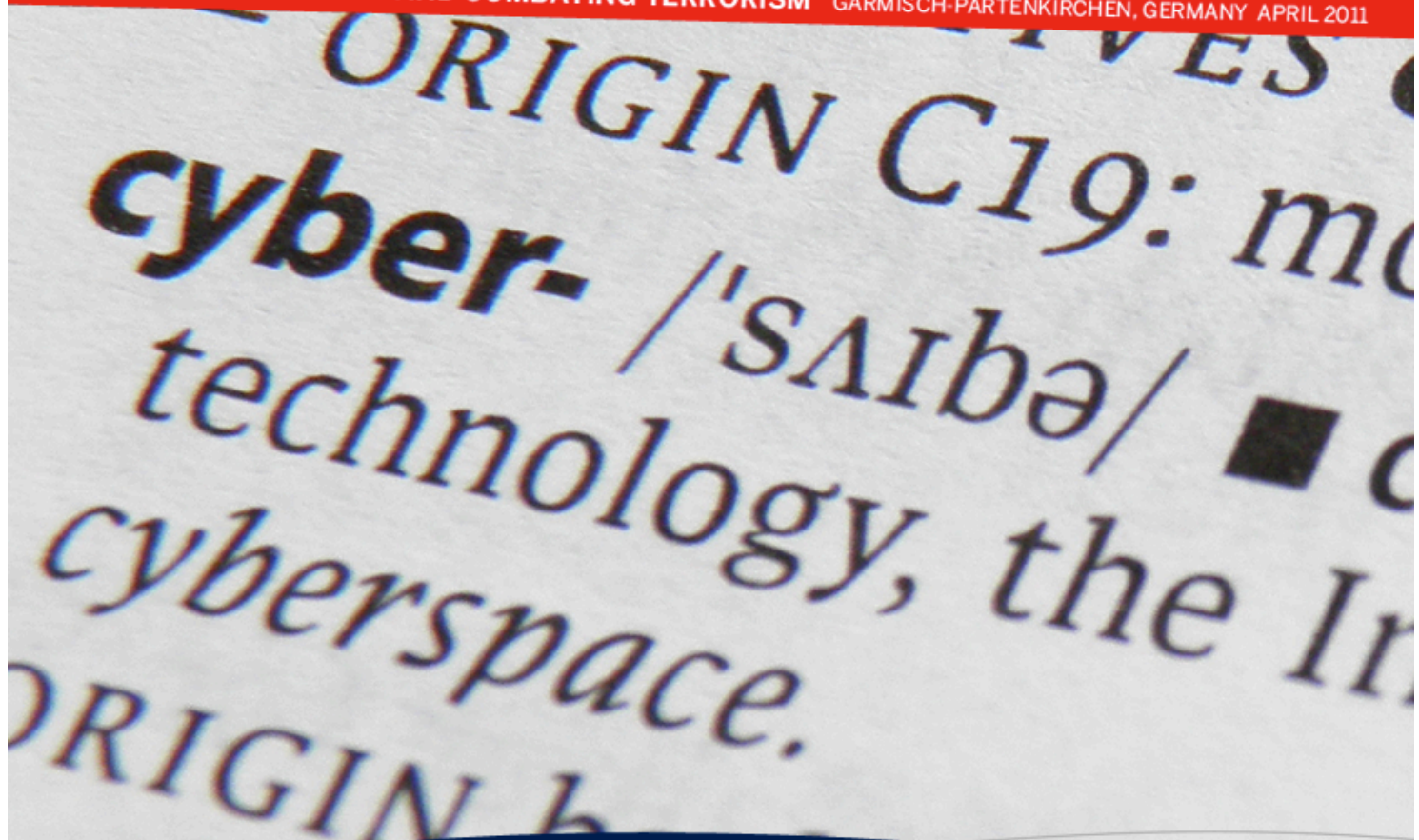


ADVANCED EDITION PREPARED FOR THE 5TH INTERNATIONAL FORUM "COOPERATION BETWEEN GOVERNMENT, CIVIL SOCIETY AND BUSINESS IN THE FIELD OF INFORMATION SECURITY AND COMBATING TERRORISM" GARMISCH-PARTENKIRCHEN, GERMANY APRIL 2011



RUSSIA-U.S. BILATERAL ON CYBERSECURITY

CRITICAL TERMINOLOGY FOUNDATIONS



**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations
Issue 1

The principle editors of this document are:

Karl Frederick Rauscher, EastWest Institute
and
Valery Yaschenko, Information Security Institute of Moscow State University.

Cover art work by Dragan Stojanovski.

Copyright © 2011 EastWest Institute and the Information Security Institute of Moscow State University

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow. For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info

www.ewi.info

Information Security Institute was founded as a separate department of Moscow University in 2003. The main aim of the Institute is to coordinate the research activity in the Moscow University, which deals with information security. For more information about the Information Security Institute, please contact:

Information Security Institute
Moscow State University
Michurinskiy prospeky, 1
Moscow, RUSSIA, 119192
7 495 932-8958
iisi@iisi.msu.ru

www.iisi.msu.ru

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS

KARL FREDERICK RAUSCHER & VALERY YASCHENKO
Chief Editors



**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

(This page intentionally left blank.)

Dedication

To those pioneers of the Russia-American relationship during the last half century,
who have avoided an unspeakable conflict.

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

(This page intentionally left blank.)

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS

Foreword

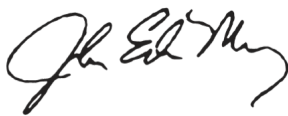
During the past year, there has been an explosion of interest in the need to create “rules of the road” for cyberspace. Unlike the domains of land, sea, air, and space, there are no agreed upon “rules of the road” for the cyber world. The first essential step in moving forward is to secure international agreement on the definitions of key terms. For years, the UN and other bodies have sponsored efforts to create agreed upon definitions of critical terminology in the cyber and information security field. These efforts have been slow and have not led to the kind of results that are needed. Many have called for Track 2 initiatives to take on the task.

The EastWest Institute’s Worldwide Cybersecurity Initiative and Moscow State University’s Information Security Initiative agreed to create a joint effort between American and Russian experts to seek consensus definitions around three key cluster areas of cybersecurity terminology, which we call *The Theatre*, *The Modes of Aggravation* and *The Art*. Our experts have created this conceptual framework as way to facilitate the challenging process of creating definitions for a common international lexicon – a necessary first step in achieving those “rules of the road.”

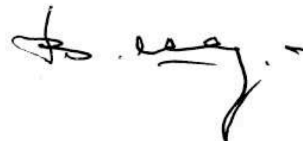
Many colleagues from Moscow and Washington were dubious that such an effort could succeed. Our fourteen colleagues, under the impressive leadership of Karl Rauscher and Valery Yaschenko, have taken on the challenge by delivering this typology and an initial twenty defined terms. We believe that this effort represents a beginning that can be built upon – both bilaterally, between our countries – and multilaterally.

We appreciate the invitation to present an advanced copy of this report at the Fifth International Forum "Cooperation between Government, Civil Society and Business in the Field of Information Security and Combating Terrorism" this month in Garmisch-Partenkirchen. Feedback from such a distinguished forum of colleagues is welcomed and will be used to tighten our presentation to the 40-nation Second Worldwide Cybersecurity Summit in London on June 1 and 2, 2011.

We look forward to moving onto the next phase of this project and trust that the work we have produced here will advance the work of many others, as we move towards the goal of seeing the international community come together and secure the breakthroughs that are so needed in the cyber and informational security field.



JOHN EDWIN MROZ
President & CEO
EastWest Institute



VLADISLAV P. SHERSTYUK
Director, Information Security Institute
Moscow State University

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

(This page intentionally left blank.)

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS

Preface

Herein are twenty terms that define cyber and information security. The objective for this exercise was to begin the long-overdue foundation building for broader “rules of the road” discussions regarding this emerging frontier for high-stakes conflict.

There are five compelling reasons why Russia and the United States form the ideal partnership for starting such an initiative. First, a cold war between our two countries has been a central preoccupation for much of the last century. Thus follows the second, that the calculations performed by our countries about the other were successful enough to avoid the dreaded, unthinkable mutually assured destruction. In fact, the larger historical statement is that our two countries have never been at war with each other. Third, Russia and America are two of the world’s cyber superpowers that have long defined the cutting edge of scientific and technical discovery and mastery. Fourth, our two countries, spanning three continents, represent very diverse histories and ideologies and nurture a proactive view for the world. Finally, both Russia and America have clear interests in worldwide stability, prosperity and peace.

We are both indebted to our team members, each of who has world-class expertise in a field related to this taxonomy, its utility and its implications.

These terms are submitted to the broader international community for review and improvement. This taxonomy is scheduled to be submitted for discussion at the Fifth International Forum “Cooperation between Government, Civil Society and Business in the Field of Information Security and Combating Terrorism,” this April in Garmisch-Partenkirchen, the EWI-IEEE Second Worldwide Cybersecurity Summit this June in London and the EWI Worldwide Security Conference this October in Brussels. In addition, consultations with members of the EWI Cyber40 and International Information Security Research Consortium (IISRC) are anticipated throughout this process.

Forward with the discussion and progress!



KARL FREDERICK RAUSCHER

Leader, U.S. Experts
Chief Technology Officer
& Distinguished Fellow
EastWest Institute

New York City, USA



VALERY YASCHENKO

Leader, Russia Experts
Senior Vice-Director,
Information Security Institute
Moscow State University

Moscow, Russia

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

(This page intentionally left blank.)

Contributors¹

Russian Federation

Sergey Komov, Information Security Institute

Andrey Kulpin, Information Security Institute

Alexey Salnikov, Information Security Institute

Anatoliy Strelcov, Security Council Staff

Vladimir Ivanov, EastWest Institute

United States of America

Charles (Chuck) Barry, National Defense University

John S. Edwards, Digicom, Inc.

J. B. (Gib) Godwin, RADM (ret.), Northrop Grumman

Stuart Goldman, Bell Labs Fellow (ret.)

Paul Nicholas, Microsoft Corporation

James Bret Michael, U.S. Naval Postgraduate School

Jack Oslund, George Washington University (ret.)

¹ Please see the biographies section for a short background of each of the primary contributors.

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

(This page intentionally left blank.)

Acknowledgements

Special recognition and sincere appreciation is here expressed

to **Vartan Sarkissian** and **Vladimir Ivanov**,
for their vision and persistence in opening the door for this opportunity.

to **Franz-Stefan Gady**,
for his project management of the engagement and vigorous policy analysis.

to **Andrew Nagorski**, **Tracy Larsen**, **Dragan Stojanovski** and **Abigail Rabinowitz**,
for their quality control of publication and for leading the communications processes.

to **Greg Austin** and **Terry Morgan**,
for their steady and continuous support and encouragement for the Russia-U.S. bilateral program.

to **Anatoly Safonov**, **Vladislav Sherstyuk**, **Andrey Krutskikh**, **Sergey Kislyak**,
William Burns, **Michael McFaul**, **John Beyrle**, **Don Kendall, Sr.**, and **John Edwin Mroz**,
*for their foresight and encouragement of such Track 2 Russian-American cooperative efforts
on the most challenging global security problems.*

and finally, to our wider community of respective stakeholder confidants
in Moscow, Washington, D.C. and around the world,
*whose appreciation for innovation in Track 2 engagements
ensures the work's long-term value.*

Contents

DEDICATION 5

FOREWORD 7

PREFACE 9

CONTRIBUTORS 11

ACKNOWLEDGEMENTS 13

CONTENTS 14

1. INTRODUCTION..... 15

 OBJECTIVES AND IMPORTANCE 15

 INFORMATION AND CYBER 16

 SCOPE 17

2. CONSENSUS DEFINITIONS 18

 2.1 THE THEATRE 19

 2.2 THE MODES OF AGGRAVATION 26

 2.3 THE ART..... 32

3. NEXT STEPS 42

BIOGRAPHIES..... 43

 CHIEF EDITORS 43

 CONTRIBUTING SUBJECT MATTER EXPERTS 44

REFERENCES 47

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

1. Introduction

The time is past due for clarity around policies for nation-state matters of high consequence in cyberspace. Indeed there is unacceptable chaos regarding the meaning of even the most basic terms – cyberspace, cyber war, cyber attack, etc. Given the serious actions of the last several years in cyberspace, it is very well-reasoned to believe that, at any time, the interpretation of one of these terms could be a watershed in determining whether or not a certain cyber action would result in intensified or violent escalation.

Russia and the United States form the ideal partnership for an initiative to generate the initial momentum toward a useful taxonomy. Among other factors, both countries are respected for their competence in the field, managing of the nuclear tensions of the modern age, and interests that promote worldwide stability, prosperity and peace.

This document is a tangible step forward toward the goal of reasonable clarity around the taxonomy of cyber conflict. It is intended to serve as a catalyst for multilateral collaboration on the subject matter.

Objectives and Importance

Three objectives were set for this bilateral engagement. The first objective was to *open genuine dialogue* between subject matter experts and stakeholders from both countries. The second objective, built on the first, was to *develop deeper understanding* of each other's perspectives. The third objective was to *establish consensus* around initial definitions of critical terms for cyber and information security.² This taxonomy is submitted for consideration, review and improvement, so that the terms can be refined and used to help enable eventual formal agreements between the two countries, and as a reference for other nation-states.³ The first two objectives were met, as is evidenced from the contents of this report. Time is needed to determine the achievement toward the third objective.⁴

The motivation for embarking on a joint effort to define cybersecurity terminology is quite clear. Many experts and stakeholders around the world feel that the time for international agreements, or “rules of the road,” is long overdue.⁵

² The constructions “cyber and information security” and “information and cyber security” were agreed to by the combined team to refer to the larger set of interests. In this construction, the words “cyber” and “security” are deliberately separated to accommodate the parallel construction as well as interests addressed in the following section. Elsewhere the compound word “cybersecurity” is used.

³ e.g., Track 1

⁴ At the time of publication, plans are underway for multiple follow-up engagements for continued dialogue and implementation of the guidance provided herein.

⁵ *Summary of Participants Polling Results*, EWI-IEEE First Worldwide Cybersecurity Summit, Dallas, May 2010.

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

For the Americans on the team, this Track 2 initiative was seen as a fulfillment of new policy for cyberspace. The 2009 *White House Cyberspace Policy Review* outlined several priorities for the U.S., naming international cooperation as its seventh point of a “Near Term Action Plan.” Specifically, the objective was laid out to “strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.”⁶

For the Russians on the team, this bilateral cooperation was seen as fulfilling United Nations guidance to develop taxonomy. They cited the June 2010 *Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, which recommended “further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions: ... (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.”⁷

Thus the goal was not to simply harmonize existing cybersecurity terms, of which there are plenty in different national documents (standards, national laws, etc.). Rather the bigger goals included confidence-building, genuine understanding and momentum for creating more expansive efforts in the arena of “rules of the road.”

The expectation is for these terms to be used first in a broader international collaboration toward defining key terms and building a common taxonomy. Thus these terms have no binding effect, but rather provide an enabling function to engage stakeholders from around the world in this important and timely objective. The manifestation of their value will be in the convergence around common definitions in the coming years. Equally of value could be the sharper contrast and clarity where irresolvable differences remain.

This first step is indeed a significant because it is born of Russian-American collaboration and because it is tangible progress.

Information and Cyber

One of the largest hurdles to overcome in the bilateral discussions was the fundamental disagreement on the starting point for the discussion. There were two perspectives:

The Russian view of information security emphasizes the holistic span of information, where cyber is one component along with others. They see information as being either artificial or natural. Cyber is artificial, and is seen as the technical representation of information. In addition to what would be included in cyber, information also includes thoughts in one’s head and information in books and documents. Further, the Russians see a logical assumption that a discussion should encompass all information, and not just a subset (i.e. cyber).

⁶ *White House Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Table 1: Near Term Action Plan, Washington, D.C., 2009, p. vi.

⁷ http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

The Russian word most equivalent to the English “security” denotes “protection.” Their view of *security of information* includes several dimensions: human, social, spiritual and technical factors (i.e. cyber). It also considers protecting the population from terrorism and censorship to be an essential aspect of “information security.”⁸

The Americans are more interested in addressing data in the emerging electronic infrastructures. They acknowledge that other information exists outside of the “cyber” arena, but feel that this is not where the need for focus is at this time. In the bilateral effort they wanted the focus to be more narrowly on the emerging cyberspace. Beyond this, there were other reasons why Americans were interested in focusing on “cybersecurity.” For one, Americans do not see information protection as something that should include censorship, or any attempt to control the population’s awareness. The thinking being that the most aware and educated population is best able to defend against harmful information. Finally, the American team believed that a government would be acting inappropriately if it used psychological operations on its citizens.

After acknowledging these differences in perspectives, an agreement was reached to restrict discussion to cyber, which was acknowledged by the combined team as being a subset of the “information” superset. More specifically, resolution came about when both sides agreed to move forward by (i) acknowledging the broader scope of “information,” (ii) recognizing that “cyber” was a subset of this larger scope, and (iii) focusing on “cyber” because it is the area that required the most attention.

Scope

There are three parameters that best define the boundaries of this discussion. These are (i) the initial *parties* being Russia and the U.S.⁹, (ii) the *focus* being ‘information and cyber security,’ with the initial discussion limited to the latter, and (iii) the *nature* of the work is to draft definitions and propose taxonomy to seed multilateral conversations.







⁸ Critical Information Space was defined as the aggregate of elements of information space that are identified as essential by national government or by international agreements.

⁹ This work was conducted by experts from Russia and the U.S. Each expert is a citizen of their respective country and had been engaged in some critical aspect related to the interests of their national security. As a Track 2 collaborative effort, these individuals were not official government authorities. The leaders of both expert groups provided periodic briefings to their respective stakeholders in Moscow and Washington, D.C. The collective experience of these experts exceeds several hundred years and includes the broad range of expertise needed for an examination of the subject matter.

2. Consensus Definitions

This section presents twenty terms for which the Russian and American experts were able to come to an agreement. The most basic arrangement of these terms is oriented around three areas: *The Theatre*, *The Modes of Aggravation* and *The Art*.










The Theatre

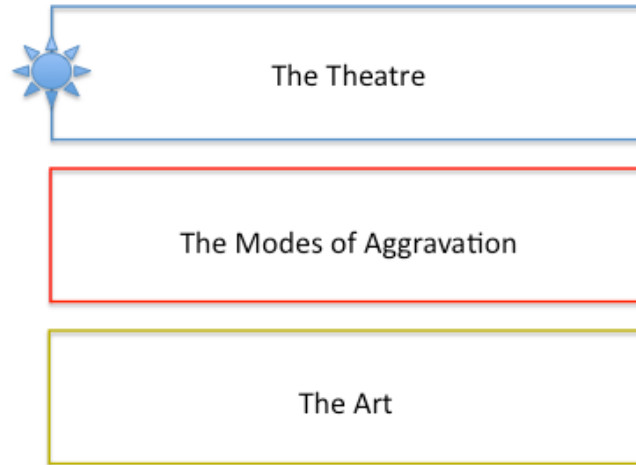
-  Cyberspace
-  Cyber Infrastructure
-  Cyber Services
-  Critical Cyberspace
-  Critical Cyber Infrastructure
-  Critical Cyber Services

The Modes of Aggravation

-  Cyber Crime
-  Cyber Terrorism
-  Cyber Conflict
-  Cyber War
-  Cybersecurity

The Art

-  Cyber Warfare
-  Cyber Attack
-  Cyber Counter-Attack
-  Cyber Defensive Countermeasure
-  Cyber Defense
-  Cyber Defensive Capability
-  Cyber Offensive Capability
-  Cyber Exploitation
-  Cyber Deterrent



2.1 The Theatre

This section presents consensus definitions for six terms, namely: cyberspace, cyber infrastructure, cyber services, critical cyberspace, critical cyber infrastructure and critical cyber services. Each of the initial three terms has a critical subset, which make up the final three definitions.

The relationship between cyberspace, cyber infrastructure and cyber services is not easily shown in a simple graphic, without conveying misinformation. Cyberspace is built with cyber infrastructure. Likewise cyber services make cyberspace of interest and value to users. Cyber services are performed by the systems that constitute cyber infrastructure.

The six definitions are presented here.

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS

Cyberspace¹⁰

is ^aan electronic medium through which ^binformation is ^ccreated,
^dtransmitted, ^ereceived, ^fstored, ^gprocessed, and ^hdeleted.

Киберпространство

^aэлектронная (включая фотоэлектронные и пр.) среда, в
(посредством) которой информация ^бсоздаётся, ^впередаётся,
^гпринимается, ^дхранится, ^еобрабатывается ^жи уничтожается.

¹⁰ Commentary

Important considerations for this term include the following:

Cyber has roots in the Greek word κυβερνητικός - meaning skilled in steering or governing. The term “cybernetics” is widely recognized as being coined in the book *Cybernetics or Control and Communication in the Animal and the Machine* (MIT Press, 1948). The author, Norbert Wiener, applied the term to in the context of the control of complex systems in the animal world and in mechanical networks. The term would later be used in the medical community in reference to the integration of humans or animals with machinery. However, since cyber has been introduced it has taken on several meanings. The term is used effectively in business, law and policy. The term currently has highly useful application in that it can readily provide a reference to the other-than-physical, virtual world created by the Internet and other electronic communications.

On the other hand, **cyberspace** does not exist without the physical ingredients from which it is composed.

The compound word’s inclusion of the word “space” implies that it should have dimension. That is, **cyberspace** must occupy an expanse. In addition, cyberspace is considered by some as a new domain like land, sea space, outerspace. However, as these for were natural, cyber is artificial, being created by man.

Known definitions were consulted during this process. The U.S. Department of Defense has a documented definition as “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” See *Dictionary of Military and Associated Terms*, U.S. Department of Defense, 31 January 2011. Pages 92-93. (CJCS CM-0363-08)

Cyber Infrastructure¹¹

is ^athe aggregation of people, processes and systems ^bthat constitute **cyberspace**.

Киберинфраструктура

^aсовокупность людей, процессов (в том числе управляющих), ^би систем, составляющих киберпространство

¹¹ *Commentary*

Important considerations for this term include the following:

The **cyber infrastructure** consists of the eight essential ingredients of 1. Environment (buildings, locations of cell towers, space where satellites orbit, sea floors where cables are laid, etc.), 2. Power (electricity, batteries, generators, etc.), 3. Hardware (semiconductor chips, electronic cards and circuit packs, metallic and fiber optic transmission facilities, etc.), 4. Software (source code, compiled programs, version control and management, databases, etc.), 5. Networks (nodes, connections, topologies, etc.), 6. Payload (information transported across the infrastructure, traffic patterns and statistics, information interception, information corruption, etc.), 7. Human (designers, implementers, operators, maintenance staff, etc.), and 8. Policy, or more completely Agreements, Standards, Policies and Regulations (ASPR). Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

The worldwide trend is for more and more legacy infrastructure to become reliant upon computers and networked, thus becoming more integrated with **cyberspace**.

Known definitions were consulted during this process.

Cyber Services¹²

are ^aa range of data exchanges in cyberspace ^bfor the direct or indirect benefit of humans.

Киберсервисы (услуги, службы)

^aразличные виды обмена данными в киберпространстве, ^bдля прямой или косвенной пользы людям

¹² *Commentary*

Important considerations for this term include the following:

A **cyber service** is provided by an application. This application may be provided by processes and data that are distributed throughout **cyberspace**. This means that the systems can be located in a wide variety of actual geographic locations.

Cyber services can be online or offline, performed by local or remote processing, in real-time or completed by time-delayed connectivity or processing.

These **cyber services** must now be viewed as an open-ended concept, as many new services are expected that have not even been imagined yet (i.e. IPv6 potential to have a vastly larger number of connected entities).

Known definitions were consulted during this process.

Critical Cyberspace¹³

is ^a**cyber infrastructure** and **cyber services** that are vital to ^bpreservation of ^cpublic safety, ^deconomic stability, ^enational security ^fand international stability.

Критически важное киберпространство

^a[часть (элементы) киберинфраструктуры и киберуслуг], которые необходимы для осуществления, ^bжизненно важных функций поддержания, ^bобщественной безопасности, ^гэкономической стабильности, ^днациональной безопасности, ^емеждународной стабильности

¹³ *Commentary*

The term represents a subset of **cyberspace**.

Known definitions were consulted during this process.

Critical Cyber Infrastructure¹⁴

is ^athe **cyber infrastructure** that is essential to ^bvital services for ^cpublic safety, ^deconomic stability, ^enational security, ^finternational stability and ^gto the sustainability and restoration of **critical cyberspace**.

Критически важная киберинфраструктура

^aкиберинфраструктура, которая необходима для, ^bосуществления жизненно важных функций, ^vподдержания общественной безопасности, ^гэкономической стабильности, ^енациональной безопасности, ^жмеждународной стабильности, (^з) а также для поддержания работоспособности и функций эффективного восстановления [критически важного киберпространства

¹⁴ *Commentary*

Important considerations for this term include the following:

The most critical infrastructures are often those providing communications, energy, transportation, financial services and continued operation of government. Thus the computers and network operations required for the basic operation of the most important aspects of these sectors are critical.

Some countries are more fully dependent on **critical cyber infrastructure** than others. This is partially due to increased sophistication and partially due to the loss of a low-tech back-up option.

Known definitions were consulted during this process.

Critical Cyber Services¹⁵

are ^a**cyber services** that are vital to ^bpreservation of ^cpublic safety, ^deconomic stability, ^enational security ^fand international stability.

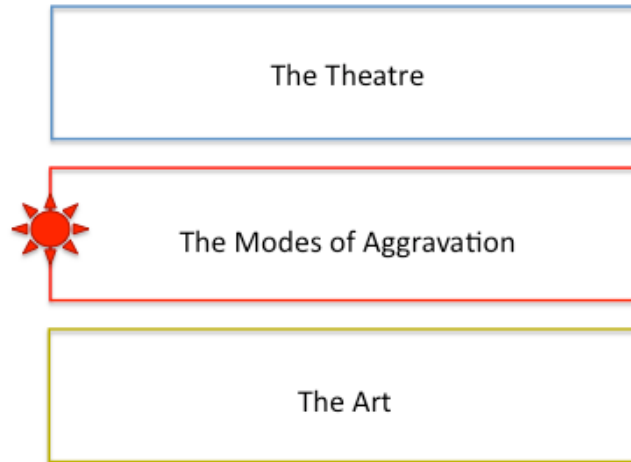
Критически важные Киберсервисы (услуги, службы)

^aчасть (элементы)] киберсервисов (услуг, служб), которые необходимы для осуществления, ^bжизненно важных функций поддержания, ^vобщественной безопасности, ^гэкономической стабильности, ^Анациональной безопасности, ^емеждународной стабильности

¹⁵ *Commentary*

The term represents a subset of **cyber services**.

Known definitions were consulted during this process.



2.2 The Modes of Aggravation

This section presents consensus definitions for five terms, namely: cyber crime, cyber terrorism, cyber conflict, cyber war and cybersecurity. The later being the state of non-aggravation.

The key distinction for cyber crime is that laws are broken. Likewise, a key distinction for cyber war is that it involves political actors. Cyber conflict is a state that is on a continuum with war, but falls short of a critical threshold.

The five definitions are presented here.

Cyber Crime¹⁶

is ^athe use of **cyberspace** ^bfor criminal purposes ^cas defined by national or ^dinternational law.

Киберпреступление

^aиспользование киберпространства, ^bв преступных целях, ^bкоторые определяются в качестве таковых национальным или международным законодательством

¹⁶ *Commentary*

Important considerations for this term include the following:

Given the considerable established laws that define criminal activity, the **Cyber Crime** term is deliberately designed to immediately reference existing legal structures.

It is understood that jurisdictional considerations have an integral role in application of this term. Complexities arise when activities are performed by an individual in one country, utilizing cyber resources in another (second) country, and affecting someone, organization or other entity in still another (third) country.

Cyber criminals are increasingly being categorized as significant Non-State Actors.

The Convention on Cybercrime (2001) is the first international treaty seeking to harmonize cyber crime legislations across countries. It was drawn up by the Council of Europe with the United States participating as an observer. The U.S. has ratified the treaty, whereas Russia has not.

Known definitions were consulted during this process.

Cyber Terrorism¹⁷

is ^athe use of **cyberspace** ^bfor terrorist purposes ^cas defined by national or ^dinternational law.

Кибертерроризм

^aиспользование киберпространства, ^бв террористических целях,
^вкоторые определяются в качестве таковых национальным или
международным законодательством

¹⁷ *Commentary*

Important considerations for this term include the following:

Given the extensive recent development of the definition of terrorism, the **Cyber Terrorism** term is deliberately designed with reliance on the existing work.

It is understood that jurisdictional considerations have an integral role in application of this term. Complexities arise when activities are performed by an individual in one country, utilizing cyber resources in another (second) country, and affecting someone, organization or other entity in still another (third) country.

Known definitions were consulted during this process.

Cyber Conflict¹⁸

is ^atense situation ^bbetween or among nation-states or organized groups ^cwhere unwelcome **cyber attacks** ^dresult in retaliation.

Киберконфликт

^aнапряженная ситуация между и/или среди государств и/или политически организованных групп, ^bпри которой враждебные (нежелательные) кибератаки, ^bпровоцируют (приводят) к ответным действиям.

¹⁸ *Commentary*

Important considerations for this term include the following:

Cyber attacks could include physical attacks on **cyber infrastructure**.

The attack-retaliation methods may be asymmetrical (i.e. cyber, physical). Thus the response does not have to be cyber. Nor does the attack need to be cyber in order to have a cyber response.

Cyber conflict can be a precursor to an escalated situation.

Known definitions were consulted during this process.

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS

Cyber War¹⁹

is ^aan escalated state ^bof **cyber conflict** ^cbetween or among states ^din which **cyber attacks** ^eare carried out by state actors ^fagainst **cyber infrastructure** ^gas part of a military campaign

^h(i) Declared: that is formally declared by an authority of one of the parties.

(ii) De Facto: with the absence of a declaration.

Кибервойна

^aвысшая степень киберконфликта, ^bмежду или среди государств, ^bво время которой государства предпринимают кибератаки, ^гпротив киберинфраструктур противника, ^дкак часть военной кампании;

^e(i) может быть объявлена формально одной (всеми) конфликтующими сторонами или

(ii) не объявляться формально и быть *de facto*

¹⁹ Commentary

Important considerations for this term include the following:

War exists as a state or condition between or among belligerent parties.

War has usually different phases. **Cyber conflict** usually precedes **cyber war**.

There is a tendency of conventional war to include **cyber warfare**.

If there are no political actors, then there is not a war. **Cyber war** can be more than strictly a military activity, especially at the outset, i.e. an intelligence operation. **Cyber war** can be conducted in different ways by different groups.

Known definitions were consulted during this process. A recent EWI Russia-U.S. Bilateral on Critical Infrastructure Protection Report introduced the concept of an "Other Than War" mode [see Recommendation 5 of: Rauscher, Karl Frederick; Korotkov, Andrey, *Working Towards Rules Governing Cyber Conflict – Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute Russia-U.S. Bilateral on Critical Infrastructure Protection, January 2011].

Cybersecurity²⁰

is ^aa property of **cyber space** ^bthat is an ability to resist ^cintentional and unintentional threats ^dand respond and recover.

Кибербезопасность

^aсвойство (киберпространства, киберсистемы), ^bпротивостоять, ^cнамеренным и/или, ^dненамеренным угрозам, а также, ^eреагировать на них и, ^fвосстанавливаться после воздействия этих угроз.

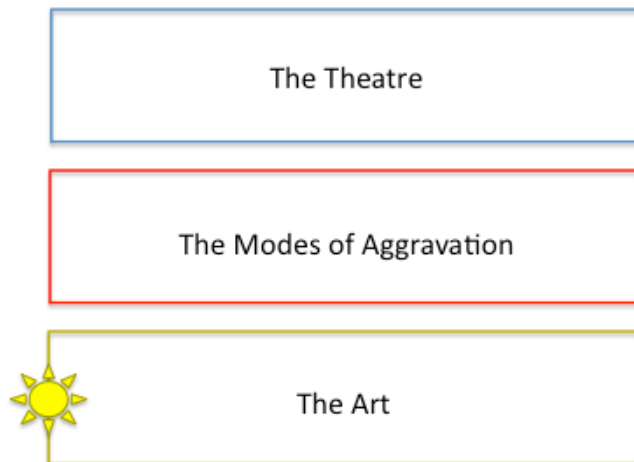
²⁰ ***Commentary***

Important considerations are included in the “information and cyber” discussion presented in Section 1.

The Russian word for “security” connotes protection, but not the additional meanings understood with the English term such as the means used to provide protection.

Known definitions were consulted during this process. Of interest is research that underscores the original concept of *being secure* is most oriented around *a sense of being safe*.

RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS



2.3 The Art

This section presents consensus definitions for nine terms, namely: cyber warfare, cyber attack, cyber counter-attack, cyber defensive countermeasure, cyber defense, cyber defensive capability, cyber offensive capability, cyber exploitation and cyber deterrent.

It is noted here that one key term yet to be presented is that of “cyber weapon.” This is significant in that several of the definitions make reference to it. Thus this is one of the terms being considered for focus during the next phase of this work.²¹

The five definitions are presented here.

²¹ The EWI Russia-U.S. Bilateral on Critical Infrastructure Protection recently offered considerable definition of a cyber weapons in the context of a system of four dispensations that are delineated by infrastructure type and weapon type. Of note from this discussion, are the observations that cyber weapons are both traditional weapons that are enhanced with ICT and purely ICT capabilities [see Section 3 of: Rauscher, Karl Frederick; Korotkov, Andrey, *Working Towards Rules Governing Cyber Conflict – Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute Russia-U.S. Bilateral on Critical Infrastructure Protection, January 2011].

Cyber Warfare²²

is ^acyber attacks ^bthat are authorized by state actors ^cagainst cyber infrastructure ^din conjunction with a government campaign.

Боевые действия в киберпространстве

^aкибератаки, ^bпроводимые государствами (группами государств, организованными политическими группами), ^cпротив киберинфраструктур, ^dи являющиеся частью военной кампании

²² *Commentary*

Important considerations for this term include the following:

Warfare refers to the acts or techniques carried out by one or more of the belligerent parties.

Known definitions were consulted during this process.

Cyber Attack²³

is ^aan offensive ^buse of a **cyber weapon** ^cintended to harm a designated target.

Кибератака

^aнаступательное, ^bиспользование [кибероружия], ^bс целью нанесения вреда определенной цели

²³ *Commentary*

Important considerations for this term include the following.

The word “harm” includes degrading, inhibiting – temporary or permanent.

An attack is only effective if it exercises an intrinsic vulnerability.

A **cyber attack** is defined by the weapon type and not the nature of the target. Thus, a **cyber attack** can be either a **cyber weapon** against a non-cyber asset or a cyber asset. But a **cyber attack** is *not* a non-cyber weapon against a non-cyber asset or cyber asset. See the previous footnote for additional insights and reference material.

Questions that the combined team left unresolved include whether the following would constitute an attack: propaganda, web site control, and an email campaign.

Known definitions were consulted during this process. The NATO Standardization Agency (NSA) has defined “computer network attack / attaque de réseaux informatiques “ (CNA) as “Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself,” with a note that “A computer network attack is a type of cyber attack.” AAP-6 (2010) - *NATO Glossary of Terms and Definitions* (English and French), 22 January 2010, page 2-C-12. This is the only use of the word “cyber” in this NATO publication. In compliance with the request of the custodian of the publication, written notification of the use of this definition here has been provided to the NSA.

Cyber Counter-Attack²⁴

is ^athe use of a **cyber weapon** ^bintended to harm a designated target ^cin response to an attack.

Киберконтратака

^aиспользование, ^бкибероружия с целью нанесения вреда определенной цели, ^вв ответ на атаку

²⁴ *Commentary*

Important considerations for this term include the following:

A **cyber counter-attack** may be asymmetrical. Thus a **cyber counter-attack** can be either a cyber weapon against a non-cyber asset or against a cyber asset. But is *not* a non-cyber weapon against a non-cyber asset or cyber asset. Thus, like a **cyber attack**, it is defined by weapon type and not the nature of the target.

Known definitions were consulted during this process.

Cyber Defensive Countermeasure²⁵

is ^athe deployment ^bof a specific **cyber defensive capability** ^cto deflect ^dor to redirect ^ea **cyber attack**.

Оборонительные средства противодействия в киберпространстве

^aразвертывание особых (оборонительных средств противодействия)
^bдля отражения и/или, ^bперенаправления кибератаки

²⁵ *Commentary*

Important considerations for this term include the following:

The inclusion of this term in this initial taxonomy related to defense is important because it helps explain the legitimate interest of nation-states to invest in the development of capabilities that may be needed to protect their interests.

Cyber defensive countermeasures are actions taken by a party as part of a defensive strategy during or after an attack on the interests of the party.

A countermeasure may be "active" or "passive." An active countermeasure could react to an attack by attempting to disrupt the attacker. A passive countermeasure could enhance a party's protection level of its interests.

Known definitions were consulted during this process.

Cyber Defense²⁶

is ^aorganized capabilities ^bto protect against, ^cmitigate from, and ^drapidly recover from ^ethe effects of **cyber attack**.

Кибероборона

^aорганизованная совокупность средств и действий, ^бдля защиты и/или, ^вдля смягчения, ^ги эффективного восстановления, ^дот враждебных кибератак (воздействий)

²⁶ *Commentary*

Important considerations for this term include the following:

Cyber defense refers to actions taken by a party to protect the interests of the party in anticipation of an attack. The inclusion of this term in this initial taxonomy related to defense is important because it helps explain the legitimate interest of nation-states to invest in the development of capabilities that may be needed to protect their interests.

Effective defense in electronic systems is typically based on detection, isolation, reporting, recovery and neutralization.

The ability to absorb an attack may be an effective defensive strategy.

An attack is only effective if it exercises an intrinsic vulnerability

Known definitions were consulted during this process.

Cyber Defensive Capability²⁷

is ^aa capability ^bto effectively protect ^cand repel ^dagainst a cyber exploitation or ^ecyber attack, ^cthat may be used as a **cyber deterrent**.

Оборонительные возможности в киберпространстве

^aвозможность эффективно защитить и/или, ^bотразить, ^bкибератаку, предотвратить киберконфликт, предупредить использование противником преимуществ в киберпространстве, ^ги которая может быть использована в качестве средства сдерживания в киберпространстве

²⁷ *Commentary*

Important considerations for this term include the following:

The inclusion of this term in this initial taxonomy related to defense is important because it helps explain the legitimate interest of nation-states to invest in the development of capabilities that may be needed to protect their interests.

Known definitions were consulted during this process.

Cyber Offensive Capability²⁸

is ^aa capability ^bto initiate ^ca **cyber attack** ^dthat may be used ^eas a **cyber deterrent**.

Наступательные возможности в киберпространстве

^aвозможность начать, ^bкибератаку, ^cкоторая может быть использована в качестве средства сдерживания в киберпространстве

²⁸ *Commentary*

Important considerations for this term include the following:

Known definitions were consulted during this process. The U.S. Department of Defense has a related definition: "cyberspace operations" being defined as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." (JP 3-0) See *Dictionary of Military and Associated Terms*, U.S. Department of Defense, 31 January 2011. Pages 92-93. (CJCS CM-0363-08)

Cyber Exploitation²⁹

is ^ataking advantage ^bof an opportunity ^cin **cyber space** ^dto achieve an objective.

Использование преимуществ в киберпространстве

^aиспользование в своих интересах, ^бимеющихся возможностей в киберпространстве, ^вдля достижения поставленной цели

²⁹ *Commentary*

Important considerations for this term include the following:

The advantage here may be either a strength of the acting party or an adversary's vulnerability.

The Russian team members indicate that this is not a term that is used in Russia.

Known definitions were consulted during this process. The NATO Standardization Agency (NSA) has defined "computer network exploitation / exploitation de réseau informatique" (CNE) as "Action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage." AAP-6 (2010) - *NATO Glossary of Terms and Definitions* (English and French), 17 January 2005, page 2-C-12. This is the only use of the word "cyber" in this NATO publication. In compliance with the request of the custodian of the publication, written notification of the use of this definition here has been provided to the NSA.

Cyber Deterrent³⁰

is ^aa declared ^bmechanism ^cthat is presumed effective ^din discouraging **cyber conflict** ^eor a threatening activity ^fin **cyberspace**.

Средства киберсдерживания

^aпризнанный, ^bмеханизм, ^bкоторый считается действенным, ^гдля препятствования, ^дкиберконфликту, ^еили угрожающей деятельности в [киберпространстве]

³⁰ *Commentary*

Important considerations for this term include the following:

The mechanisms for a **cyber deterrent** include policy, posture, weapon, capability or alliance.

Known definitions were consulted during this process.

3. Next Steps

This joint paper presents twenty consensus terms that have been agreed upon by experts from Russia and the United States. The terms are some of the most critical to defining and understanding “rules of the road” for conflict in the emerging cyber and information space. There have been multiple attempts for a Russian-American glossary for cyber terms for more than a decade. They have stalled for some of the reasons discussed throughout. This is the first to bear the intended fruit. This joint team has accomplished something with this beginning taxonomy that it hopes can be improved upon in the coming months and years. While twenty terms are a small step for most lexicons, these terms represent a significant stride, as they are the beginning of a path that must be taken if the emerging information and cyber domain is to be tamed.

The next steps include addressing “information” and “information security” more rigorously and likewise defining the relationship between these terms. Next steps also include broadening the discussion to a multilateral one. This means ensuring input from EWI’s Cyber40 and International Information Security Research Consortium (IISRC). Specific planned outreach events include multilateral engagement in:

- The Fifth International Forum, “Cooperation between Government, Civil Society and Business in the Field of Information Security and Combating Terrorism” this April in Garmisch-Partenkirchen;
- The EWI-IEEE Second Worldwide Cybersecurity Summit this June in London;
- The EWI Worldwide Security Conference this October in Brussels.

The team looks forward to the rigorous engagement that is sure to follow, to the refinement of this taxonomy that is worth the effort given the stakes for the world, and to the benefits it can offer to a world that is wandering in information and cyberspace without much-needed reference points.

BIOGRAPHIES

Chief Editors

Karl Frederick Rauscher

Karl Frederick Rauscher is Chief Technology Officer and a Distinguished Fellow at the EastWest Institute. He previously served as the Executive Director of the Bell Labs Network Reliability & Security Office of Alcatel-Lucent and is a Bell Labs Fellow. Karl has served as an advisor for senior government and industry leaders on five continents, including as vice chair of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC) industry executive committee and as leader of the European Commission-sponsored study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI). Recent publications include the IEEE Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report. Karl serves as the chair-emeritus of the IEEE Communications Quality & Reliability (CQR) advisory board and is the founder and president of the non-profit Wireless Emergency Response Team (WERT). He is an inventor with over 50 patents/pending in fields that span artificial intelligence, critical infrastructure protection, emergency communications, energy conservation, telemedicine, , has personally discovered over 1,000 software bugs in live networks, and facilitated the development of over 600 industry-consensus expert best practices.

Valery Yaschenko

Valery Yaschenko was born on the 12 of February 1947 in the Bryanskiy region USSR.

In 1967 graduated of the Mechanics and Mathematics Department of the Moscow University named after M.V.LOMONOSOV. In 1971 graduated of the post-graduate course of the same Department.

From 1971 till 1991 served on the different positions of the KGB - Committee of the State Security USSR. In 1991 retired on the rank of Colonel.

From 1991 till 2003 kept the position of the vice-chief of the mathematical studies in cryptography laboratory of the Moscow University named after M.V.LOMONOSOV. At the some period of time is an advisor of the Moscow University rector and represents him in the several Committees of the Security Council of Russian Federation.

From 2003 is employed at the position of the senior vice-Director in the Information Security Institute Moscow University named after M.V. LOMONOSOV.

He has a PhD on mathematics (1983).

Contributing Subject Matter Experts

Charles (Chuck) Barry

Charles Barry is a Senior Research Fellow at the National Defense University's Institute for National Strategic Studies. A retired military officer with extensive operational and senior staff experience, Dr. Barry has researched and published work on transatlantic relations, political-military affairs and operational command and control systems for more than 30 years. He is a member of the Pi Alpha Alpha National Honor Society in Public Administration and a Woodrow Wilson Foundation Fellow. He holds a Doctorate of Public Administration (Information Management) from the University of Baltimore.

John S. Edwards

John S. Edwards has over 51 years of experience in the telecommunications field, spanning design, analysis, and business planning. He successfully established and managed several design groups and founded three companies, one of which was later a billion dollar acquisition by a large corporation. Dr. Edwards has held senior-level management positions at a variety of companies, and represented Nortel Networks on the Industry Executive Subcommittee of the Presidential National Security Telecommunications Advisory Committee for 25 years where he chaired several committee task forces. He is currently the President of Digicom, Inc., and serves on the Department of Commerce's Information Systems Technical Advisory Committee. He holds a PhD in Electrical Engineering from the University of Pennsylvania.

J. B. (Gib) Godwin

RADM (ret) Gib Godwin currently serves as vice president of Cybersecurity and Systems Integration for Northrop Grumman Information Systems, and is leveraging his expertise in acquisition and military information systems to emerge as a thought leader and innovator in the development of new approaches to cyber-assurance. Mr. Godwin honed his acquisition expertise over 15 years in the Naval Air Systems Command and Space and Naval Warfare Systems Command and rose to the rank of Rear Admiral in the US Navy. There, he was the program executive officer (PEO) for Enterprise Information Systems, where he served as the Department of the Navy's interface with industry on all land-based network systems.

Stuart Goldman

Stuart Goldman contributed to the computer and telecommunications industries for 45. During this period he architected a number of communication systems and participated extensively in several national and international standards bodies, including in a variety of leadership roles. He has been granted 28 patents and has an additional 50 pending applications. Stuart is a Bell Labs Fellow.

Vladimir Ivanov

Vladimir Ivanov is the Director of the EastWest Institute's Moscow Office. Before his current position, he was responsible for managing EWI's Fiscal Transparency Program, including the publication of a series of studies on fiscal flows between the Russian federal budget and the regions. In 2006-2009 he played a leading role in EWI's cooperation with Russia on promoting international private-public partnerships to

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

combat terrorism, particularly in the areas of cybersecurity, critical infrastructure protection and countering illicit trade in precious metals and gemstones. Vladimir currently is involved in all EWI projects with a 'Russia dimension,' particularly US-Russia bi-lateral dialogue on cybersecurity and Euro-Atlantic Security. His previous professional experience includes work in the fields of social sciences research, business journalism and public relations. Vladimir is the author of numerous articles published in the *Russki Telegraf* and *Vremya Novostej* on Russian economics. He received a B.A. in International Journalism and a PhD in History from the Moscow State Institute of International Relations (MGIMO). In addition to his native Russian, Vladimir is fluent in English and French.

Sergey Komov

Sergey Komov graduated from Kiev High School of Radio Engineering of Air Defense with a diploma of Military in radio Engineer. He holds a Doctor's degree in Military Science, is a Professor, and an author of more than 100 scientific works dedicated to information warfare and information security, including 8 certificates of invention authorship. Took part in the development of *The Doctrine of Information Security of the Russian Federation*. He is a member of experts groups on international information security of the Ministry of Defense of Russian Federation. He took part in conferences for this problem in format of the UN Group of Government Experts (2004-2005), Shanghai Cooperation Organization (2006-2009), Collective Security Treaty Organization (2008-2009). Scientific Adviser to the Director of the Lomonosov Moscow State University Institute of Information Security Issues.

Andrey Kulpin

Andrey Kulpin is the Director's Adviser for International Cooperation of the Institute of Information Security Issues (IISI), Lomonosov Moscow State University. He has also worked with and consulted to other United Nations entities including and the United Nations Counter-Terrorism Implementation Task Force on measures to counter terrorist use of the Internet and Anti-Terrorist Unit group of experts of The Organization for Security and Co-operation in Europe and the United Nation's Office on Drugs and Crime on transnational organized cybercrime.

James Bret Michael

James Bret Michael is a Professor of Computer Science and Electrical Engineering at the U.S. Naval Postgraduate School. He is an expert on distributed systems and trustworthy, dependable computing. Dr. Michael is the Lead Technical Advisor to the Group of Experts for the Tallinn Manual on the Law of Armed Conflict in Cyberspace. He is a Senior Member of the Institute of Electrical and Electronics Engineers, is a recipient of the IEEE Reliability Society's Engineer of the Year Award, and holds a Ph.D. in Information Technology from George Mason University.

Paul Nicholas

J. Paul Nicholas leads Microsoft's Global Security Strategy and Diplomacy Team, which focuses on driving strategic change to advance infrastructure security and resiliency, both within Microsoft and externally. He has over a decade of experience addressing global challenges related to risk management, incident response, emergency communications, and information sharing. Mr. Nicholas has served as White House Director of Cybersecurity and Critical Infrastructure Protection, Assistant Director at the U.S. Government Accountability Office, a senior Senate staffer, and as an analyst for the Department of Defense. He earned his B.A. from Indiana University and his M.A. from Georgetown University, and is a Certified Information Systems Security Professional.

**RUSSIA-U.S. BILATERAL ON CYBERSECURITY
CRITICAL TERMINOLOGY FOUNDATIONS**

Jack Oslund

Jack Oslund has over 40 years of experience in government, industry and academia in the areas of national security and international communications. He holds a Ph.D. in International Studies from the School of International Service of the American University. He was a faculty member at the National Defense Intelligence College, was on the international staff at the White House Office of Telecommunications Policy, and has held senior management positions at the Communications Satellite Corporation. He also participated in the National Security Telecommunications Advisory Committee (NSTAC) and has taught as an adjunct professor at George Washington University. He was a Senior Fellow at the University's Homeland Security Policy Institute.

Alexey Salnikov

Alexey Salnikov is vice-director of Information Security Institute of Moscow State University named after M. V. Lomonosov. His education includes programs at the Technical Department of Highest School of the KGB, where he specialized in mathematics and cryptology. His additional education includes the participation in programs at the George C. Marshall European Center for Security Studies. From 1990 through 2003 he served in different positions of the KGB, including the Committee of State Security, USSR; the Federal Agency of Government Communications and Information (FAPSI), Russian Federation; and the Federal Security Service (FSB), Russian Federation. He retired with the rank of Colonel. From 2003 he has been employed at Lomonosov Moscow University. He is the author of more than 30 articles, and co-author of one monograph on mathematical issues of cryptology. His current interests are political issues of cybersecurity, Internet monitoring, cryptographic protocols, and mathematical problems of cryptology.

Anatoly Streltsov

Anatoly Streltsov is the head of the department of the Security Council of the Russian Federation and Full State Counselor of the Russian Federation of the 3rd class, colonel (retired). He graduated from Leningrad Suvorov military school (1964) and Kalinin Artillery Military Academy (1969). He has been on the staff of the Security Council of the Russian Federation since 1995. He holds a Doctor of technical science (1987), a Doctor of juridical science (2004), the title of professor (1994), and is a Corresponding Member of the Academy of Cryptography of the Russian Federation (2005). Also, he currently serves as an Adviser to the Director of the Lomonosov Moscow State University Institute of Information Security Issues.

REFERENCES

In English

Dictionary of Military and Associated Terms, U.S. Department of Defense, 31 January 2011.

Glossary of Terms and Definitions (English and French), NATO Standardization Agency (NSA), AAP-6, 2010.

National Information Assurance (IA) Glossary, Committee on National Security Systems, CNSS Instruction No. 4009, 26 April 2010.

Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

Rauscher, Karl Frederick; Korotkov, Andrey, *Working Towards Rules Governing Cyber Conflict – Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute Russia-U.S. Bilateral on Critical Infrastructure Protection, January 2011.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. www.unidir.org/pdf/activites/pdf5-act483.pdf

In Russian

Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации» www.rg.ru/2006/07/29/informacia-dok.html

ГОСТ Р 50922-96 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения www.minpech.ru/zaschita_info/928.html

Доктрина информационной безопасности РФ www.scrf.gov.ru/documents/5.html



Институт Восток-Запад



Information Security Institute