for the furtherance of criminal ends. The latter kind may manifest itself as a threat of violence, maintaining a permanent state of fear in order to achieve political or other ends, coercion, or drawing attention to an individual cyberterrorist or terrorist organization that the cyberterrorist represents. In this case, causing harm or threatening to cause harm serves as something of a warning of the possibility of more serious consequences if the cyberterrorist's conditions are not met.

As for the second kind of cyberterrorism, it may be noted that it is debatable whether the use of cyberspace by a terrorist organization to carry out or publicize its activities but not to commit terrorist acts directly can be regarded as cyberterrorism. Of course, such actions can hardly be qualified as terrorism under criminal law, but nonetheless it seems reasonable to call such actions, cyberterrorism, and apparently this will be done in the near future. This type of cyberterrorism may include such things as:

- Using the Internet to collect detailed information about possible targets, their location and characteristics.
- Creating sites containing detailed information about terrorist movements, their aims and purposes; publishing on those sites information about times and places for meeting people interested in supporting terrorists; information about forms of protest and so forth, that is, synergistically acting upon groups that support terrorists.

THE ASSOCIATED PRESS

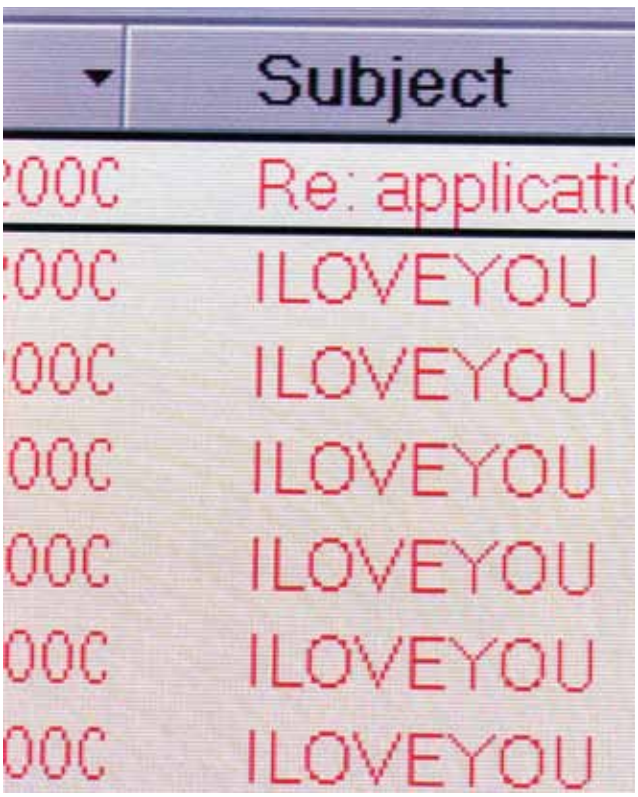
Scottish computer hacker Matthew Anderson appears outside a London courthouse in November 2010. Anderson admitted being a key member of an international gang of hackers who targeted hundreds of businesses with spam.

THE ASSOCIATED PRESS

Briton Gary McKinnon leaves a courtroom in London after facing a hearing for his extradition to the United States in 2005. McKinnon was accused of hacking into U.S. military computers.

- Using the Internet to address a mass audience to report on future or planned actions on the pages of sites or mass e-mailing of similar messages. This includes terrorists using the Internet to publicly claim responsibility for the commission of terrorist acts.
- Using the Internet for informational or psychological effect, including the initiation of "psychological terrorism." The Internet can be used to sow panic, to mislead or for destruction. The World Wide Web provides an abundance of means to spread rumors, including disquieting ones, and this capacity is used by terrorist organizations.
- Raising funds to support terrorist movements.
- Extorting money from financial institutions to spare them from acts of cyberterrorism and damage to their reputation.
- Drawing unsuspecting accomplices into terrorist networks — for example, hackers who do not realize where their actions may ultimately lead. Also, if in the past terrorist networks were usually built around a far-flung structure with a strong center, nowadays they are networks without clearly discernible command points. This is one advantage the Internet provides.
- Setting up Internet sites with a terrorist orientation that contain information about explosives and explosive devices, toxins, and poisonous gases and how to produce them. In the Russian-language segment of the Internet alone there are dozens of sites where one can find such information.
- Using the Internet for communications, and in particular using e-mail or electronic billboard services to send encoded messages. For example, Ramzi Yousef, who organized the bombing of the World Trade Center, received instructions on arranging acts of terrorism via encoded messages sent directly to his laptop. Other terrorist groups, the Black Tigers (a wing of Sri Lanka's defeated separatist Liberation Tigers of Tamil Eelam) for instance, attacked government websites and e-mail addresses.
- Relocating training bases for terrorist operations. Terrorism is no longer confined to the territory of the state in which the terrorists are hiding. Moreover, terrorist training bases are, as a rule, no longer located within the same countries as the terrorists' targets.[14]

As for the third kind of cyberterrorism, actions that may be committed by hooligans and are not aimed at achieving political objectives, but nonetheless may constitute a threat to public and/or national security, can also be regarded as terrorism. This category of cyberterrorism might include intentionally spreading viruses, "Trojan horse" programs, "worms" and so forth, or intruding into and paralyzing the operation of government or other public institutions.



THE ASSOCIATED PRESS

A computer screen in Frankfurt, Germany, shows an e-mail inbox jammed with the powerful "I Love You" virus, which struck global communications systems and crippled government and corporate computer networks in 2000.

THE "I LOVE YOU" VIRUS

A computer virus known as "I Love You" (or the "Love Bug") was launched on the Internet on May 1, 2000, in Asia and spread throughout the planet with astonishing speed. It disrupted the operation of government institutions, parliaments and corporations in many countries, corrupting about 45 million computer networks. For example, in the U.S., this computer virus struck the networks of 14 federal agencies, including the CIA, the Department of Defense, the White House and Congress.[15] It also damaged the British Parliament's network. Altogether, in the first five days after its appearance, it caused material damage totaling $6.7 billion. Thus, it is not surprising that the Computer Economics group assessed the "I Love You" virus as an act of cyberterrorism.

Also in May 2000, Franklin Adams of Houston, in the United States, was convicted of spreading a "worm" that affected computers whose modems were programmed to automatically dial the emergency phone number 911. This resulted in several thousand computers in hospitals, police departments and fire departments being put out of commission, which obviously caused a threat to public security.

An analysis of worldwide trends in the development of cyberterrorism makes it possible to project with a high degree of probability that the threat will continue to increase every year. Technical progress is advancing so swiftly that society is too late to grasp some of its implications, and correcting the situation requires significant effort. In addition, dependence on computer systems and information technologies grows constantly.

Thus, it can be stated that cyberterrorism is a serious threat to humanity, comparable to nuclear, biological and chemical weapons, though because of its recent emergence the degree of the threat is not yet fully recognized and studied. The world community's experience in this area is obvious evidence of the undeniable vulnerability of all countries, especially considering that cyberterrorism does not respect national borders and that a cyberterrorist can threaten information systems located practically anywhere in the world. And finding and neutralizing the cyberterrorist is exceedingly difficult owing to the dearth of clues left behind, in contrast to the real world, where evidence of crime is sometimes easier to collect.

SOLUTIONS IN FIGHTING THE CYBER WAR

All of this requires organizing a broad range of efforts to combat cyberterrorism and cybercrime in general. These efforts may be applied in several areas:

- **Legislative** — Something has been, and continues to be done, in this regard. For instance, national legislatures have adopted specialized laws concerning computer and Internet crime; moreover, legislation in the area of computer crime is becoming a field in and of itself, with ever stricter sanctions against crimes. As time goes by, international legal acts are regulating relations within the Internet and are aimed at countering cybercrime, in particular the European Convention on Cyber Crime. Further refinement of laws, primarily international laws, in the area of combating cybercrime will undoubtedly be a means of fighting this phenomenon.
- **Organizational** — This implies that states organize and cooperate effectively with other states, their law enforcement agencies and special services, and international organizations tasked with combating cyberterrorism and transnational computer crime. There is also a need to create a single international organization, patterned after Interpol, that would exclusively fight cybercrime. A number of countries are already cooperating, but it needs to be expanded and qualitatively improved.
- **Technological** — There is no question that improvements in technologies for protecting society from cybercrimes and responding to them are an important direction in which to move, since this makes it possible to prevent criminals from achieving their objectives, if not from actually committing crimes. Effective partnerships between government institutions and private companies working in high-tech and software development, as well as individual computer technology experts, may help to develop such technologies. This kind of joint effort will enable us to stay ahead of the game rather than being in reaction mode.

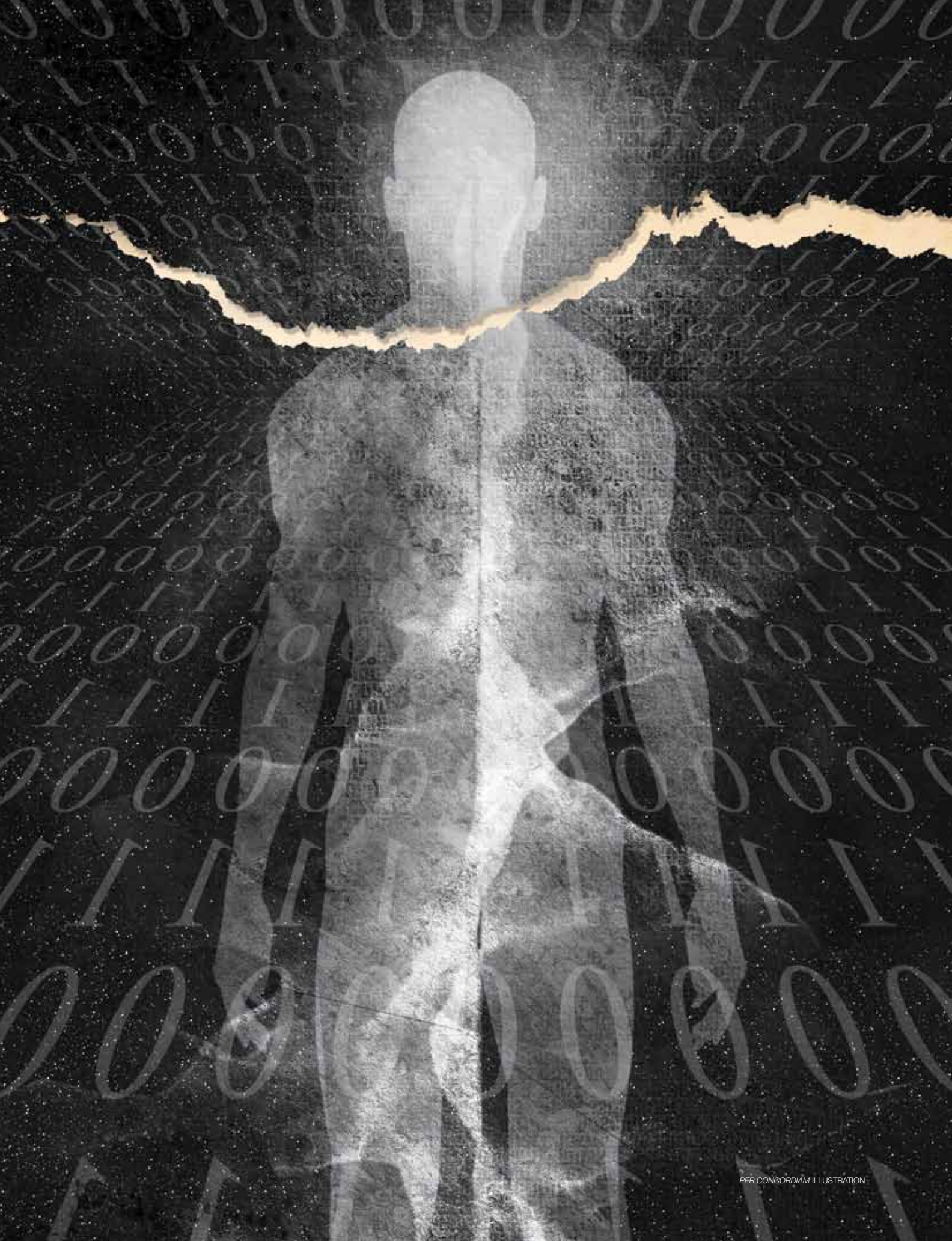
All three of the directions outlined above are important and can deliver substantial success in the fight against cybercrime. In principle, some work is being done in these areas. But, paradoxically, implementing these efforts helps to facilitate those very characteristics of cyberspace that make it possible to commit cybercrimes: global reach, accessibility and constant development of technology. However, there is another avenue of action that, in my opinion, is not being given sufficient attention by government bodies. That is decreasing the base of cybercrime, i.e., the number of people who commit cybercrimes. This could be done through focused reorientation of their values. But this area of endeavor requires specific consideration that is beyond the scope of this article.

Today practically any military or political conflict is accompanied by organized opposition on the Internet.

Thus it may be stated that, unfortunately, the development of computer and telecommunications networks, primarily the Internet and the social interactions that arise from it, can be characterized by a constant increase in the number of criminal deeds and other socially dangerous acts in cyberspace. And the high social cost of these acts is primarily due to their transnational nature because the consequences may involve an unlimited number of individuals in the most widespread countries.

Considering this global negative trend, a variety of decisive measures are needed to counter and prevent cyberthreats, bearing in mind the penetration of the Internet and the "virtual world" into all spheres of life. This should become the main thrust of efforts to ensure information security as well as national security in general. □

1. Golubev, V. A., "'Cyberterrorism' – Myth or Reality?" http://www.crime-research.org.
2. Lukatskiy, A. [Лукацкий. А.], "Hackers Are Running the Reactor," Computer Crime Research Center. http://www.crime-research.org/library/Lukac0103.html.
3. Mentor, "Hacker Manifesto," January 8, 1986. http://project.cyberpunk.ru/idb/hacker_manifesto.html.
4. Kurakov, L. P., Smirnov, S. N., Information as an Object of Legal Protection, Moscow: Helios, 1998, p. 220–221.
5. Robert Lemos, "Cyberterrorism: The Real Risk," Computer Crime Research Center. http://www.crime-research.org/library/Robert1.htm.
6. Denning, D., "Activity, Hactivity and Cyberterrorism: The Internet as a Means of Influence on Foreign Policy," Vladivostok Center for the Study of Organized Crime, translated by T. L. Tropina. http://www.crime.vl.ru/index.php?p=1114&more=1&c=1&tb=1&pb=1.
7. Andreyev, A., Davydovich, "On Informational Opposition During the Military Conflict in Kosovo," PSY-FACTOR Center for Practical Psychology. http://www.psyfactor.org/warkosovo.htm.
8. See: http://www.lenta.ru/news/2009/03/12/confess.
9. See: http://www.securitylab.ru/news/384118.php.
10. Rrasavin S., "What is Cyber-terrorism?" http://rr.sans.org/infowar.
11. Denning D. E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." http://www.nautilus.org/ info-policy/ workshop/ papers/ denning.html.
12. Thomas, Timothy L., Deterrence of Asymmetric Terrorist Threats which Society Faces in the Information Age, International Society Against the Globalization of Crime and Terrorism, international conference proceedings, Moscow, 2002, p. 165.
13. Ronald L. Dick, Issue of Intrusions into Government Computer Networks. http://www.fbi.gov/congress/congress01/rondick.htm.
14. Thomas, Timothy L., Deterrence of Asymmetric Terrorist Threats which Society Faces in the Information Age, International Society Against the Globalization of Crime and Terrorism, international conference proceedings, Moscow, 2002.
15. Ronald L. Dick, Issue of Intrusions into Government Computer Networks. http://www.fbi.gov/congress/congress01/rondick.htm.



PER CONCORDIAM ILLUSTRATION

HEADING OFF HACKERS

CRIMINALS WIELD COMPUTERS AS CHEAP, ANONYMOUS WEAPONS

KENNETH GEERS
U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

The Internet has changed almost all aspects of human life, including warfare. Every political and military conflict now has a cyber dimension whose size and impact are difficult to predict.

Computers and computer networks have provided a new delivery mechanism that can increase the speed, diffusion and significance of a national security threat. The constant evolution of information technology tends to leave both cyber law and cyber defense breathless. The ubiquity and amplification power of the Internet often make the battles fought there seem more important than events taking place on the ground.

The intangible nature of cyberspace, however, can make the calculation of victory, defeat, and battle damage a highly subjective undertaking. Even knowing whether one is under cyber attack can be a challenge.

National security thinkers are therefore struggling with the complexities of cyber conflict for a wide variety of reasons, including an ignorance of its technical foundations, media-fueled paranoia, and a desire to take advantage of hacking's high return-on-investment before it goes away.

This article seeks to articulate cyber warfare in basic concepts and definitions, enhancing the discussion on cyber defense strategies and tactics.

History

What military officers refer to as the "battlespace" grows more difficult to define and defend over time. Advances in technology are normally evolutionary, but they can be revolutionary, such as when artillery shells reached over the front lines of battle and rockets and airplanes crossed national boundaries. Today, cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity.

In 1965, Gordon Moore correctly predicted that the number of transistors on a computer chip would double every two years. There has been similar growth in almost all aspects of information technology, including the availability of practical encryption, user-friendly hacker tools, and Web-enabled open source intelligence, or OSINT.

Every political and military conflict now has a cyber dimension whose size and impact are difficult to predict.

To achieve their objectives, political and military strategists now use and abuse computers, databases and the networks that connect them. In the early 1980s, this concept was already known in the Soviet Union as the Military Technological Revolution. Following the 1991 Gulf War, the Pentagon's Revolution in Military Affairs was almost a household term.

Cyberspace as a war-fighting domain currently favors the attacker, which stands in contrast to our historical understanding of warfare, whereby the defender normally enjoys a significant home field advantage. Further, the terrestrial proximity of adversaries is unimportant because in cyberspace everyone is a next-door neighbor. And there is little moral inhibition to computer hacking because it relates primarily to the use and abuse of computer code. So far, there is little perceived human suffering.

In spite of these advantages for the attacker, many analysts remain skeptical of the seriousness of the cyber threat. In part, this is because a real-world outcome is not guaranteed. In cyber warfare, tactical victories amount to a successful reshuffling of the bits — also known as ones and zeros — inside a computer. At that point, the attacker must wait to see if the intended real-world effects occur.

Motivations for hacking

Experts cite five main reasons for hacking:

• **Vulnerability:** Flaws in the Internet's design allow hackers to secretly read, delete or modify information stored on or traveling between computers. The rapid proliferation of Internet technologies makes it impossible for defenders to keep up with all of the latest attack methods. There are about 100 additions to the Common Vulnerabilities and Exposures, or CVE, database each month. In short, hackers have more paths into a network than its system administrators can protect.

• **Return on investment:** This applies to government, civil society and individuals. A hacker's goals are self-explanatory: the theft of research and development data, eavesdropping on sensitive communications, and the delivery of propaganda behind enemy lines. The elegance of computer hacking lies in the fact that it can be attempted for a fraction of the cost (and risk) of any other information collection or manipulation strategy.

• **Inadequate cyber defense:** Computer network security is still an immature discipline. Traditional security skills are of marginal help in cyber warfare, and it is difficult to retain personnel with marketable technical expertise. Challenging computer investigations are further complicated by the international nature of the Internet. And in the case of state-sponsored cyber operations, law enforcement cooperation is naturally nonexistent.

• **Plausible deniability:** The mazelike architecture of the Internet offers a high degree of anonymity to cyber attackers. Smart hackers route their attacks through countries where the victim's government has poor diplomatic relations or no law enforcement cooperation. Even successful cyber investigations often lead only to another hacked computer. Governments today face the prospect of losing a cyber conflict without even knowing the identity of an adversary.

• **Empowerment of nonstate actors:** The Internet era offers vastly increased participation on the world stage. Governments would like to control international conflict, but globalization and the Internet have considerably strengthened the ability of anyone to follow current events, and have provided a powerful means to influence them. Transnational subcultures now coalesce online, sway myriad political agendas, and do not

AGENCE FRANCE-PRESSE

The computer hacker known as "Mafiaboy," accused of disrupting traffic over the Internet, leaves court following his trial in Montreal in 2001.

AGENCE FRANCE-PRESSE

A man walks inside the Pionen White Mountains high-security computer storage facility of Swedish Internet service provider Bahnhof in Stockholm. The Pionen data center, once a Cold War era nuclear bunker, is one of the most well-protected in the world.

report to a chain of command. A future challenge for world leaders is whether their own citizens could spin delicate international diplomacy out of control.

Hacker targets

There are three basic types of cyber attack, from which all others derive:

• **Confidentiality**: This encompasses any unauthorized acquisition of information, including via "traffic analysis," in which an attacker infers communication content merely by observing communication patterns. Because global network connectivity is currently well ahead of global network security, it can be easy for hackers to steal enormous amounts of information.

Cyberterrorism and cyber warfare may still lie in our future, but we are already living in a golden age of cyber espionage. The most famous case to date is "GhostNet," investigated by Information Warfare Monitor, in which a cyber espionage network of more than 1,000 compromised computers in 103 countries targeted diplomatic, political, economic and military information.

• **Integrity:** This is the unauthorized modification of information or information resources such as a database. Such attacks can involve the "sabotage" of data for criminal, political or military purposes. Cybercriminals have encrypted data on a victim's hard drive, and then demanded a ransom payment in exchange for the decryption key. Governments that censor Google results return part, but not all, of the search engine's suggestions to an end user.

• **Availability:** The goal here is to prevent authorized users from gaining access to the systems or data they require to perform certain tasks. This is commonly referred to as a denial-of-service (DoS), and encompasses a wide range of malware, network traffic or physical attacks on computers, databases and the networks that connect them.

In 2001, "mafiaboy," a 15-year-old student from Montreal, conducted a successful DoS attack against some of the world's biggest online companies, likely causing over $1 billion in financial damage.

Hacker goals

A cyber attack is not an end in itself, but an extraordinary means to a wide variety of ends, limited primarily by the imagination of the attacker.

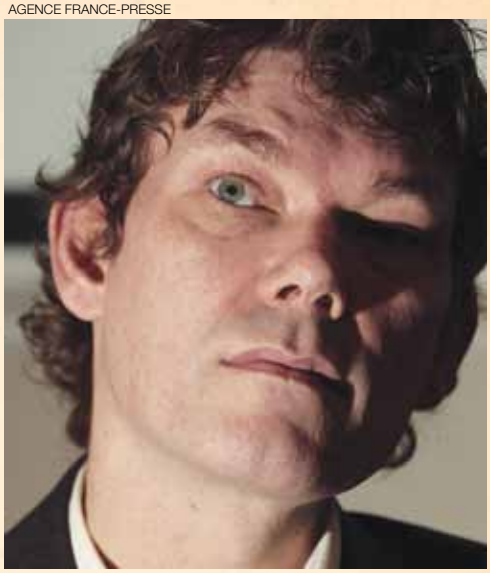
• **Espionage:** Every day, anonymous computer hackers steal vast quantities of computer data and network communications. In fact, it is possible to conduct devastating intelligence-gathering operations, even on highly sensitive political and military correspondence, remotely from anywhere in the world.

• **Propaganda:** Cheap and effective, this is often the easiest and most powerful form of attack. Digital information in text or image format — regardless of whether it is true — can be instantly copied and sent anywhere in the world, even deep behind enemy lines. And provocative information that is censored from the Web can reappear in seconds elsewhere.

• **Denial-of-service (DoS):** The simple goal is to deny the use of data or computers to legitimate users. The most common tactic is to flood the target with so much superfluous data that it cannot respond to real requests for services or information. Other DoS attacks include the

AGENCE FRANCE-PRESSE

AGENCE FRANCE-PRESSE



physical destruction of computer hardware and use of electromagnetic interference designed to destroy unshielded electronics via current or voltage surges.

• **Data modification:** A successful attack on the integrity of sensitive data can mean that legitimate users (human or machine) will make important decisions based on maliciously altered information. Such attacks range from website defacement, which is often referred to as "electronic graffiti," but which can still carry propaganda or misinformation, to the corruption of advanced weapons systems.

• **Infrastructure manipulation:** National critical infrastructures, or CI, are increasingly connected to the Internet. However, because instant response may be required, and associated hardware may have insufficient computing resources, CI security may not be robust. The management of electricity could be especially important for national security planners to evaluate, because electricity has no substitute, and all other infrastructures depend on it. Finally, it is important to note that many CI are in private hands.

Cyber attacks in war

In the future, the ultimate goal of warfare — victory — will not change. And the advice of Sun Tzu and Clausewitz will still apply. However, the tactics of war are radically different in cyberspace, and if there is a war between major world powers, the first victim of the conflict could be the Internet itself.

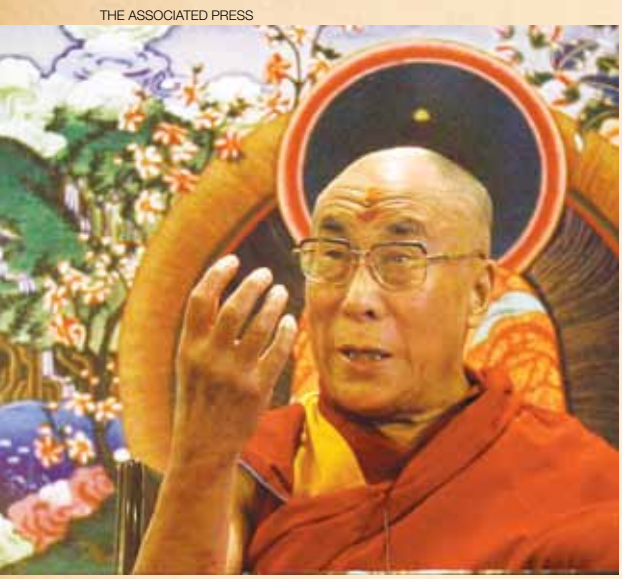
There will be two broad categories of cyber attacks during a major war:

• **Military forces:** The attacks would be conducted as part of a broader effort to disable the adversary's weaponry and to disrupt military command-and-control systems.

In 1997, the U.S. Department of Defense held a large-scale cyber attack red team exercise called Eligible Receiver. The simulation was a success. As James Adams wrote in Foreign Affairs, 35 National Security Agency personnel posing as North Korean hackers used a variety of cyber-enabled information warfare tactics to "infect the human command-and-control system with a

If there is a war between major world powers, the first victim of the conflict could be the Internet itself.

THE ASSOCIATED PRESS



From far left: An alleged militant with the Global Islamic Media Front is led into a courtroom in Vienna in August 2009. He was sentenced to four years behind bars for producing an Islamic threat video distributed on the Internet.

Scottish hacker Gary McKinnon faces extradition to the U.S. under anti-terrorism laws following his breaching of military computers dating back to 2001. He could face up to 70 years in prison.

The Dalai Lama, Tibet's spiritual leader, responds to reports that a cyber spy network based mainly in China hacked into classified documents stored on computers of the Dalai Lama and Tibetan exiles.

paralyzing level of mistrust. … As a result, nobody in the chain of command, from the president on down, could believe anything."

In 2008, unknown hackers broke into both unclassified and classified computers at U.S. Central Command, the organization that manages both wars in which the U.S. is engaged. The Pentagon was so alarmed by the attack that Chairman of the Joint Chiefs of Staff Michael Mullen personally briefed President George Bush.

In the event of a war between major powers, it is wise to assume that the above-mentioned attacks would pale in comparison to the sophistication and scale of cyber tools and tactics that governments may hold in reserve for a time of national security crisis.

• **Civilian infrastructure:** These would target the adversary's ability and willingness to wage war for extended periods, and may include an adversary's financial sector, industry and national morale.

One of the most effective ways to undermine a variety of these second-tier targets is to disrupt power generation and supply. In May 2009, President Barack Obama made a dramatic announcement: "cyber intruders have probed our electrical grid. … In other countries, cyber attacks have plunged entire cities into darkness." It is believed that these attacks took place in Brazil in 2005 and 2007, affecting millions of civilians, and that the source of the attacks is still unknown.

Referring to theoretical cyber attacks on the financial sector, former U.S. Director of National Intelligence Mike McConnell said his primary concern was not the theft of money, but an attack on the integrity of the financial system itself, designed to destroy public confidence in the security and supply of money.

Today, militaries can exploit global connectivity to conduct a full range of cyber attacks against adversary CI, deep behind the front lines of battle.

Looking to the future

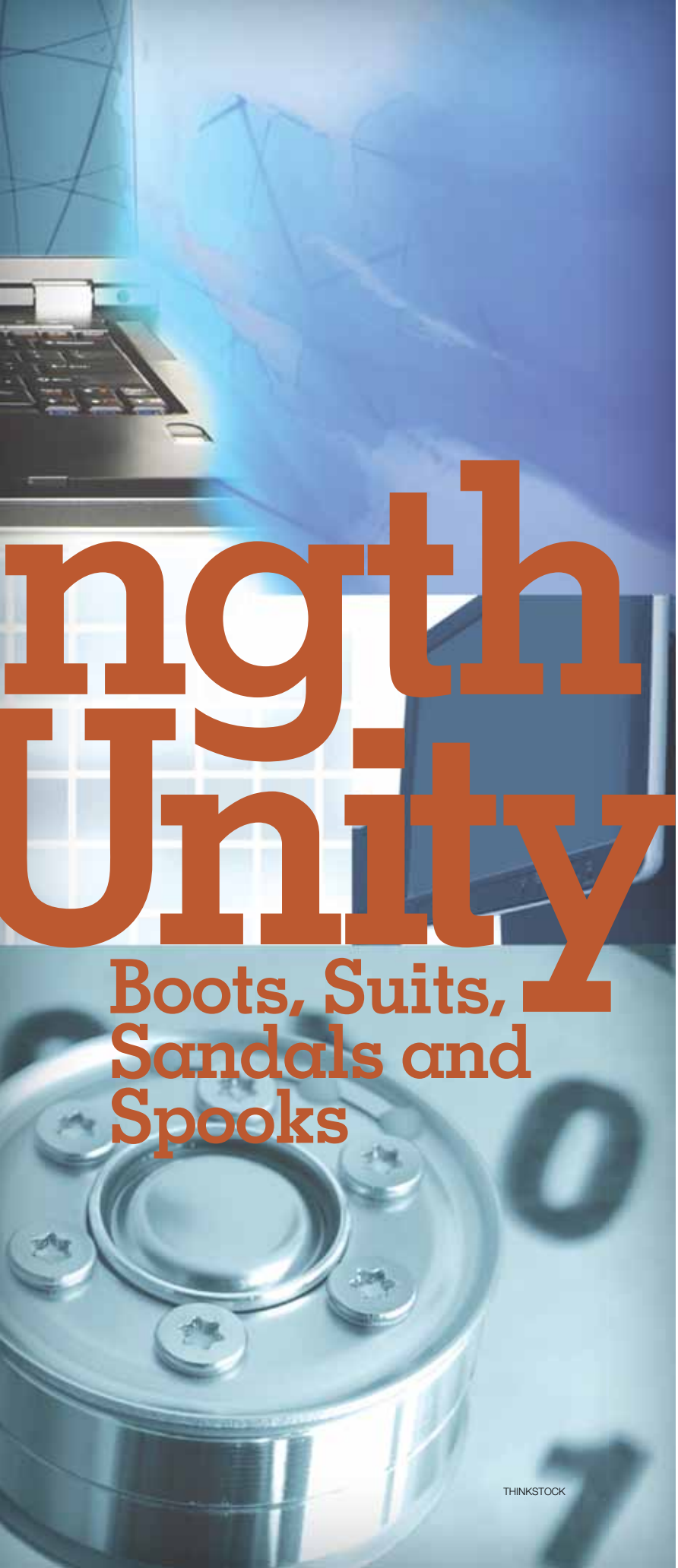
The Internet has changed the nature of warfare. Computers are both a weapon and target. As with terrorism, hackers have found success in pure media hype. As with weapons of mass destruction, it is difficult to retaliate against an asymmetric attack.

On balance, cyber warfare may favor nations robust in IT, but the Internet is a prodigious weapon for a weaker party to attack a stronger conventional foe. And Internet-dependent nations have more to lose when the network goes down.

From a defensive standpoint, nations should invest in technologies that mitigate two key hacker advantages: poor attacker attribution and a high level of asymmetry. The often anonymous nature of computer hacking and its very high return on investment can prevent traditional risk mitigation, such as deterrence and arms control.

At this point in history, many governments may feel compelled to invest in cyber warfare, not only as a way to project national power, but as the only means to defend their presence in cyberspace. □


Stre
Through



ngth Unity

Boots, Suits, Sandals and Spooks

THINKSTOCK

Lessons from the Comprehensive Approach for Whole of Nation Cybersecurity

Alexander Klimburg,
Austrian Institute for International Affairs

A defining element of national cyber security is the importance of nongovernmental actors. For more than a decade, many governments have maintained Critical Infrastructure Protection, or CIP programs to encourage cooperation between government and certain key private sector companies, especially on cybersecurity. Results have been mixed, and there is a growing understanding that the wide-ranging involvement of nongovernmental actors is only possible within a "Whole of Nation," or WoN approach — a method of cross-organizational collaboration.

Within national cybersecurity, the importance of the private sector and civil society is obvious. The private sector is responsible for virtually all of the software and hardware that is exploited for cyber attacks, maintains most of the network infrastructure over which these attacks are conducted, and often owns the critical infrastructure against which these attacks are directed. Further, civil society actors — as distinct from the private sector — dominate cyberspace, defining the programmed parameters (i.e. the software protocols) of the cyber domain, as well as executing, researching and ultimately publicly speculating on cyber attacks. Together, these nongovernment actors account for the bulk of what is termed "national" cybersecurity. They are only partially accounted for in most national CIP programs.

Some critics, especially in the United States, may worry that the WoN approach allows the military a greater role in CIP efforts, as recently witnessed with the public activity of the new U.S. Cyber Command. There is some truth to this, but the criticism threatens to obfuscate a more important issue than the entry of the military into a mostly civilian domain. All relevant actors, in and outside government, need to be more involved in cybersecurity.

The difference between CIP and WoN is primarily related to scope. While CIP (when applied to cybersecurity) is concerned with defeating individual attacks, WoN cybersecurity is more concerned with addressing entire attack methods — for example, improving the quality of software to prevent errors in it from being exploited, or addressing issues of data retention and data sharing. Also, WoN cybersecurity has to address possible "catastrophic" cyber attacks on

national infrastructure, attacks that are likely to be waged within the context of cyber warfare. A reality of hostile acts in cyberspace is that some may well be state-sponsored, or even a first step toward cyber warfare. To be able to prepare for cyber warfare, it is therefore necessary to closely monitor purported cybercrime and cyberterrorist behavior.

While the WoN approach remains poorly defined within cybersecurity, similar approaches have successfully been implemented by a number of countries. Within the context of so-called Conflict Prevention or Fragile States strategies — which within the military includes stabilization operations such as in Afghanistan and Iraq —WoN has been employed for a number of years, even if not always under that specific name.

The NATO Comprehensive Approach is one such example of this approach in operation. There are many national doctrines as well, most notably in the United Kingdom, the Netherlands, Canada, Denmark and Finland, to name a few. The collaboration of defense, diplomacy and development actors is always paramount within these doctrines. This requires the joint cooperation of the military, political experts, civil society and intelligence communities — or "boots, suits, sandals and spooks" — to find common solutions not only at the operational level within the respective area of operations, but also at the political level within respective national capitals.

WoN refers to the joint integrated application of state (whole of government) and nonstate (business, civil society) efforts to attain a common objective. In Fragile States policies, this objective usually is the stabilization of a country or region. In cybersecurity, the objective is usually to decrease the vulnerability of a nation's networks

REUTERS

At the U.K. Government Communications Headquarters in Cheltenham, terrorism and cybersecurity take center stage in the country's national security strategy.

and critical infrastructure. In the next three to five years, a wide array of issues will need to be tackled in cybersecurity. A short list of hot topics would include data retention versus privacy, the liability of software companies, encouraging a nation's citizens to implement basic cybersecurity, the cooperation of critical network infrastructure owners, and, above all, information sharing within and between government and nongovernment.

To avoid reinventing the wheel in cybersecurity, it is advisable to learn from past experiences with whole of nation approaches. In essence, WoN is about process, and, like all processes, should be largely reproducible. Despite the seeming lack of communality between stability operations and cybersecurity, the two, after all, share one major common factor: the importance of working with nongovernmental actors.

REUTERS

A network defense specialist works at the U.S. Air Force Space Command Network Operations & Security Center at Peterson Air Force Base in Colorado. National security planners propose that critical infrastructure such as power grids, communications and financial networks be similarly shielded from cyber marauders.

The Austrian Institute of International Affairs has researched different national WoN approaches on behalf of Austrian government clients over the past several years. Based in part on this research, a new Comprehensive Approach for International Operations (known as AEK: Auslandseinsatzkonzept) as well as the Austrian Program for Critical Infrastructure Protection, or APCIP are currently being formulated. Although an exhaustive "lessons learned" list would fill many pages, some common conclusions regarding the WoN process, especially related to CIP, can be made.

Top-down or bottom-up?

The need for top-level leadership to initiate the process, within the domains of both conflict prevention and cybersecurity, is a priority. While this may seem obvious, the considerable cultural barriers often encountered in WoN mean that top-level ownership is paramount. Different organizations can have entrenched interests that, at first glance, appear insurmountable. Only a top-down approach can have any hope in overcoming these obstacles, although building on the experiences of the operational base can prove useful. Indeed, sometimes the best approach involves "bottoming up" ("grass-roots approach") on the pre-existing working group-level networks.

This is particularly important when the goal is information sharing. Perhaps the most important tool in cybersecurity, information sharing involves the exchange of highly sensitive data, mostly on cyber attacks suffered and their consequences. In most of Europe, these exchanges are often referred to in general as Public-Private Partnerships, or PPPs, although such exchanges can also occur between government organizations and indeed between private businesses directly. In the U.S., the most prevalent form of cyber PPPs are known as ISACs, Information Sharing and Analysis Centers, which are maintained within specific industrial verticals, such as in power, water, finance and others. Although ISACs make a valuable contribution to U.S. cybersecurity, their initial years were problematic, in part because there was little senior-level buy-in from industry and virtually no attempt to connect with pre-existing initiatives. A similar model in the U.K., called WARPs, had more success because of support from business and government.

It is important to note that for military cyber warriors, some of the most important intelligence is generated in these groups. To get access to this information, it is necessary to participate in the exchange process. In other words, intelligence has to be shared with these nongovernment actors as well. One tested tool in this information exchange is known as the "Traffic-Light Protocol," although for some government actors this often requires legal changes in the way confidential material is handled.

Patiently building trust

In cases in which actors are unfamiliar with one another and start with considerable preconceptions, getting to know each other is important. This applies especially to the "boots versus sandals" group, development actors and the military, and data protection advocates and national security officials.

In the experience of this author, initial meetings can appear to go badly, but both sides nearly always agree to continue the dialogue. Subsequent meetings greatly contribute to mutual cultural understanding. This is a key requisite for any trust-building exercise and requires patience. Experience also shows that it is highly advisable to insist on group stability, meaning that the same individuals are present at each meeting.

It is important also to appreciate that "changing core ideologies" cannot be a deliverable of a WoN approach. Certain notions important to business and civil society actors, such as protecting intellectual property or preserving "humanitarian space," might seem to be at odds with the requirements of government actors. However, personal misconceptions can be changed, and often need to, if government and nongovernment are to work together.

In Switzerland, the highly successful cybersecurity organization MELANI (a government cybersecurity center that supports critical infrastructure protection efforts) had only a dozen private sector clients when it first went online. The private sector expressed concerns that seemed insurmountable. These concerns included data protection and private-sector doubts as to the overall competence of the public sector. Four years later, MELANI has several hundred clients — including most of the world's leading banks — and is highly regarded both at home and abroad. This trust was earned over a number of years. The benefits did not only apply to the private sector. As a result of this wide trust network, Swiss civilian and military cybersecurity operators possess some of the best cyber intelligence.

THINKSTOCK

Honest brokering

WoN efforts do not operate in a political-social vacuum, and will reflect common perceptions of the relative political power of the actors. Often, if not always, the state or public-sector will be perceived as the strongest political actor at the table. Usually it's the state that also will initiate the WoN process. Some of the other actors will initially be less convinced of the relevance of the process itself, and will treat most aspects of the process (including participation) as being contingent on negotiations in other fields as well.

As the initiating actor, the state has two choices on how to approach this delicate matter. It could behave as a *primus-inter-pares* (first-among-equals) actor. Here, the state directly seeks to represent its interest at the table as well as moderating the process. The advantage is that the state is directly able to engage with the other actors, and also places the outcome before the process. The disadvantage is that the state must be able to present a completely united front (i.e., if more than one governmental actor is represented, the respective hierarchy between them must be clear to all participants).

Also, the process might degenerate into "horse-trading" of the state with individual nonstate actors, failing to create any institutional buy-in on the part of these actors. Countries that have engaged in the *primus-inter-pares* role include, in particular, the U.S., U.K., and Australia. In each case, a single government agency or department was empowered to lead these discussions. In the U.K., for example, this falls within the responsibilities of the Centre for the Protection of National Infrastructure, or CPNI.

A second approach is to utilize an "honest broker" intermediary. This actor does not have a direct stake in the outcome and is therefore only concerned with the process. Often a nonstate actor, such as a think tank, is entrusted with the task through the state and occupies a hybrid role within the process.

An advantage of this approach is that by separating process and outcome, the process is endowed with a more impartial nature, arguably more conducive to creating a whole of nation mindset among the actors. Also, it is particularly useful when a number of government actors are at the table, and no one particular actor is able or willing to represent the state. The drawback of this approach is that the intermediary can overstate the importance of process over outcome, thus curtailing possible positive externalities, such as new initiatives. Also, the scope of individual negotiations is reduced, as the process is endowed with a more collective nature. An example of this approach is the National Institute to Combat Cybercrime or NICC, in the Netherlands.

Does a "big tent" approach work?

Transparency and inclusiveness have benefits, but also pitfalls. In case studies, there were striking differences between the small, select and confidential approach versus the "big tent" approach. Evidence suggests it is better to start small and later go big.

In cybersecurity, there have been clear indications that the small-group approach is more likely to pay dividends. For example, as the U.S. Deputy Secretary of Defense William Lynn recently discussed, U.S. Cyber Command has pioneered a number of new security measures, such as the introduction of automated active defenses against cyber attacks to protect the defense industrial base. These results were mostly possible due to close collaboration between the command and a few defense contractors.

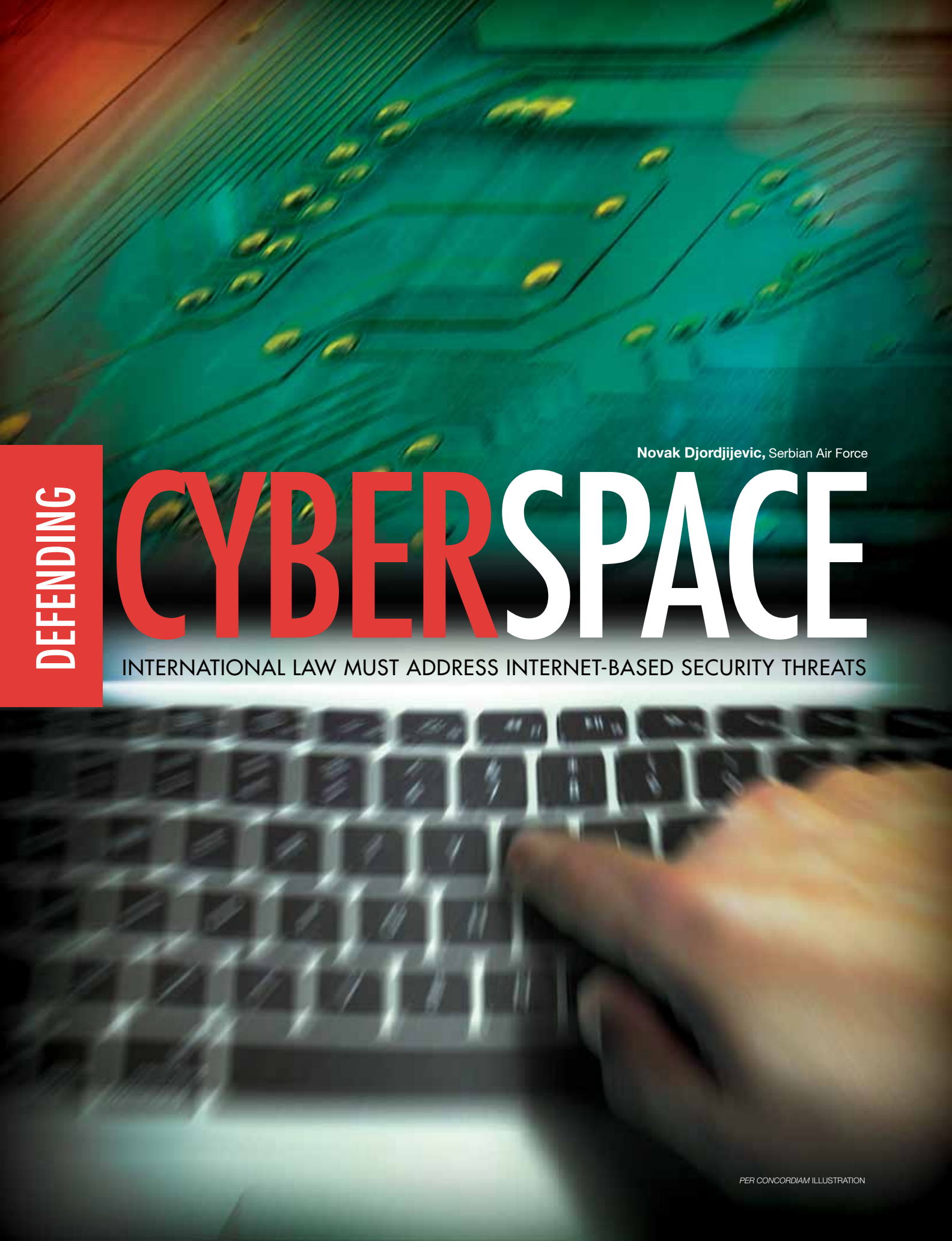
On a smaller, tactical level there is often common understanding that smaller groups are much better at information sharing than larger groups. Both the CPNI and the NICC, for instance, cap membership of a particular group at no more than a couple dozen participants.

However, WoN seems to imply the need for much wider participation than is currently covered in conventional CIP programs. Unlike CIP programs, WoN is supposed to deliver much wider changes in policy than the "operational measures" described above. For example, how would government motivate software companies to take more responsibility for the integrity of their products, given that the majority of cyber attacks are delivered through errors in their programs? How would it persuade more private businesses to contribute to national cybersecurity by sharing data? These issues cannot be tackled in small, secret working groups, but require widespread consultation and political support, even if it can be helpful to consult earlier with a select group.

In conflict prevention, this approach has already paid dividends. In one country examined, civilians and government initiated a confidential consultation process named after a local beachside hotel. One outcome was the civilians' tacit support for military engagement in Afghanistan. Another outcome was a wide-ranging public discussion on development and development aid, and how it should be best employed. A result of this public discussion was that even during the upheaval of the recent financial crisis, the humanitarian and development aid budget remain untouched. Clearly, the public discussion, which proved beneficial to the community as a whole, was only possible with the small-group trust-building and experience-sharing that preceded it.

While there are additional lessons learned than those described above (and include multiple caveats), these illustrate that the WoN approach is indeed a process, and like all processes should be replicable in different circumstances. The "boots, suits, sandals and spooks" do not always represent exactly the same actors. For example, the "sandals" can refer to development workers as well as bloggers. Also, the private sector is decisive within CIP, while in conflict prevention nongovernmental organizations are the main nonstate group. However, in both cases the principal issue is the broad cooperation of traditionally antagonistic actor groups.

Overall, the WoN process represents a paradigm shift in how security policy can be conducted in liberal democracies, a paradigm based on trust, common interest and the increasing reality of distributed power. □



Novak Djordjijevic, Serbian Air Force

DEFENDING CYBERSPACE

INTERNATIONAL LAW MUST ADDRESS INTERNET-BASED SECURITY THREATS

PER CONCORDIAM ILLUSTRATION

Contemporary security threats are characterized by, among other things, asymmetry and flexibility. However, in the modern world, security threats transcend the limits of the physical domain, physical security and freedom of the individual and impinge on the economic, intellectual and privacy domain. In addition to activities and relationships in the physical domain of reality, using services available over the global network — the Internet — we communicate, exchange information, perform tasks, have fun and make purchases in a parallel, virtual reality. In the Internet information cloud we leave traces of our activities, traces that connect us to other people, institutions, companies and organizations. By leaving behind this information, we unintentionally reveal more about ourselves than we would have wanted.

These traces are useful information to cybercriminals. Using this and other information, cybercrime can reach unimaginable goals. In addition to individuals who are frequent points of attack, criminals are targeting websites, information portals, e-mail systems, social networks, corporate networks or networks of governmental and nongovernmental organizations, and even other criminals.

But what is a cybercrime? Simply put, cybercrime is the illegal use of computers and the Internet, or a crime committed using computers or the Internet.[1] This definition should be extended to include other telecommunication devices such as mobile phones, personal digital assistants (PDAs) and other devices that establish connections with other devices.

MOTIVATION FOR CYBERCRIME

It is often difficult to understand what drives cybercrime and motivates cybercriminals. It is difficult to classify motives, but some of the most common are listed below[2]:

- Political/religious (expansion of political, religious or other ideas, the realization of political, religious or other aims, retaliation for political or other activities, etc.)
- Financial gain
- Idealistic (activity to prove skills and abilities, without expectation of financial or other benefits or rewards)
- Curiosity, adventure (mostly beginners who have not yet entered into serious criminal activity, "coders/hackers/techies," people who are looking for a quick route to riches or fame but lack the knowledge and skill)

This limited classification helps to show how modern cybercrime is able to recruit large numbers of people. If one can promote political ideas on the Internet by illegal means, make money illicitly, or simply try to hack a site without consequences, nothing really prevents one from doing that except personal ethics. This leads to the assumption that this type of crime will continue to grow and develop. Not only has cybercrime been growing for years, but some forecast darkly[3] that production of malware (malicious software) could soon surpass production of legal software[4].

According to some experts, one of the causes for proliferating crime is an unfavorable relationship of three factors: risk, effort and benefit.[5] According to the current state of affairs, the risk that criminals face is very small and the efforts required modest, while the benefit to be achieved is relatively high. If this relationship could be reversed through use of a tailored strategy (high risk — moderate effort — small benefit), there could be a significant drop in cybercrime.

KNOW YOUR ENEMY

According to the Internet Crime Complaint Center (IC3) 2009 year report,[6] IC3 received 336,665 complaints compared to 16,883 complaints in 2000, an increase of almost 2,000 percent. The increase in financial losses in the same period is close to 3,200 percent. Most people reported financial losses in the amount of $100 to $1,000 (36.7%), and nearly 87 percent of victims lost less than $5,000. This data clearly indicates that cybercrime is growing.

However, do we take this threat seriously? The general public's understanding of cybercrime is vague. Unlike traditional forms of crime, it seems that cybercrime is faceless, and it is unclear whether the criminal structures consist of individuals, criminal groups or a combination of both. The cybercriminal personality is created because of special social, technological, economic, hereditary or other factors. Theoretically, anyone could become a cybercriminal.

The computer security firm Symantec recently published the results of a study in which it analyzed cybercrime and human relationships based on a sample of about 7,000 respondents from 14 countries.[7] Some results show that most people mistakenly believe that cybercrime is not organized crime, although the analysis revealed that "90 percent of today's cyber attacks are a direct result of organized crime." In other words, most people believe that cybercrime is an individual activity, while evidence shows that cybercrime is mostly organized crime. This means solving the problem of cybercrime requires an organized, systematic, international approach.

To determine appropriate strategies against cybercrime, it is necessary to understand the order of criminal mechanisms in the physical domain (modus operandi). This is best done through interpretation of the topology of cybercrime. Cybercriminals are often organized into small groups proficient in using software and hardware. However, criminals from a single group do not have to be in the same physical location, but can be dispersed across cities, regions, countries and even continents. In addition, they rely on hardware that can be rented in any country. Criminals can use the Internet to execute their operations remotely.

Such amorphous organizations and activities are very difficult to detect and track, and almost untouchable by legal means. This topology makes cybercrime an organized global criminal phenomenon and a growing global threat to all of us.[8] Cybercrime is like cyber cancer. The removal of one problem usually represents just a short break before a new problem pops up somewhere else. Like a cancer, cybercrime seems to elude efforts to curb it.

DEFENSE IS NOT ENOUGH

Is there a strategy for controlling the growth rate and extent of cybercrime? Why do current methods of combating cybercrime render modest results?

Methods of combating cybercrime were developed in the early days of computers, when malicious programs spread through floppy disks and the spread of a virus took a relatively long time. With the emergence of networks, dissemination of harmful programs multiplied rapidly. This means the spread of harmful programs is almost immediate. The only things that stand between two network nodes are safeguard mechanisms.

However, existing methods of protection are defensive and reactive, which means that protection systems wait for the occurrence of harmful programs (defensiveness) and recognize and block known harmful programs (reactivity), but have trouble coping with the inventiveness of cybercriminals. The reactive method means that it is possible to fight known threats. The new threat appears, after being uncovered and identified, then the appropriate protective mechanism is created (patch, infected files deletion, blockade of certain actions, etc.), and finally is distributed as part of the protective mechanism. The problem is that this process is relatively slow, so there is always damage. The security model is a shield that strives to protect the computer from attackers. Examples of access controls are firewalls, passwords, anti-virus programs and anti-spam filters. But it's just passive defense. Without active mechanisms, current security systems lack the ability to prevent the cybercriminal from causing damage before he enters the grid.

In contrast to defensive and reactive methods, active methods could be created, but it requires a significant change in the technology on which the Internet rests. First, it should be realized that cybercrime is a social activity that pervades several physical and virtual layers.

As a social individual, a cybercriminal is at the bottom of a crime scheme. This person is wrapped in layers that hide him, starting with hiding behind pseudonyms and avatars, a country's privacy laws, the characteristics of telecommunications hardware and software that may or may not track the malicious programs' network movements.

The scenario of a cybercrime occurring in one country and the criminals located in another country could be called a "crime projection," where the cause of the problem is not creating a problem in its environment but it is projecting it at a distance, in an environment that cannot effectively fight against pathogens. This is the fundamental strategy of cybercrime, which allows it to survive and develop almost undisturbed. To fight this strategy, a global response needs to be developed.

A GLOBAL RESPONSE

Good active strategy against cybercrime would imply:

- Legal regulation of international relations in terms of cybercrime treatment.
- Redefining telecommunications standards (hardware, software).
- Redefining the framework of privacy protection.
- User education (positive social engineering).
- International cooperation and coordination regarding criminal detection, monitoring and elimination.

The essential obstacle to dealing with cybercrime is the inadequacy of legal mechanisms. Laws established at the state and interstate level are the underlying premise for creation of a global mechanism for combating cybercrime.[9] Of course, the fight against cybercrime is possible even in the existing model of "every man for himself," but such a model is expensive, barely effective and hardly sustainable. In the longer term, if there is no significant change regarding cybercrime, each of us will be chasing one piranha while the piranha pack is devouring us all.

Redefined telecommunications standards would allow for information traffic flow monitoring and recording of the source, path and destination of telecommunications packages. This would enable authorities to — if necessary — analyze traffic data and identify the sources of criminal activity. This would be a key support mechanism for detecting and identifying cybercriminals.

However, it is certain that this would raise great privacy concerns. Traffic flow records would have to be stored and safeguarded for some time. It is a serious issue outside the scope of this paper, but let's mention one scenario. If someone illegally accesses traffic flow records, he could erase them or extract information, using data mining and other techniques, for illegal gain (e.g. competitive advantage). This problem requires legal regulations, access limits and appropriate software and hardware applications.

Education requires extensive and continuous effort, but it is at precisely this level that one can achieve the best and most enduring results. Proper education significantly reduces the chances that individuals become victims of cybercriminals. On the other hand, criminals have long used social engineering to persuade the individual to "click here" and become a victim. Education in this field is just as necessary as literacy education was a few centuries ago. However, in addition to education for ordinary computer users, the world needs education for professionals. That's especially true for professions that deal with cybercrime but lack technical training: judges, lawyers and prosecutors in the EU.[10]

In the absence of a more extensive and generally accepted international policy to combat cybercrime, individuals,[11] NGOs,[12] academic institutions[13] and security equipment and software manufacturers took the initiative, despite relatively diverse interests. Individuals, nonprofit organizations and academics have largely focused on the need to solve the problem systematically (public information, education, defining new security strategy, open software, etc.), whereas the interest of manufacturers lies partly in achieving higher profits.[14]

Coordinating anti-crime activities on the international level is complex. Activities of this type require participation of many actors, some of whom have begun to take matters into their own hands, not willing to waste more time waiting for governments to realize the need for international agreement on the issue.

FIRST STEP, LONG JOURNEY

The current security situation with regard to cybercrime is too lax. It's like a huge dam, patched up to avoid deterioration, that is about to collapse with negative security, political, financial and social consequences. Security mechanisms developed so far are no longer effective enough. They even generate an unwelcome side effect — the illusion of security.

In the current situation, where everyone takes care of his own problems, everyone fights cybercrime anyway he can. The state may have laws and enforcement mechanisms. Institutions may have hardware and software protection designed and maintained by professionals. An individual may have a personal protection system. The security device and software market is growing — it grows and develops to keep pace with the crime rate. Known names in the field of security earn big profits, but despite the benefits of the status quo, they recognize[15] that the challenges are growing.[16]

Cybercrime is a serious threat to all. It must be taken seriously. Simple actions limited to a single country will achieve modest results. Our semblance of security can be blown at any moment with a cybercrime on a horrific scale.

The road to creating an active protection model must cross many obstacles, one of which is the creation of international laws against this type of crime. Other problems are organizational and technical and will be easier to overcome once an international legal basis for the fight against this new global threat is established. □

1. The Free Dictionary, http://www.thefreedictionary.com/Cybercriminal
2. Wipul Jayawickrama, "Cyber crime – Threats, trends and challenges," Computer security week 2008 – Brisbane, http://www.auscert.org.au/download.html?f=290
3. Symantec, "Symantec Internet Security Report, Trends for July – December 07," published in April 2008, citation: "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications. " http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
4. Dr. Igor Muttik, "Cooperation is key to Internet Security", McAfee Security journal 6/2010, citation: "If we do not succeed in stopping the malware flood, then in a few years we could see more malware created than legitimate programs."http://www.mcafee.com/us/local_content/misc/threat_center/mcafee_security_journal_summer2010_en.zip
5. Joe Stewart, "Beyond takedowns: Offense in Depth," McAfee Security journal 6/2010 http://www.mcafee.com/us/local_content/misc/threat_center/mcafee_security_journal_summer2010_en.zip
6. Internet Crime Complaint Center, "2009 Internet Crime Report," published in 2010, see pages 2 and 6, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
7. Same as footnote 1.
8. National Fraud Center, "The growing global threat of economic and cyber crime," December 2000, http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf
9. International Telecommunication Union, "ITU Toolkit for cybercrime legislation," http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html , citation: "The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security."
10. Cybexa in partnership with UNICRI (financed by European Commission (AGIS 2005)), "European Certificates on Cybercrime and Electronic Evidence," http://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/ecce.php
11. Example: http://www.schneier.com/
12. Example: http://www.owasp.org/index.php/Main_Page
13. Example: http://cci.ucd.ie/
14. Example: "The Symantec Alliance Network provides a platform for expanding their channel partner ecosystem and driving more revenue with their solutions." http://www.symantec.com/about/news/release/article.jsp?prid=20100923_01
15. McAfee, "McAfee Virtual Criminology Report - Cybercrime: The Next Wave," citation: "Ingenious cyber criminals have evolved "super-strength" threats that are harder and harder to detect and can be modified on the fly." http://www.mcafee.com/us/research/criminology_report/default.html
16. Safe Internet Alliance, "International cyber crime creates new challenges for US authorities," http://safeinternet.org/blog/international-cyber-crime-creates-new-challenges-us-authorities

A New Era of Accountability

PER CONCORDIAM ILLUSTRATION

International legal reform could make states liable for cyber abuse

Dr. Bret Michael and Prof. Thomas Wingfield

The poor quality of security services offered by providers of information and communication technology, or ICT, complicates, even stymies, domestic and international efforts to discourage and lawfully respond to criminal activity, acts of terrorism and armed aggression in cyberspace. As a result, cyberspace has become a parallel universe in which the criminal, terrorist and unlawful combatant can operate with a high degree of impunity. Adding to the challenge, the privacy services provided in the form of user anonymity and data encryption make it difficult for law enforcement, intelligence organizations and militaries to attribute actions, whether lawful or not, to specific individuals or state actors.

An example is the widely reported Stuxnet worm — an integrated set of malware tools used to target a particular type of industrial control system.[1] Stuxnet takes advantage of gaping holes in the specification, implementation and assurance of security policy. The users of Stuxnet were able to exploit these failings to command and control the malware anonymously and to do their bidding remotely. There are few clues as to who developed or used Stuxnet. There is concern that Stuxnet will be used as a template for developing similar-purposed malware that will take advantage of other still-to-be-exploited weaknesses in current and future ICTs, much like the computer viruses and worms of today are variants of those described in Cohen's dissertation[2] and Morris' worm.[3]

However, the accountability problem is more than just technological. There are gray areas in international law, such as in determining the responsibility of a state when nonstate entities take action under the direction, instigation or control of a state's organs. At present, there are conflicting legal opinions about the immunity of the state in such situations. At one extreme, represented by the ruling in *Nicaragua v. United States of America*,[4] the state is immune from accountability. Another, more balanced interpretation is illustrated in *Prosecutor v. Duško Tadic*.[5] Where does this leave us? Given the legal uncertainty in this area, in addition to the ease of conducting covert and clandestine operations in cyberspace, states are incentivized to employ others to act on their behalf, for example, to incite riots or disrupt critical infrastructures in a target state. This lack of legal clarity has two effects: It provides cover for aggressors wishing to push the law beyond its actual limits, and creates uncertainty for law-abiding defenders who may choose to restrain themselves from activities that would protect themselves from lawlessness.

Because of the current technical structures — or lack thereof — and the current legal frameworks, we expect to see more attacks that are difficult if not impossible to attribute via technical means.

To be an internationally wrongful act, a state's action or omission must be attributable to the state and constitute a breach of an international obligation. Moreover, the state is treated as a single entity, so governmental action at any level implicates the state as a whole. International law extends these criteria to the actions of any group whose actions may result in the creation of a new state.

At the international workshop, "Scientific and Legal Problems: Creation of the International Information Security Systems,"[6] we proposed that the international community consider taking some specific initial steps that would make it more difficult for malefactors operating in cyberspace to leverage the gray areas of international law to their benefit.

AGENCE FRANCE-PRESSE

Gen. Keith Alexander, commander of U.S. Cyber Command and director of the National Security Agency, testifies before a Congressional committee on "U.S. Cyber Command: Organizing for Cyberspace Operations" in September 2010.

Analysts at the U.S. National Cybersecurity and Communications Integration Center in Virginia prepare for a cybersecurity exercise.

AGENCE FRANCE-PRESSE

Step One: Debunking myths

We must debunk these three commonly held myths.

One of the three burdens of proof used in criminal law must be met: beyond a reasonable doubt, clear and compelling, and preponderance of the evidence — These standards of proof do not apply to military and intelligence operations. In addition, decision-makers rarely have the luxury of such certainty of attribution before having to act to thwart or respond to attacks, especially in the case of cyberspace, in which there is a high level of time and space compression: Attacks can unfold in milliseconds, and the physical distance between the source of the attack and the target is, for the most part, immaterial.

There are some nontechnical methods to determine the source of a possible attack — Determining the source of an act within the required time to mount an effective response is often impossible because of such factors as spoofing identities and the lack of bilateral or multilateral agreements for sharing data about the paths that messages take in crossing one or more national borders. Given the way the Internet messaging protocols are designed, this is the norm rather than the exception. However, such factors are not showstoppers in determining culpability. There are many other methodologies that may be used to establish culpability, such as those that take advantage of open source, human and signals intelligence. The impossibility of reliable trace-back does not preclude the use of all other sources and methods to build a clear mosaic of responsibility, possibly after the fact.

It is necessary to attribute an act to a state in order to act internationally — On the contrary, individuals and groups may be investigated and prosecuted under another country's domestic law, if one of five conditions is met, commonly referred to as the principles of international jurisdiction:

- **Territorial:** Action in territory, or "substantial effect" in territory
- **Nationality (Active):** Malefactor is your citizen
- **Nationality (Passive):** Victim is your citizen
- **Protective:** Action poses a national security threat to your country
- **Universal:** Crime is so severe that any nation may take jurisdiction (e.g., piracy, slavery, genocide)

Step Two: Developing a framework

We recommended that a legal framework be developed for assessing the intelligence and military activities conducted in physical or cyberspace to reduce the legal uncertainty associated with such activities. As a starting point for discussion and development of such a framework, we proposed creating a two-dimensional space, which would map an intelligence or military activity to a level of state responsibility based on two factors: (1) the degree of state involvement in the activity and (2) our certainty of involvement of the state measured, for example, by determining whether the state is selecting targets, funding the activity, etc.

Step Three: Providing guidance in applying black-letter law

To advance the discussion and formulation of policy on conducting intelligence and military activities in cyberspace, we recommended that realistic examples of activities in cyberspace be given when formulating drafts of black-letter rules at the International Law Commission.[7] Such examples would be of particular value in developing a common lexicon and understanding of issues and solutions among the legal, policy and technical experts involved in discussions of attribution and accountability. At a recent conference in

Moscow, it was evident that participants' interpretations of even commonly used terms varied from one country to another.

The technical challenge

As international discussions ensue, participants in those discussions need to keep in mind that attribution is asymmetric. Parties to communications can have different goals and requirements for attribution, from perfect attribution to perfect nonattribution. Attribution involves a negotiation among the sender, receiver, and any other parties involved in communications and collaborations. In addition, one must have confidence that attribution is accurate and correct. As described above, this is a matter of degree rather than an absolute.

Moreover, attribution will remain a technically challenging problem — there are no silver bullets or quick fixes. For instance, the Internet was conceived without a requirement for user accountability. Retrofitting the Internet with that requirement has proved elusive. Short of starting over, it will require a major shift in the current Internet structure.

We also are repeating similar mistakes in our cellular communications infrastructures. Many of the current cellular infrastructures, for example Global System for Mobile Communications (GSM), rely on one-way authentication between the service subscriber and the service provider, by which the subscriber authenticates himself to the base station, but not vice versa, leaving GSM-based systems open to abuse by malefactors. At the DEF CON 18 exhibition in August 2010, a prominent conference on hacking, a participant with a laptop and antenna demonstrated his ability to turn off cellular encryption in the room by issuing a simple set of GSM instructions.[8]

Users of ICT have two options: (1) trust the infrastructure to deliver the contents of messages correctly or (2) have the sender and receiver agree in advance on how to judge the integrity of messages without relying on knowledge of the path the message followed from its origin to its destination. For option 1, there is little certainty about the integrity of messages when they arrive at their destination, so attribution is problematic. For option 2, technical issues abound, chief among them specifying and correctly implementing the policy and protocols for creation, maintenance or even prevention of strong bindings between the sender and his or her message, as pointed out by Simmons.[9]

Stakeholders aren't limited to the parties exchanging messages. Others interested in the outcome of discussions on state responsibility may include:

- States and organizations directly associated with the sender or receiver
- States and organizations not associated with the sender or receiver, but ones that are interested in some aspect of the provision, negotiation or enforcement of attribution
- States in whose territory messages originate or transit en route to their destination
- Providers of communication services such as Internet access and network/grid infrastructures

Conclusion

As Thomas Buergenthal and Sean Murphy[10] succinctly put it: "even the strongest states have long-term and short-term political and economic interests in an international order in which conflicts are resolved in accordance with generally accepted rules, in a manner that is reasonably predictable, and that reduces the likelihood of resort to force."

What is needed are solutions that are holistic in the sense that they take into account policy, legal and technical considerations, while at the same time are practical to implement and agreeable to states that are mutually distrustful of one another. As the entire history of international relations has played out with these forces at work, the challenges of integrating cyber law, policy and technology are not insurmountable. □

THE ASSOCIATED PRESS

Professor John McCanny is the principal investigator at the Centre for Secure Information Technologies at Queen's University in Belfast, Northern Ireland, which opened in 2009 to spearhead the fight against cybercrime.

1. See http://en.wikipedia.org/wiki/Stuxnet for details about Stuxnet.
2. F. Cohen, Computer Viruses, Ph.D. dissertation, University of Southern California, 1986.
3. J. Markoff, "Computer Intruder is Put on Probation and Fined $10,000," New York Times, May 5, 1990, p. 9.
4. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. U.S.), 1986 International Court of Justice 14, at 100-1 (June 27).
5. Prosecutor v. Dusko Tadic (Judgment in Sentencing Appeals), IT-94-1-A and IT-94-1-Abis, International Criminal Tribunal for the former Yugoslavia (ICTY), January 26, 2000.
6. The workshop was held at Lomonosov Moscow State University in November 2010 as part of the sixth International Scientific Conference on Security and Counter Terrorism Issues.
7. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, United Nations, in Yearbook of the International Law Commission, 2001, vol. II, Part Two.
8. See http://www.computerworld.com/s/article/9179959/Hacker_snoops_on_GSM_cell_phones_in_demo
9. G. J. Simmons, Subliminal Channels: Past and Present, IEEE European Transactions on Telecommunication, vol. 5, pp. 459-473, 1994.
10. Thomas Buergenthal and Sean D. Murphy, Public International Law in a Nutshell, St. Paul, Minn.: West Group, 4th edition, 2006.

The views and conclusions in this article are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

COOPERATION IS CRITICAL IN BOOSTING WIND

An Electrifying Start

A happy marriage of energy supply and demand — a growing fleet of electric and hybrid cars energized by wind mills in the North Sea and solar panels along the Mediterranean basin — is set to transform European transportation over the next decade.

Driving the transformation are freshly signed multinational agreements to capture, pool and transmit the generating power of ocean-borne winds, combined with regulations, taking effect in 2014, that require cleaner-burning automobile engines across the 27 states of the European Union.

This cooperative approach advanced by the EU addresses several of the continent's pressing problems: air pollution from an overreliance on coal-generated electricity, precariousness of petroleum supplies, and lackluster economic growth that undermines the continent's ability to defend itself and project its values.

"Putting our energy system on to a new, more sustainable and secure path may take time but ambitious decisions need to be taken now," EU Energy Commissioner Günther Oettinger announced in November 2010. "To have an efficient, competitive and low-carbon economy we have to Europeanise our energy policy and focus on a few, but pressing, priorities."

A large part of that policy is the implementation of the "Euro 6" regulations aimed at reducing tailpipe emissions starting in 2014. Euro 6 is widely seen as a way to steer automakers towards electric cars and away from the diesel cars that make up close to half of all European auto sales. Europe's diesel car industry isn't going away, but emissions reductions are compelling large manufacturers such as Mercedes, Volvo, Peugeot and Volkswagen to come up with diesel-electric hybrids to satisfy regulators. EU ministers agreed in 2010 that although gasoline and diesel engines "will remain dominant in the short- and medium-term," electric cars were a "highly promising ultra-low-carbon" technology that would reduce the EU's reliance on foreign fossil fuel.

"One of the big things in Euro 6 is the relatively harsh penalty on diesel," Colin Couchman, an analyst for London-based IHS Automotive, told Bloomberg news agency in late 2010. The new rules require that engines release 56 percent less nitrogen oxide, a reduction few diesel engines could accomplish in 2010. Automakers say strengthening that anti-pollution law will raise manufacturing costs, but it's still unclear how much of the cost will be passed to consumers.

Europeans are deliberating on how to standardize outlets

REUTERS

wind solar

and charging stations, setting off a race to see whether European, Asian or American standards will prevail. Speed of recharge is vital since most electric cars can travel only about 100 kilometers before they need to plug into an outlet. For sales of electric cars to become widespread, buyers can't afford to wait 8 hours for a household recharge. The gold standard is a half-hour recharge. In 2009 and 2010, countries such as Hungary, the Netherlands, Germany, Portugal, Croatia and others set up prototypes of what they hope will be national car-charging networks.

In October 2010, Portuguese Energy Secretary Carlos Zorrinho announced the availability, starting in 2011, of a system of charging stations that will grow to 1,300 locations in 25 towns across the country. "It will be possible to go through the whole country without problems of charging electric vehicles," Zorrinho told Reuters. Hungary reportedly opened its first public electric car refueling station in Székesfehérvár in September 2010. In May 2010, the Netherlands opened one of the continent's first fast-charging stations in the town of Leeuwarden.

At the 2009 Frankfurt Auto Show, Renault proposed another way to overcome the limited range of purely electric cars. A continent-wide battery swap program, modeled on old-fashioned stage coaches that required a change of horses at predictable intervals, would let car owners trade one leased battery for another when fuel ran low.

Electric cars by themselves are no panacea. Europe already produces an efficient alternative in clean diesel cars, which deliver stellar fuel economy without the grimy exhaust associated with previous generations of oil-burning engines. Peugeot, Europe's second largest carmaker, predicts it will sell 100,000 hybrid cars a year beginning in 2015. That number equals less than 5 percent of Peugeot's recent annual sales, which exceed 3 million cars and trucks.

And the price of electric cars, at least initially, could force them into the category of luxury vehicles without luxury accoutrements. Electric cars come with sticker prices nearly double that of similarly equipped economy cars. As German automotive executive Rainer Kurek told *Der Spiegel* in a story that appeared in December 2010, electric cars will ultimately succeed only as lower cost transportation, not as status symbols for wealthy greens. "Such cars satisfy only a very limited desire for mobility and are hardly well-suited to be expensive prestige items," Kurek told the magazine.

+ SOLAR POWER IN EUROPE

Windmills turn in the breeze at Horns Rev 2, one of the world's largest wind farms, off of the west coast of Denmark. The project came online in 2009 and will help Europe reduce reliance on coal-fueled power generation.

REUTERS

A driver plugs his electric car into a filling station in Dresden in August 2010. The German state of Saxony has installed battery recharging centers, part of what could become a continental car charging network.

AGENCE FRANCE-PRESSE

IHS Automotive told Bloomberg it expected sales of electric and hybrid cars, sparked by the Euro 6 regulations, to approach 13 percent in 2020, up from about 0.1 percent in 2010. *Automotive News Europe* noted a less enthusiastic forecast by J.D. Power and Associates, which estimated electrics and hybrids would carve out only 7 percent of sales in Europe over the next decade. Volkswagen chairman Martin Winterkorn was less smitten by what he called "electro-hype." In a 2009 speech reported in Germany's *Handelsblatt*, he predicted electric cars would total less than 2 percent of worldwide sales in 2020 and that reports of petroleum's impending demise have been greatly exaggerated.

When it comes to reducing pollution, electric cars are only as good as the type of electricity that fuels them. For example, in Poland, which gets most power from coal, electric cars won't ease pollution as much as they would in France, which gets most electricity from emissions-free nuclear power. That's where wind and solar power enter the picture. The EU has ambitious goals to have renewable energy provide 20 percent of member states' power in 2020 and 50 percent by 2050.

Wind has been the best bet in northern Europe, where solar power generation suffers from the region's frequent cloud cover. In December 2010, 10 countries announced an agreement to create a North Sea "supergrid" to collect and share wind-driven power. The countries are Germany, France, the United Kingdom, Sweden, Denmark, Ireland, Holland, Luxembourg, Norway and Belgium. Recognizing the region's wind potential, supporters talk of the North Sea as the Saudi Arabia of renewable energy. "Large-scale interconnection with our European neighbours is vital if we are to connect up our massive offshore wind potential and integrate it into European Markets," Gordon Edge, an executive with British renewable energy trade association RenewableUK, said in December 2010.

More fanciful schemes are reaching farther abroad. Thirty European companies have formed a consortium, Desertec Industrial Initiative, that is trying to corral investors for a 400 billion-euro project to develop North African solar and wind farms. With luck, Desertec could build its first power plant by 2013. Supporters say it would be one of the largest infrastructure projects in history if it accomplishes its goal of providing 15 percent of Europe's power by 2050. Desertec would capture the sun's power in two main ways: mirrors to focus the sun's rays to heat turbines and photovoltaic cells to capture solar energy more directly.

The project comes loaded with problems, not the least of which is the cost of North African solar power, quadruple that of power from coal and gas-fired generators. Desertec is lobbying for preferential treatment from the EU, mostly in the form of subsidies. Then there's the difficulty of building support south of the Mediterranean. Although potential partners such as Morocco and Egypt praised the project, Algeria is leaning toward building its own solar plants, *Bloomberg Businessweek* wrote in September 2010. "European countries can develop faster and cheaper than Desertec a renewable energy supply from indigenous sources," Hermann Scheer, German Bundestag member and head of the solar energy research group Eurosolar, told *Businessweek*. Spanish solar power holds promise, too, though a 2010 EU report said transmitting Spain's excess electricity to France would require a tripling of power line capacity.

But if most of the projects succeed, green car and renewable energy manufacturers would create hundreds of thousands of jobs partly counterbalanced by jobs lost in industries that rely on traditional power generation. Technology developed in places such as Germany and France, including automobile charging stations and windmill blade innovations, is exportable to the EU's eastern European and Central Asian neighbors. Furthermore, North African solar power ventures would require high levels of international cooperation, generating economic spinoffs beneficial to a less developed region that supplies many of Europe's illegal immigrants.

Energy independence would grow. Natural gas used to fuel European electric turbines comes from Russia and Algeria, among other places. Petroleum to make gasoline and diesel fuel heads the list of exports from the Middle East and Russia. Clean, domestic supplies of fuel would snap some of the tethers that bind the EU to not-always-friendly regimes. As the European Wind Energy Association reported in 2010, wind-generating capacity expanded faster in 2009 than that of any other power source. Whether or not manmade carbon dioxide is the main driver of what some believe is global warming, a reduction in noxious emissions is good for society.

"It will take decades to steer our energy systems onto a more secure and sustainable path," the European Commission proclaimed in November 2010. "Yet the decisions to set us on the right path are needed urgently as failing to achieve a well-functioning European energy market will only increase the costs for consumers and put Europe's competitiveness at risk." □

From Hostility To Hospitality

Calm in the Caucasus could help revive the region's tourism industry

In October 2010, Georgian President Mikheil Saakashvili, with newspaper and television reporters in tow, stripped off his shirt and plunged into the Black Sea for a 3-kilometer swim. The goal of Saakashvili's stunt was the economic revival of the Georgian coast surrounding the town of Batumi, a popular Soviet-era vacation spot hungry for a resumption of euro and dollar tourism. In between such feats of endurance, Saakashvili also praised the semi-neglected ski industry in the country's mountainous interior.

"For dozens of years we have been explaining to the Europeans that Georgia can be Switzerland of Caucasus. There is nowhere in the world with such a combination of sea and ski resorts — that's not an exaggeration," the president told the news site Georgia Today in 2010. "So instead of us becoming Switzerland of Caucasus, let Switzerland now become Europe's Georgia. … Let others compare themselves to us; but for now, Georgia needs a lot of work and a lot of investments."

For two decades after the fall of the Soviet Union, political and economic instability had chased away most of the tourists with a taste for the region's subtropical beaches, sparkling wine, rocky peaks and historical sites. But in this relatively remote corner of Eurasia, which includes Georgia, Armenia, Azerbaijan and parts of Russia, a tourism Renaissance is under way.

Mestia, a village in the Svaneti region of Georgia, hopes to draw more skiers and other tourists.

AGENCE FRANCE-PRESSE

Travelers now have much more from which to choose. Armenia has strung the world's longest cable car line, at 5.7 kilometers, over the Vorotan River Gorge that leads to the famed 9th-century Tatev monastery. In the landlocked nation north of Turkey, economic recovery includes a surge in sightseeing from Armenians living abroad, known as "diaspora tourism." Azerbaijan aspires to be an "elite" tourist destination that possesses the attractions of neighboring Iran without the political and religious drawbacks. A 2010 story in the *Caspian Business News* said Azerbaijan had spent the previous four years renovating and constructing 370 hotels containing 30,706 rooms. As part of its rebranding to international travelers, Georgia has launched an anti-pollution campaign to create a "golden sand beach" out of Batumi's waterfront by 2012.

The largest tourism investment of all is Russia's multi-billion-euro overhaul of the Black Sea coastal town of Sochi, host of the 2014 Winter Olympics, where palm trees will sway to a backdrop of snowy peaks. To handle hundreds of thousands of tourists, Moscow is bankrolling what is one of Europe's largest building projects, erecting from scratch ski pavilions, hockey and skating arenas, a 69,000-seat stadium, 90,000 hotel rooms and high-speed rail lines.

"Sochi 2014 is currently one of the largest complex ongoing investment projects in the world. Over 800 separate venue construction projects are being delivered simultaneously in time for 2014. The successful completion of these developments will create over 50 new enterprises and 43,000 new jobs," Russian Deputy Prime Minister Dmitry Kozak said in May 2010.

During the days of the Soviet Union, the Caucasus, coined the "Russian Riviera," developed into an exotic alternative to the ice-bound north. Its surf and slopes were favored by communist apparatchiks frolicking with wives and girlfriends. Spa-like beach resorts, stuffily reminiscent of Soviet and even Czarist days, give way to ski lodges in the foothills rimming the Black Sea coast. Farther inland is the realm of "adventure tourism," ideal terrain for foreigners eager to rough it at semi-accessible mountain villages and isolated monasteries. Adding to the vacation-land atmosphere are the wines and brandies produced in abundance in the region.

But another prime feature of the Caucasus — its dozens of ethnicities and languages — has bred violence, especially after the heavy hand of Soviet authoritarianism loosened its grip. Among the most publicized disagreements are the so-called frozen conflicts in South Ossetia, Abkhazia and Nagorno-Karabakh.

Kurt Volker, a recent U.S. ambassador to NATO, urged the international community to use the Sochi Olympics to smooth over disputes holding down the region. In a May 2010 article in *The Christian Science Monitor,* Volker worried that open Russian recognition of Abkhazia and South Ossetia, two regions that broke away from Georgia with Russian backing, would tarnish the games. Self-proclaimed Abkhaz and South Ossetian leaders declared independence from

THE ASSOCIATED PRESS

AGENCE FRANCE-PRESSE

Top: A ski lift under construction is shown near Sochi, site of the 2014 Winter Olympics. The games could bring hundreds of thousands of tourists to the Caucasus, a region that is trying to revive its economy.

Bottom: A bather enjoys the surf in Batumi on the Black Sea coast of Georgia as construction cranes build luxury hotels in the distance. In 2009, Georgia reported that its seaside resorts attracted the greatest number of foreign tourists since the demise of the Soviet Union.

Georgia in the early 1990s, and the last vestiges of Georgian authority were expelled in 2008 by the Russian military. Diplomatic recognition of the breakaway republics has been minimal: NATO, the European Union and the Organization for Security and Co-operation in Europe consider the territories part of Georgia.

"The Sochi Olympics could become a catalyst for resolving long-standing conflicts, bringing the Caucasus region into the 21st century," Volker wrote. Russia's interest in a successful Olympics "should be a powerful incentive for consigning to history Moscow's … approach to the Caucasus. This would surely be the best outcome for the states and peoples in the region, for Moscow, for the athletes and for the Olympics."

"The Sochi Olympics could become a catalyst for resolving long-standing conflicts, bringing the Caucasus region into the 21st century…"

An example of the ability of tourism to rebound quickly is Adjaria, Georgia's coastal region north of the Turkish border. It attracted an estimated 162,000 foreign tourists in 2009, the largest number in the post-Soviet era, just a year after Georgian and Russian soldiers contested South Ossetia and Abkhazia with gunfire. The allure of tourist investment could also help resolve differences over Nagorno-Karabakh, a mostly Armenian section of Azerbaijan that helped spark fighting between the two countries in 1991. Open warfare between the two countries ended in 1994, but fear of further outbreaks devastated South Caucasus tourism for years afterward.

The healing has begun. A 2010 tourism fair held in Yerevan, Armenia, drew travel industry professionals from Turkey, the United States, the Czech Republic and Germany. The Armenian government reported that tourism has grown about 25 percent per year since 2001, when the country celebrated the 1,700th anniversary of its conversion to Christianity. Azerbaijani tourism is also recovering thanks largely to its resorts and hotels centered mostly on the city of Baku on the Caspian Sea. A July 2010 article on EurasiaNet said five luxury international hotels, including those from the Four Seasons, Hilton and Kempinski chains, were rising in the city. Turkish businessmen have been prominent in the tourism trade, taking advantage of the Turkish language's kinship to Azerbaijani.

AGENCE FRANCE-PRESSE

Azerbaijani President Ilham Aliyev and Russian President Dmitry Medvedev share a chair lift at the Krasnaya Polyana ski resort in Sochi in 2010. Negotiators hope to use momentum from the 2014 Winter Olympics, which Sochi is hosting, to resolve conflicts such as the standoff between Azerbaijan and Armenia over Nagorno-Karabakh.

"This is an issue on which Russia, the United States and Europe have been working together well for years, and the outlines of a possible settlement have long been on the table," Volker wrote in May 2010. "An Azeri-Armenian settlement could spur travel, trade, investment and economic prosperity in the region."

A certain inflexibility left over from the days of the U.S.S.R. has acted as a hindrance to increased tourism. In a report on the South Caucasus, the World Bank noted that national governments have been slow in dismantling the expensive, top-down hospitality system modeled on Intourist, the stodgy Soviet tourism agency that doubled as a spy network during the Cold War. "The interpretation of the role and responsibilities of such institutions often does not correspond to the demands of a market economy," the report said. "The persisting approach is one of overzealous control versus creating incentives for private sector investments." In fact, when it comes to Russian tourists, Turkey is capturing some of the millions of travelers who used to cluster in the Caucasus. In a story about Russo-Turkish tourism in 2007, the *Guardian* reported that it's cheaper for a Russian to fly to Turkey than to Sochi. "Even staying in a country hotel just outside Moscow costs more than a holiday in Turkey," the *Guardian* noted.

Nevertheless, the Caucasus has taken pains to attract more tourists, most aggressively in Georgia. The country offers training in hotel management that includes internships at five-star establishments in Turkey. Its recently appointed tourism minister, Maia Sidamonidze, created a stir in September 2010 by proposing a "tourism alliance" with Turkey, Armenia and Azerbaijan to host cross-border package tours. When it comes to attracting private casinos and hotels, Georgia has offered to waive licensing fees and value-added taxes. Visitors from more than 30 countries no longer need tourist visas.

The biggest cheerleader remains Saakashvili, who, aside from promoting the allures of the sea, is pushing large investments in the hopes of turning Georgia's mountainous Svaneti region into a heavily touristed alpine paradise by 2011. A highway and airport overhaul costing an estimated $25 million will boost access to the regional capital of Mestia. In an October 2010 article published on EurasiaNet, regional government head Shmagi Nagani suggested skiers and nature lovers were the keys to bringing jobs to this remote region near the Russian border. "Tourism is, in general, the only path for the region to develop economically," he said. □

Upholding Afghan Women's Rights

Success of ISAF mission would end Taliban terror

In 2001, Afghanistan adopted a new constitution declaring men and women equal before the law. As a result, during the past 10 years the political and cultural position of women in Afghanistan has improved significantly. For the first time, women are graduating from the national police academy, joining the Afghanistan Armed Forces and obtaining powerful positions in government, including a provincial governorship. However, Afghan women fear that the last decade's improvements are threatened should the International Security Assistance Force, or ISAF, leave before completing its mission. They worry that their newfound rights will not be preserved if the Taliban reestablishes its rule.

More than 1,000 women serve in the Afghan military. They complete six months of training at a Kabul-based academy for women that prepares them for jobs in administration, communications, logistical support and medicine. Women are trained to search private houses and conduct roadside security checks alongside male officers. They are particularly helpful in this role because the Afghan culture does not allow men to search a woman's body or bags. However, attracting recruits can be difficult because of frequent threats by the Taliban against female Soldiers.

"We cannot and should not wait until these threats, risks, and problems disappear. We have to fight to overcome them, to build a better country," Gen. Khatool Muhammadzai, Afghanistan's highest-ranking female officer, told Radio Free Europe/Radio Liberty in November 2010. "So many women from foreign countries are in Afghanistan as a part of international coalition troops and to protect our nation. For us, Afghanistan is our home. Why shouldn't we serve our own country?"

Through the use of "female engagement teams," the U.S. Marine Corps has reached out to Afghan women. After going through a "do's and don'ts" crash course on local female customs, the Marines don headscarves under their helmets and set out to win over rural Afghan women by meeting in their homes, assessing their needs and gathering information. Afghan culture frowns on women talking to male Soldiers, so these female missions offer Afghan women a rare chance to speak frankly. A team's protocol is to ask the senior male leader for permission to speak to village women, distribute medicine, tea and school supplies, and then make conversation. The goal is to gain the trust of the women. "It's good news for us. The female Marines came and talked to the women and found out their problems. I am very happy," an Afghan sergeant told the Marine Corps in an article published on the ISAF website in December 2009.

ISAF troops also offer medical care to Afghan women and children. Oftentimes, mothers and daughters go without medical treatment based on the cultural fear of being examined by a male doctor. Some must travel long distances and cross the national border into Pakistan for acceptable medical care. For many,

AGENCE FRANCE-PRESSE

Female officers in the Afghan National Army attend a graduation ceremony in Kabul in September 2010. The Army currently has 100,000 troops, with plans to expand to 240,000.

the medical treatment provided by ISAF Soldiers is the first they experience.

Engaging women is important in improving security. Female recruits could help expand the Afghan security forces from 80,000 to 160,000, a number the Afghan Interior Ministry says is necessary to combat insurgents. Another 16 women graduated from the police academy in August 2010 in Kabul, adding to the hundreds of women already on duty. Policewomen provide important functions in Afghanistan. They are more adept at handling female criminals and frisking women, and their very presence helps counter negative stereotypes, according to a Radio Free Europe/Radio Liberty report. Still, policewomen are "often the victims of abuse or public acts of disrespect by people who think they should be living a more traditional way of life," the report said. Trainees at the academy receive instruction in conducting house searches, neutralizing explosive devices, using firearms, making arrests and detecting drug smuggling.

Afghan women are also expanding representation in Afghanistan's government. The September 2010 parliamentary elections demonstrate just how far women have come. Sixty-nine female candidates won seats in the Wolesi Jirga, the lower house of the Afghan National Assembly, out of 249 seats available, Deutsche Welle reported in November 2010. The Afghanistan Constitution established a 25 percent quota of women in the Wolesi Jirga, but women exceeded that by securing 28 percent of the seats. Women are working toward occupying more cabinet positions as well. In January 2010, President Hamid Karzai nominated a record three women for positions in his new cabinet, Reuters reported. Women's rights advocates and Karzai were dealt a blow, however, when only one was approved. "It's probably still too early to expect this much from a parliament that is led by conservative elements," women's rights activist Orzala Ashraf Nemat told *The Telegraph* of London in January 2010.

Women strive to improve themselves even in parts of Afghanistan where tradition reigns. Underground schools and secret shelters are some of the only ways these women can protect and improve themselves. As the British newspaper *The Independent* reported in April 2010, secret literacy classes are held under the guise of prayer meetings in dozens of villages in Zabul province. "The lessons concentrate on Pashto literacy, arithmetic and health and hygiene," the man behind the underground schools, Ehsanullah Ehsan, told *The Independent* in April 2010. The article explains that he teaches with a

Left: Suhaila Siddiqi served as the health minister in the transitional Afghan government. The Taliban once dismissed her from her job as a top surgeon because she is a woman.

Right: Afghan policewomen welcome a female U.S. civil affairs officer as she arrives to attend a ceremony to mark International Women's Day in Lashkar Gah, Helmand province, in March 2010. U.S. and Afghan female forces cooperate and discuss the successes and challenges of women-centered activities.

ASSOCIATED PRESS

AGENCE FRANCE-PRESSE

blackboard when unable to smuggle in schoolbooks, and hopes to broaden the curriculum to history, science and ethics. Children are also attending school more than ever. The number of Afghan children enrolled in primary school is at an all-time high of 6 million. Education is one way females can break the cycle of repression, a cycle that aids groups such as the Taliban.

Despite progress, repression remains in rural areas. Spousal abuse, forced marriages, strict restrictions on public movement and denial of education still impede women. Some women still suffer torture at the hands of the Taliban. Women in Afghanistan sometimes revert to setting themselves on fire to end lives of abuse, the U.N. Dispatch reported in November 2010.

Likewise, an article in a 2010 *Time* magazine epitomized life under Taliban rule. Aisha, an 18-year-old girl featured on the cover, was punished by a Taliban commander for running away from her husband's house, after alleged abuse by her in-laws. With the Taliban's approval, her brother-in-law held her down while her husband sliced off her ears and nose. She was left for dead, choking on her own blood and passing out from the pain. Rescued by ISAF troops and given medical care, Aisha is one of many women who fear the return of the Taliban.

Rules enforced by the Taliban still hold sway in some rural areas. They include a ban on all women's activities outside of the home unless accompanied by a *mahram*, a close male relative such as a father, brother or husband. Women can't ride bikes or play sports and are whipped if they leave even an ankle exposed. The Taliban demand that window panes be painted, so that women cannot be seen through the windows of their homes. They impose their will with threatening letters delivered at night. "We warn you to leave your job as a teacher as soon as possible otherwise we will cut the heads off your children and shall set fire to your daughter," read one letter quoted in the *Time* article.

Afghan women in more progressive parts of the country have accomplished a tremendous amount in the past decade and do not want to revert to barbarism. Afghan women admit they have a long way to go to catch up. They sit beside men in government, as required by law, but many are not taken seriously, the Deutsche Welle reported in October 2010. "They are not heard and they have no chance to influence the negotiation in any way," said Afghan woman's rights advocate Soraya Parlika. She said some women gain important government positions through bribes and connections, not based on their qualifications.

TIME

The August 2010 issue of Time magazine features Aisha, an 18-year-old Afghan woman maimed by order of the Taliban for running away from her husband's house.

International leaders have voiced support for Afghan women's rights. A Reuters article in July 2010 mentioned U.S. Secretary of State Hillary Clinton's "personal commitment" to ensuring that such rights be fully guaranteed in any future Afghan political system. NATO is similarly committed. "NATO will support a political deal between the Afghanistan government and the Taliban only if it respects the constitutional rights of women," Secretary-General Anders Fogh Rasmussen announced in October 2010. He went on to say that "progress has been made in women's rights in Afghanistan, with more girls in school, more women in parliament, and more women setting up and running businesses or joining the police. All of this shows — in very concrete terms — the progress in Afghanistan for women's rights."

The British newspaper, the *Guardian*, suggests that the best way to safeguard the rights of Afghan women is through the development of Afghanistan itself. "It will also require a surge of efforts at a local level, to ensure that Afghans get the services they need and strong partnership with nongovernmental organizations who at the moment are the only ones capable of delivering at scale at local level," a September 2010 *Guardian* article said.

It may take many years for Afghan women to reach equality with Afghan men, but the country will truly benefit by harnessing the hidden talents of half of the Afghan population. □

Touting Reform in Central Asia

Fear of regional instability sparks cooperation

Samarkand, Bukhara, Merv, Tashkent and Osh are ancient cities of the Silk Road with histories dating back thousands of years. Residents of these cities have seen numerous empires come and go throughout history and now belong to nation-states carved out of the former Soviet Union: Uzbekistan, Tajikistan, Kyrgyzstan, Turkmenistan and Kazakhstan. Since the collapse of the U.S.S.R. in 1991, these nations have worked to establish national identities as part of the larger international community. Now, Central Asia scholars are increasingly concerned that this resource-rich and geopolitically sensitive region could become a hotbed of failed states that never sufficiently evolved following independence.

The European Union and NATO have expressed an interest in aiding Central Asian states to establish stable, secure, free and prosperous societies. Former U.S. Secretary of State Condoleezza Rice wrote in *The Washington Post:* "Weak and failing states serve as global pathways that facilitate the spread of pandemics, the movement of criminals and terrorists, and the proliferation of the world's most dangerous weapons." This statement is still true today.

REUTERS

Workers from Russian energy company LUKOIL inspect pipes at the Khauzak gas field, 350 km northwest of Bukhara, Uzbekistan. The field is part of a project that is expected to contribute one fifth of Uzbekistan's gas output.

Local problems, international impact

An unstable and failing Central Asia threatens Europe and the world. The region, which borders on Afghanistan to the south, has seen violent Islamist groups, most notably the Islamic Movement of Uzbekistan, or IMU, and the Islamic Jihad Union, or IJU. The IMU and IJU have been affiliated with al-Qaida and the Taliban. As recently as November 2010, Tajik security forces were engaged in operations against alleged IMU extremists in the Rasht Valley following the escape of several high-profile militants from a prison in the capital of Dushanbe.

Cooperation among the region's governments, and support from the EU and neighboring powers such as Russia and China, could help stabilize the region and promote economic growth. The issue provides territory whereby Russia and the West can cooperate after decades of Cold War rivalry. While the objective is significant, the road is strewn with obstacles.

Border conflict

As in Kyrgyzstan, regional ethnic tensions have inhibited cooperation among Central Asian governments. These tensions can be traced to the creation of Central Asian Soviet republics in 1924 when, in the words of *The Economist,* "Stalin divided it into a patchwork of states whose borders were designed to fracture races and smash nationalism. He succeeded in preventing ethnic groups from uniting against him, and also in ensuring that each state is a hotbed of ethnic rivalry."

Natural resources are a primary source of friction among governments, and allocation of water rights has been the most divisive. Agriculture in this semi-arid region requires irrigation and water management. Kyrgyzstan and Tajikistan possess Soviet era reservoirs that farmers downstream in Uzbekistan, Kazakhstan and Turkmenistan depend on. "The Soviet command

economy would order the upstream countries to collect water in their dams to be released downstream in spring and summer during irrigation periods. In return, the downstream countries rich in fossil fuels (especially gas, oil and coal) were ordered to provide the upstream countries with these natural resources and electricity, which they did not possess," explains Umida Hashimova in the *Central Asia-Caucasus Analyst*.

The Soviet successor states have struggled to come to terms over use of these resources, and the situation became more complex when Uzbekistan left the regional electricity network in December 2009. According to Erica Marat of the Jamestown Foundation, Uzbekistan uses gas exports to pressure the upstream countries, charging market prices unaffordable to their poorer neighbors. To offset higher costs, Kyrgyzstan and Tajikistan want to build more hydroelectric dams. Uzbekistan strongly opposes new dams, worried about water shortages during the summer. Kazakhstan has taken the lead in supporting regional energy cooperation and has supported increasing Tajik and Kyrgyz energy independence

"Historically, autocratic rulers have governed the lands of Central Asia. Tribal and clan connections still play a significant role in the political, social and economic interactions amongst the populations…"

— Yevgeny Bendersky
Eurasian affairs analyst

Ethnic Uzbek refugees wait at the Kyrgyzstan-Uzbekistan border outside Suratash in June 2010. Uzbekistan closed its border to prevent a mass exodus of refugees fleeing clashes between rival groups in Kyrgyzstan.

AGENCE FRANCE-PRESSE

and measures to build an electricity grid that bypasses Uzbekistan, if necessary. And if a new gas field in Tajikistan meets expectations, the country could become energy independent by the end of 2011.

The energy riches of Kazakhstan, Turkmenistan and Uzbekistan provide economic opportunities not readily available to their poorer neighbors. Their energy resources also underline the importance of establishing a stable and secure political and economic environment. According to *World Politics Review,* the region is "estimated to contain as much as 250 billion barrels of recoverable oil, boosted by more than 200 billion barrels of potential reserves. That's aside from up to 328 trillion cubic feet of recoverable natural gas." Western Europe hopes to ship plentiful Central Asian gas through the Nabucco pipeline, which bypasses Russia and reduces European dependence on Russian gas supplier Gazprom.

While Central Asian governments view one another with suspicion, the IMU and other pan-Islamic extremists view the entire region as their territory and exploit the lack of interstate cooperation to operate across borders. The IMU has conducted attacks in Uzbekistan, Kyrgyzstan and Tajikistan. Drug smugglers also take advantage of porous borders. A report from the U.N. Office on Drugs and Crime says that lack of cooperation between Central Asian law enforcement agencies also hurts the fight against narcotics trafficking: "Combating illicit drug trafficking requires well-organized systems of information collection, processing and analysis, as well as the exchange of the final information product among agencies involved at national and regional levels. Unfortunately, major deficiencies in intelligence collection and sharing continue to hamper effective policing of Central Asia's borders with Afghanistan."

THE ASSOCIATED PRESS

A Kyrgyz man votes at a polling station in the city of Osh during a referendum on a new constitution in June 2010. The constitution approved by voters makes Kyrgyzstan the first parliamentary democracy in Central Asia.

Engaging the region

For Western nations, the importance of stability and security in Central Asia can create policy conflict. How should governments that strongly espouse democracy, freedom and openness relate to the authoritarian regimes of the region? Some proponents of democracy think the West compromises itself by supporting repressive, authoritarian regimes, even if stability created by those regimes increases trade and investment, curtails drug trafficking and forestalls the spread of Islamic extremism. A second school of thought prefers a strategy of engagement: The West provides training and resources to Central Asian governments while encouraging democratic reforms.

Some argue that liberal democracy is alien to the culture of Central Asia. On Eurasianet.org, Eurasian affairs analyst Yevgeny Bendersky wrote: "Historically, autocratic rulers have governed the lands of Central Asia. Tribal and clan connections still play a significant role in the political, social and economic interactions amongst the populations, but are now effectively utilized to maintain the ruling elite in power, not to successfully mobilize any significant opposition." Kazakh political scientist Marat Shibutov sees President Nursultan

RIA NOVOSTI

Soldiers from a Kazakh air-assault brigade deploy after landing in the final round of the Interaction-2010 military drills held by the Collective Security Treaty Organization at the Chebarkul training ground in Russia.

Nazerbayev "as the only thing holding Kazakhstan together" and thinks that citizens are far more concerned with economic security than political freedoms, according to *Der Spiegel*. However, others argue that while an authoritarian government may give the impression of stability, these regimes are fragile and can crumble under extreme stress.

Recognizing the importance of NATO operations in Afghanistan and the continued development of Central Asian states into modern democracies, NATO announced in November 2010 that it plans to expand security cooperation. The quantity of equipment and supplies shipped through the Northern Distribution Network, or NDN, will increase substantially with 98 percent transiting through Uzbekistan, according to Eurasianet.org. Officials are touting improved relations and "continue to encourage the Uzbek authorities to address significant human rights concerns." The U.S. Department of Defense estimates that the NDN will stimulate economic growth and "has the potential to one day reconnect Central Asia to India, Pakistan, and other formerly closed markets, in a direct land route from the heart of Asia to the heart of Europe."

The Central Asian Nuclear-Weapon-Free Zone, or CANWFZ, is an example of the benefits of regional cooperation and engagement by the international community. Signed in September 2006, the CANWFZ "is the first nuclear-weapon-free zone located entirely in the northern hemisphere," the International Atomic Energy Agency said. It "forbids the development, manufacture, stockpiling, acquisition or possession of any nuclear explosive device within the zone," and commits signatory nations to meet international standards for security at nuclear facilities and to comply with the Comprehensive Nuclear-Test-Ban Treaty, reducing the risk of nuclear smuggling.

Organizations such as the Central Asia Regional Economic Cooperation Institute, which also includes China, Azerbaijan, Afghanistan and Mongolia, are also making progress in promoting a cooperative multinational environment in the region. Most of the Central Asian states are also members of the Chinese-led Shanghai Cooperation Organization and the Russian-led Collective Security Treaty Organization. Increasing engagement and cooperation between NATO and the EU and governments and organizations in the region promise to increase security by inhibiting the spread of terrorism and narcotics trafficking while helping Central Asian states stabilize and transition into modern democracies. □

AGENCE FRANCE-PRESSE

Supporters of Wikileaks founder Julian Assange wear Guy Fawkes masks as they demonstrate against his arrest in Amsterdam in December 2010. The "Hacktivist" group "Anonymous" has adopted the Guy Fawkes image as its public face.

"Hacktivists" Strike Back

Cyber attacks on financial institutions serve as a warning sign

In December 2010, the websites of international financial services giants Visa, MasterCard and PayPal were temporarily shut down, victims of a coordinated cyber attack dubbed Operation Payback by its perpetrators. "Hacktivists" who support Wikileaks and its founder Julian Assange attacked after the companies terminated service and disabled donations to the website. The economic impact of the attack remains unclear and the targeted companies denied suffering consequential losses. But the attackers, using the names "Anon" and "Anonymous," demonstrated the ability of cyber attacks to infiltrate and damage businesses and government agencies.

A modern form of protest

Anonymous didn't protest by chanting slogans or waving signs — it struck against Wikileaks' perceived enemies in the spirit of the virtual world they share. Wikileaks, whose *raison d'être* is exposing classified or confidential government or corporate information, is under pressure from the United States and other governments after leaking more than 250,000 U.S. State Department diplomatic cables in November 2010. The U.S. accuses Wikileaks of endangering lives by revealing unlawfully obtained secret government information and requested that companies cut ties with the website, as reported in *The Independent*.

Amazon, the online retailer that hosted Wikileaks on its servers, was the first to pull out. Visa, MasterCard and PayPal soon followed, essentially crippling Wikileaks' ability to accept donations that support publishing efforts. The cyber attacks started soon after.

When Anonymous staged its attack in the virtual world, it used a favorite weapon of the cyber warrior — distributed denial of service attacks. DOS attacks work by flooding a targeted computer system with incoming messages, denying service to legitimate users. A typical DOS attack uses thousands of "compromised" computers, usually surreptitiously infected with malicious programs, or malware, allowing a master con-

troller to direct the computers remotely. These networks, or botnets, are widely used by organized crime. Cyber gangsters have used DDOS to extort "protection" money from businesses in the same way traditional gangsters extort businesses in person.

Operation Payback hacktivists created a voluntary botnet. They recruited people from within their network and asked them to download malware, avoiding the need to infect strangers' computers, Noa Bar Yossef, a security strategist at data security company Imperva, told *PC World*. Hacktivists used sites such as Twitter to plan attacks and communicate and coordinate their efforts, according to technology magazine *Fast Company*.

Ironically, Wikileaks itself was hit with a DDOS attack. "The Jester," who calls himself a "hacktivist for good," attacked Wikileaks in November 2010, shutting the site down briefly before hundreds of thousands of classified diplomatic cables were posted. According to a CNN story, "The Jester" has attacked websites involved in "online incitement to cause young Muslims to carry out acts of violent Jihad." He told CNN he is against Wikileaks "for attempting to endanger the lives of our troops, other assets and foreign relations."

> "CONSUMERS AND TAXPAYERS MAY NOT REALIZE IT, BUT BENEATH THE SURFACE, THE RISING THREAT OF CYBER ATTACKS, COMPUTER VIRUSES AND IDENTITY FRAUD IS COSTING THEM BILLIONS."
>
> — Henry Truc, personal finance writer for GoBankingRates.com

How effective were hacktivists?

According to the BBC, the websites targeted by Anonymous experienced service disruptions, but the attacks on credit card companies left transaction processing capabilities unaffected. MasterCard acknowledged it experienced a "service interruption" in some Web-based services, but neither its core processing capabilities nor its cardholder account data were compromised. Ted Carr, spokesman for Visa, told the BBC that the network handling cardholder transactions continued normal operations. Anonymous originally announced an attack on Amazon, but later shifted its target to PayPal. The online money transfer service reported that its blog went offline, but that transactions continued, though more slowly than usual.

Other attacks were more successful. News reports indicated that Swiss bank PostFinance suffered disruptions for 10 hours and the website of the Swedish prosecutors handling Assange's sexual assault case was taken down for several hours.

Anonymous aimed high with its attacks on Visa, MasterCard, PayPal and Amazon. Visa and MasterCard are the two largest consumer payment systems in the world, reporting 2010 revenues of $8 billion and $5.5 billion, respectively. PayPal, a subsidiary of online auctioneer eBay, announced revenue of almost $2.8 billion in 2010. There is nothing to indicate that the DDOS attacks caused significant financial damage to the targeted companies, amounting to little more than virtual graffiti on the online bank "lobbies."

The aftermath

After the attacks by Wikileaks supporters, law enforcement officials arrested several people. Five hacktivists from Anonymous were arrested in England in January 2011, although police there declined to confirm their involvement. Additionally, two teenage hackers were arrested in the Netherlands in December 2010. As of early 2011, police in Europe and North America continued to issue arrest warrants for suspects associated with the unlawful cyber attacks.

Though these recent attacks were largely unsucessful, they focused attention on the potential for criminals and terrorists to create large-scale financial havoc and expose confidential credit data to the world. British officials estimate that Internet attacks and viruses cost the world economy about $86 billion annually, a cost ultimately borne by consumers and taxpayers. Securing financial institutions and other critical civilian infrastructure will clearly remain a costly challenge. □

Europe's Mixing Bowl

Integrating minorities will benefit the region

In July 2010, an officer with France's National Gendarmerie shot and killed a Roma man in the small village of Saint-Aignan. According to police, the man was wanted in connection with a burglary and had sped through two police checkpoints, injuring an officer. Two days later, dozens of Roma from a nearby camp, armed with hatchets and iron bars, attacked the local police station and rioted in the streets. BBC News reported that in the aftermath of the riots, French President Nicolas Sarkozy "promised that those responsible for the violence would be 'severely punished,' " and ordered hundreds of illegal Roma camps to be destroyed and many illegal occupants repatriated to their countries of origin. That same day, Muslim youth also rioted in the French city of Grenoble after an ethnic North African armed robbery suspect died in a shoot-out with police.

AGENCE FRANCE-PRESSE

Sarkozy's crackdown was designed to project a tough law enforcement response to an alarmed public concerned with increasing violence centered in Roma and other ethnic minority communities. Instead it has initiated a contentious trans-European debate over minority rights and integration of ethnic minorities, a debate many in Europe, including civil rights groups dedicated to fighting anti-Roma discrimination, believe has been too long in coming. As Tara Bedard of the European Roma Rights Centre told the BBC: Sarkozy's campaign had finally put Roma issues "at the center of Europe's agenda." However, the debate is relevant not only to the Roma community but also to growing Muslim immigrant communities from Central Asia, the Middle East and North Africa.

Multiethnic Europe

The first Roma, of Indian descent, arrived in Europe no later than the 14th century and were commonly known as Gypsies because they were believed — inaccurately — to have originated in Egypt. The current Roma population in Europe, estimated at 11 million to 16 million, is the continent's largest and fastest-growing ethnic minority. Roma have suffered various levels of discrimination and abuse throughout centuries of European history. Endemic discrimination, combined with the Roma's insular, self-protective and nomadic culture, led to mutual fear and distrust between the Roma and their host communities. In modern Europe, Roma continue to experience high unemployment, widespread illiteracy and endemic poverty.

The Roma are a somewhat unusual case study for the failure — or rejection — of cultural integration. Understanding the situation of the Roma minority in Europe and the history of Roma interrelations with majority cultures is essential to "effectively address the profound social, political, and cultural challenges the Roma face in Europe," according to Iskra Uzunova, writing in the *Arizona Journal of International & Comparative Law*. It should also be useful in developing unified European policies on minority rights and integration with regard to more recent groups of immigrants from Asia and Africa.

The modern wave of immigration began as European countries, rebuilding from World War II, sought immigrants to compensate for labor shortages. Like the Roma, they arrived in Europe with cultures, languages and religions that differed significantly from those of ethnic Europeans. Many of these Asian and African immigrants were Muslim, and the first wave came predominantly from Europe's former colonies, with Pakistanis and Bangladeshis moving to the United Kingdom and Algerians moving to France. Germany and the Netherlands also attracted large numbers of Muslim immigrants, from Turkey and Indonesia respectively. Because most early immigrants came for economic reasons and didn't intend to stay, they "had no vision of themselves

A child eats in the arms of a woman in a camp of Roma people in Villeneuve-d'Ascq, France, a day after their deportation from another camp. The U.N. anti-racism committee urged France to "avoid" collective deportations of Roma.

Roma and Romanian children study together in Darvari, Romania. Roma children suffer from segregation and discrimination in education in many European countries.

AGENCE FRANCE-PRESSE

AGENCE FRANCE-PRESSE

Imams attend a service to inaugurate the new Omar Mosque in Berlin's Kreuzberg district during the inauguration of the Islamic Maschari Centre. Europe's Muslim population is growing rapidly.

Ozlem Cekic, a newly elected member of the Folketinget, the Danish parliament, poses with her newborn daughter in Copenhagen. Cekic and Yildiz Akdogan, are the first ever female Muslim members of the Danish parliament.

REUTERS


AGENCE FRANCE-PRESSE

as Western or European Muslims," Olivier Roy of the French National Center for Scientific Research said. Integration might have seemed irrelevant to the first generation, but the second and third generations "are here to stay," Roy said.

Immigrants tend to congregate with others from their home countries, or even hometowns, where they try to re-create social networks and support structures. Esther Ben-David of the *Middle East Quarterly* asserted that this "immigration dynamic" limits interaction with the rest of society, leading immigrants to build insular societies that inhibit cultural integration. In this way, Muslim immigrants partly resemble the Roma, who have maintained an "ethnocentric" separation from predominant European culture. Although this separation helps ease the transition to Europe and limits exposure to discrimination, segregation — voluntary or not — can itself contribute to prejudice and discrimination by inhibiting cross-cultural understanding.

Segregation, discrimination and radicalization

According to the European Union Counterradicalization Strategy, published in 2008, political and cultural factors are most prevalent in radicalization of European Muslim immigrants. Poor political representation is a leading contributor. "The lack of political prospects" can result in a feeling that nonpolitical means are necessary to address grievances. The document also pointed to "marginalization in employment, education and housing, as well as negative stereotyping and prejudicial attitudes." This leads to alienation and a strengthened attachment to, and perhaps distorted understanding of, native culture and religion. "Integration and Security: Muslim Minorities and Public Policy in Europe and the United States," a report from Rutgers University, asserted that post-9/11 security initiatives have impeded the integration of Muslim immigrants and led to greater discrimination and alienation. "In effect, extreme security measures have countermanding effects resulting in a 'security/insecurity paradox': The struggle for security leads to greater radicalization."

Ethnic and cultural separation also limits economic opportunity. In Eurozine, Nikoleta Popkostadinova reported that even before the global recession, official Roma unemployment rates ranged from 50 percent to 75 percent in Central and Eastern Europe. The data also show that Roma continue to face discrimination, as Roma unemployment rates are three times those of the rest of the population when adjusted for education levels. The Roma also suffer from discrimination in education, compounding the severity of the problem. Popkostadinova said that in Bulgaria, "a policy of effective segregation has deprived generations of Roma a chance to advance towards equal participation in the labor market."

Integration failure costs society as a whole, not only the affected minorities. Productivity suffers when the talents of an entire group are withheld from the economy. There is less competition and potential shortages of qualified workers, reducing production and gross domestic product. Bulgarian economists

Headscarves are displayed in a women's fashion stall at the annual meeting of French Muslims organized by the Union of Islamic Organisations of France. Strictly secular France banned the wearing of Muslim headscarves and other conspicuously religious apparel in public schools, hospitals and government buildings.

Lachezar Bogdanov and Georgi Angelov authored a report arguing that the Roma are an untapped source of economic potential, advocating for investment in education and occupational training.

The economic potential of the Muslim community is also underutilized. The 2005 riots in French Muslim ghettos have been widely blamed on high rates of unemployment among Muslim youth. A 2005 Congressional Research Service Report on integration of European Muslims noted Muslim unemployment rates were up to three times higher than those of the entire population, a discrepancy that suggests discrimination is sometimes involved. Belgian businesswoman Imane Karich, writing in a report by the Centre for European Policy Studies, emphasized that Muslims came to Europe in pursuit of economic opportunity. "The Islamic ethos emphasizes the importance of education, trust and hard work as the main components of economic development," she said.

Moving forward

Europe continues working to create diverse and integrated societies that include the Roma, Muslims and other ethnic minorities. To "manage diversity" in an increasingly diverse Europe, the European Council initiated the Intercultural Cities program in 2008. Based on the premise that "successful cities and societies of the future will be intercultural," the program began with 11 pilot cities creating strategies for intercultural integration.

Though integration is uneven, success stories proliferate. Muslims have been elected to parliament in the U.K., the Netherlands, Denmark, France and Germany. After the 2009 elections, the EU Parliament included 11 Muslim members. The Centre for European Policy Studies reported that Muslims are increasingly successful in business and academia, helped by the EU's Muslim Council of Cooperation in Europe.

Western European nations, struggling with a large migration of Roma from Eastern Europe, have called on Romania and Bulgaria to do more to integrate their Roma citizens. The new EU countries, joined by nongovernmental organizations and Roma rights advocates, look to the EU to create a comprehensive Roma policy. Portuguese State Secretary for European Affairs Pedro Lourtie explained: "Considering this is not just one nation's issue, the EU must play a part in integrating these groups."

Bogdanov and Angelov's report called for a more innovative and proactive approach. They propose to focus on occupational training rather than welfare and support a "short-term increase in government spending to expedite mobilization of the Roma into the labor force." Romanian Gelu Domenica agreed: "We must change our discourse from the human rights perspective to reasons to invest in Roma communities. We need to make the state aware that labor in the Roma community is cheaper and easier to find than bringing in labor from abroad."

Education is key to opportunity

Successful integration of ethnic minorities depends on educational systems that have not always treated Muslims and Roma as equal players. A joint report on Roma migration from the Organization for Security and Co-Operation in Europe and the Council of Europe cited "severe under-attainment by Roma at school and the perpetuation of intergenerational under-attainment in schooling via practices of racially segregated educational facilities, arbitrary refusals to enroll Romani children and other similar practices." A 2006 EU publication titled "Muslims in the European Union: Discrimination and Islamophobia" reported that ethnic minorities do not perform as well in school and are much more likely to leave school earlier.

But integration is a two-way street. Traditionally, many Roma, especially in Central and Eastern Europe, have an ingrained cultural distrust of formal education, which contributes to illiteracy and poverty. Jake Bowers, a British ethnic Roma journalist, pointed out that Roma have traditionally placed little value on formalized education, preferring the freedom of self-education and self-employment. "Education remains a double-edged sword for many Gypsies," Bowers noted on the Travellers' Times Online website. "It is valued as a way of learning to read and write, but distrusted because of the 'cultural pollution' that comes with it."

Some European Muslims also view public education as a cultural threat. According to a study by Holger Daun and Reza Arjmand in *Review of Education*: "Often parents who have emigrated from predominantly Islamic areas feel uncertain about the opportunities in their new home countries to foster Muslim values and norms in their children. For many of these parents, Islamic moral training is important, whether it takes place in the formal education system or in non-formal socialization arrangements."

Job training and education will empower the Roma and Muslim communities in Europe and allow them to realize their economic potential. But to integrate and enjoy the economic opportunities available in Europe, ethnic minorities must acclimate to the societies in which they live, leaders from countries such as Great Britain and Germany reiterated in 2010 and 2011. A European program that successfully integrates a historically insular ethnic group such as the Roma could provide a model for integration of other immigrant groups, reducing the cultural alienation that can lead to radicalization and creating more productive and prosperous intercultural communities. As British Prime Minister David Cameron told attendees at the Munich Security Conference in February 2011, many European countries, by opting for "state multiculturalism," have inadvertently segregated citizens by ethnicity and religion. "Instead of encouraging people to live apart," Cameron said, "we need a clear sense of shared national identify that is open to everybody." □

Inside Cyber Warfare

By Jeffrey Carr
Sebastopol, CA: O'Reilly Media, 2009; 240 pages

Reviewed by Lt. Col. Joe Matthews
Managing Editor, *per Concordiam*

Jeffrey Carr uses his wealth of experience and knowledge in cyber warfare to consolidate a collection of articles in the informative book *Inside Cyber Warfare*. Carr is a cyber expert and the founder and CEO of Taia Global, a U.S.-based information and cyber security company. He specializes in the investigation of cyber attacks. In his book, he touches briefly on the issues facing nations that are attempting to protect critical data, while facilitating information sharing. His book is a rapid-fire attempt to educate policymakers and security officials on the challenges of protecting cyberspace. This book is a quick read for those familiar with the Internet and an insightful experience for casual users of cyberspace who want to dive deeper to understand security issues.

The book simply and directly points out one of the biggest problems for decision-makers regarding cybersecurity: There is no international agreement on what constitutes a cyber attack. The examples of recent cyber attacks and the notion of nations fighting a war of ideas in cyberspace, searching for victory without human casualties, are powerful images of what the future could hold. The book also contains a very detailed description of the rise of the nonstate hacker.

Some of the most pressing concerns discussed are the legal status of cyber warfare and attribution. Along with their murky legal status is the need for increasing police cooperation and strengthening policy to address illegal cyber activity. Investigating cyber crime — and identifying the culprits — is another difficulty. Anonymity in cyberspace is one of the main reasons why organized crime prospers online. The book lays out detailed examples of how criminal organizations and nonstate hackers are able to operate anonymously on the Internet.

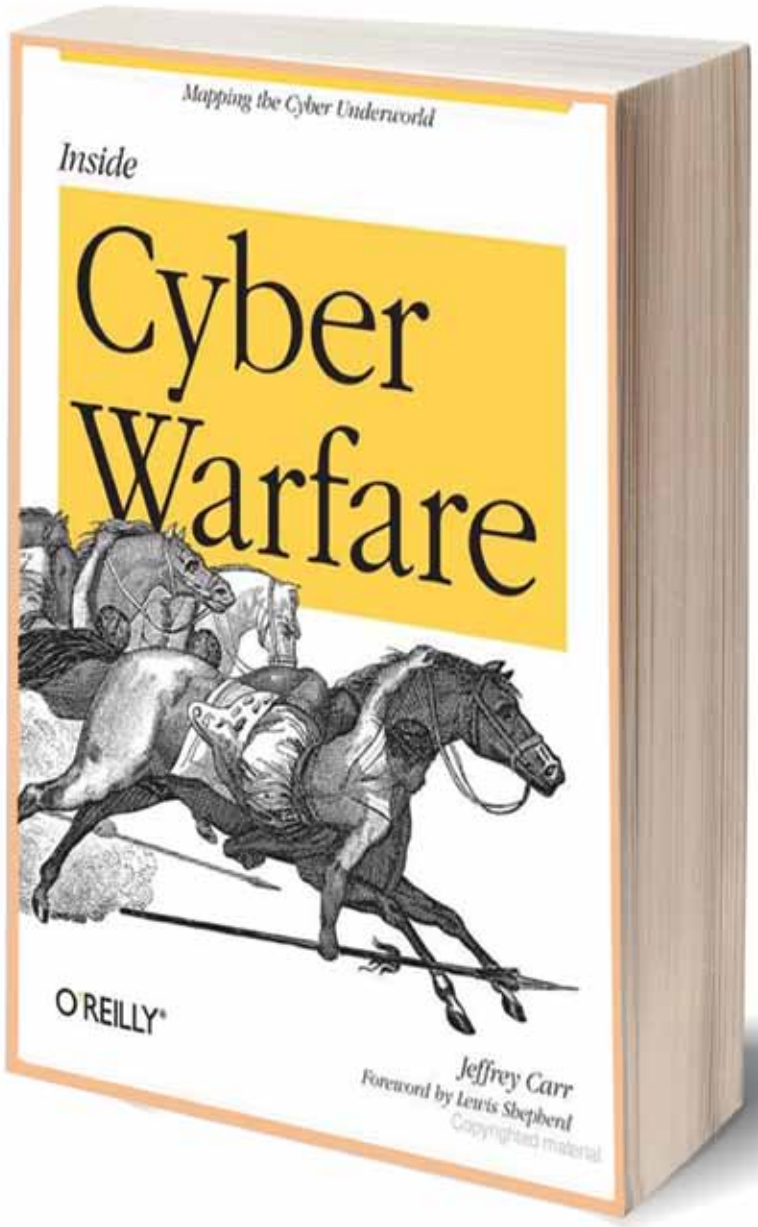
The chapter on nonstate hackers and the social Web makes a convincing argument for the power of social media to galvanize support for a political cause. The Internet is now a medium for informational awareness, advancing education, and the collection of support for social action.

> “The book lays out detailed examples of how criminal organizations and nonstate hackers are able to operate anonymously on the Internet.”

This unprecedented volume of communication allows the transmission of false reporting. Under the guise of truthful information, these falsehoods try to influence a specific section of a society or nation.

If the reader has time for only one chapter, he should read the chapter describing a cyber early warning model. This chapter was written by Ned Moran, a senior intelligence analyst and adjunct professor in intelligence studies at Georgetown University in Washington. Moran describes the construction of an analytical framework to predict the possibility of politically motivated cyber attacks. He uses three case studies to support his framework. A more predictive method of locating the source of a possible cyber attack could greatly enhance the capabilities of emerging national cybersecurity centers.

Inside Cyber Warfare is worthwhile reading for policymakers, even if they are only reading the last chapter of the book. This chapter includes advice from a collection of articles recommending ideas such as policy changes, operating system changes and holding Internet-hosting and service providers accountable for illegal activities. One such recommendation is switching from the Microsoft Windows operating system to Red Hat Linux to eliminate the majority of malware threats. Other advice includes shifting to an active defense policy for critical information systems and taking a whole-of-nation approach to cyber security. This is substantive advice for those in a position to ignite change. □



Disclaimer: The views and conclusion of this book review are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

Resident Courses

Democratia per fidem et concordiam

Democracy through trust and friendship

Registrar
George C. Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany

Telephone: +49-8821-750-2656
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, e-mail requests to: registrar@marshallcenter.org

PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

The five-week, twice yearly program addresses the different aspects of threats to nations and is for mid- and upper-level management, military, government and police officials in counterterrorism organizations. The focus is on combating terrorism while adhering to the basic values of a democratic society. The five-module course provides a historical and theoretical overview of terrorism, the vulnerabilities of terrorist groups, the role of law, the financing of terrorism and security cooperation.

PTSS 12-3
February 10 –
March 16, 2012
(Nominations due Dec. 16, 2011)

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	29			

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

PROGRAM IN ADVANCED SECURITY STUDIES (PASS)

The Marshall Center's flagship course, a 12-week, twice yearly program, is rigorous and intellectually stimulating and provides graduate-level study in security policy, defense affairs, international relations and related topics. It consists of core studies and electives, including assigned readings, seminar discussions, debates, panels, role-playing exercises and field studies. Participants must be proficient in one of the three languages in which the program is taught: English, German or Russian.

PASS 12-5
March 23 –
May 31, 2012
(Nominations due Jan. 27, 2012)

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

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					

May

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		

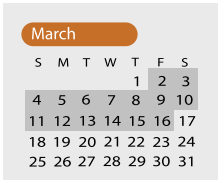
SEMINAR ON COMBATING WEAPONS OF MASS DESTRUCTION/TERRORISM (SCWMD/T)

The two-week seminar provides national security professionals a comprehensive look at combating weapons of mass destruction (WMD) and the challenges posed by chemical, biological, radiological and nuclear (CBRN) threats by examining best practices for ensuring that participating nations have fundamental knowledge about the issue.

SCWMD/T 12-4

March 2-16, 2012

(Nominations due Jan. 6, 2012)



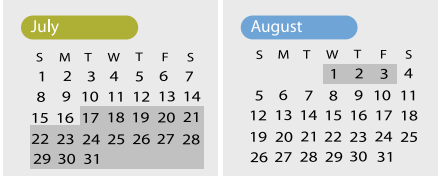
SEMINAR ON TRANSATLANTIC CIVIL SECURITY (STACS)

The seminar is a three-week, twice-a-year class that provides civil security professionals from Europe, Eurasia and North America an in-depth look at how nations can effectively address domestic security issues with regional and international impact. Organized into four modules — threats and hazards, prepare and protect, response and recover, and a field study — it focuses on the development of core knowledge and skills.

STACS 12-7

July 17 – August 3, 2012

(Nominations due May 22, 2012)



THE SENIOR EXECUTIVE SEMINAR (SES)

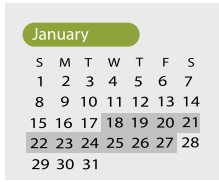
The seminar is a forum that allows for the in-depth exploration of international security issues. Participants in winter and fall sessions include high-level government officials, general officers, senior diplomats, ambassadors, ministers and parliamentarians. The SES format includes presentations by senior officials and recognized experts followed by discussions in seminar groups.

SES 12-1

January 18-27, 2012

(Nominations due Nov. 22, 2011)

"Events in North Africa and Arab Middle East - Impact on Europe and Eurasia."



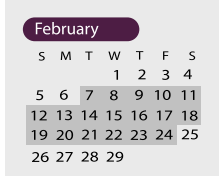
THE STABILITY, SECURITY, TRANSITION, AND RECONSTRUCTION (SSTaR)

The program is a three-week, twice-a-year course that addresses why and when stability, security, transition and reconstruction operations are required in the global security environment and how a nation can participate productively. Its four modules focus on the challenges inherent to SSTaR, the basic organizational and operational requirements of such operations, and the capacity-building resources available to participant nations.

SSTaR 12-2

February 7-24, 2012

(Nominations due Dec. 13, 2011)



Alumni Support Office

Dean Dwigans
Tel +49 8821 750 2378.
dwigansd@marshallcenter.org

Barbara Wither
Coordinator for: Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Kosovo, Macedonia, Montenegro, Romania, Serbia, Slovenia, Turkey

Languages: English, Russian, German

Tel +49-(0)8821-750-2291
witherb@marshallcenter.org
Building 102, Room 206 B

Chris O'Connor
Coordinator for: Belarus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Moldova, Poland, Slovak Republic, Ukraine

Languages: English, Russian, Polish

Tel +49-(0)8821-750-2706
oconnorc@marshallcenter.org
Building 102, Room 205

Milla Beckwith
Coordinator for: Afghanistan, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyz Republic, Mongolia, Pakistan, Tajikistan, Turkmenistan, Uzbekistan

Languages: English, German, Russian

Tel +49-(0)8821-750-2014
ludmilla.beckwith@marshallcenter.org
Building 102, Room 206 A

Frank Bär
Coordinator for: German Element, Germany, Austria, Switzerland

Languages: German, English

Tel +49-(0)8821-750-2814
frank.baer@marshallcenter.org
Building 102, Room 217

Randy Karpinen
Coordinator for: Russian Federation, Middle East, Africa, Southern & Southeast Asia, North and South America, West Europe

Languages: English, Finnish, German, Russian, Spanish

Tel +49-(0)8821-750-2112
karpinenr@marshallcenter.org
Building 102, Room 219

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: **http://tinyurl.com/per-concordiam-magazine**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **http://tinyurl.com/perConcordiam-Facebook**
MC Knowledge Portal: **https://members.marshallcenter.org**
Alumni Support Office: **mcalumni@marshallcenter.org**

MARSHALL CENTER PHOTO

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