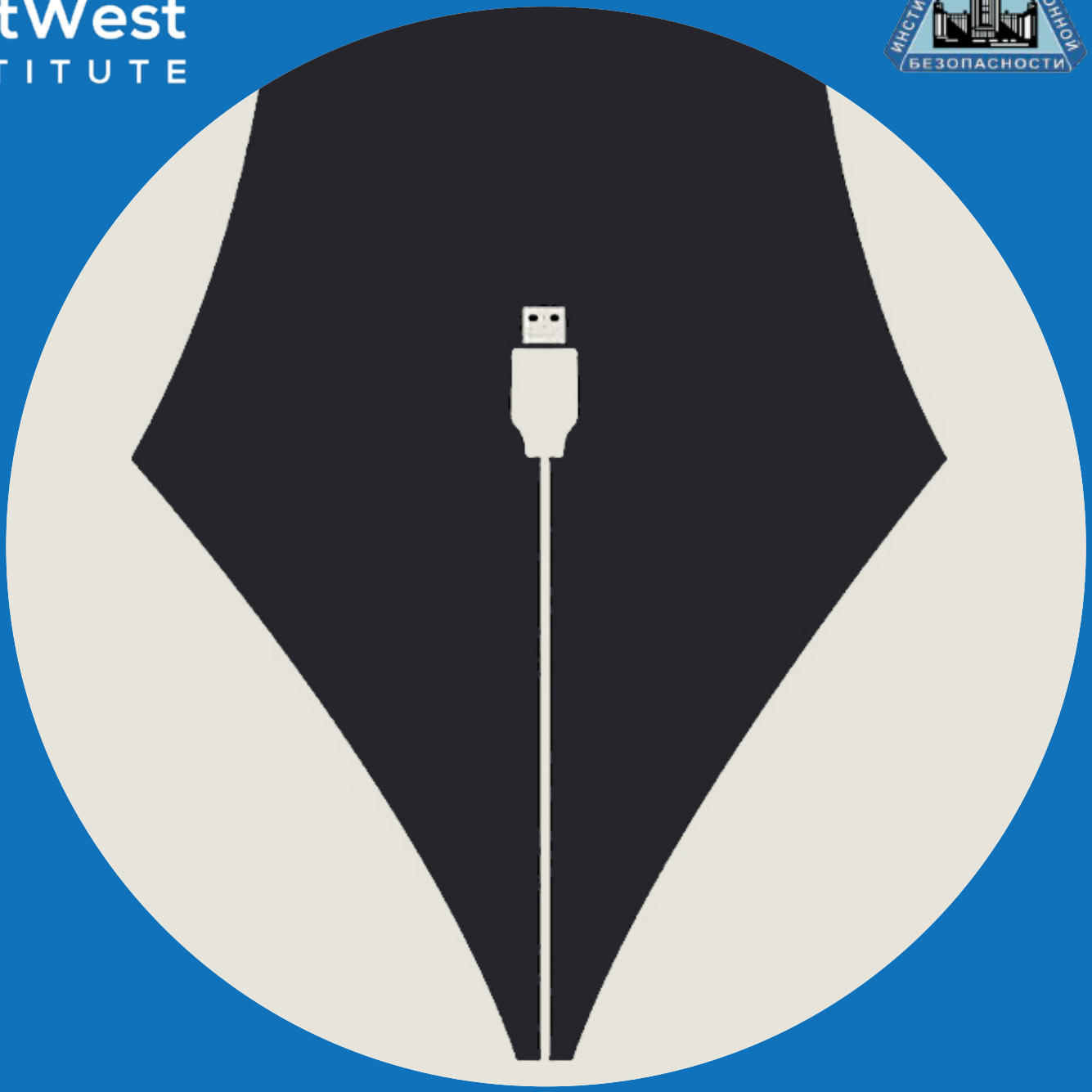
EastWest INSTITUTE

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Critical Terminology Foundations 2

Russia-U.S. Bilateral on Cybersecurity

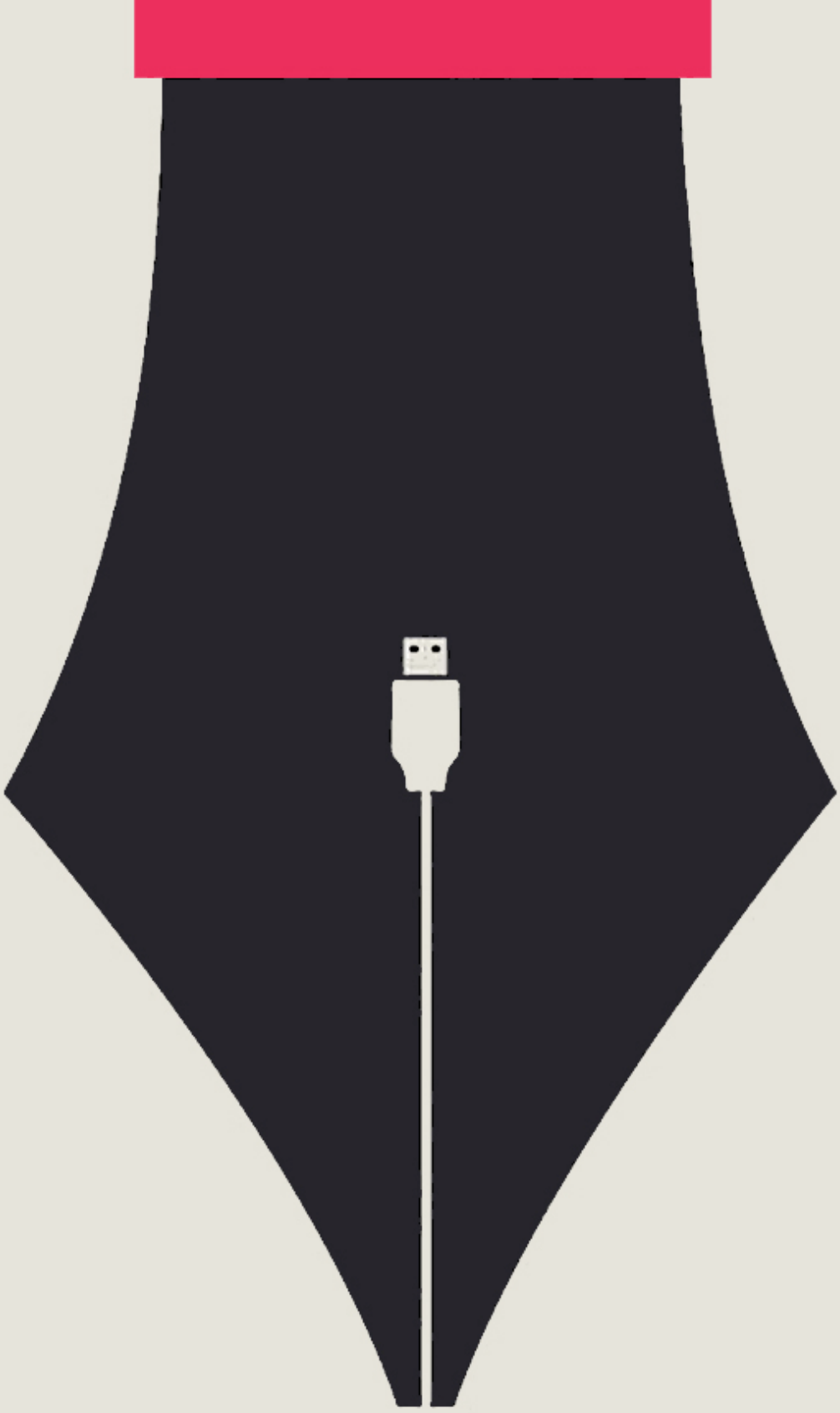
POLICY REPORT

2/2014

Russia-U.S. Bilateral on Cybersecurity

Critical Terminology Foundations 2

James B. Godwin III, Andrey Kulpin,
Karl Frederick Rauscher and **Valery Yaschenko**
Chief Editors



The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2

–

The principle editors of this document are:
James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko

–

Cover artwork by Dragan Stojanovski
ISBN No. 978-0-9856824-4-6

–

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a global go-to place for building trust, influencing policies and delivering solutions.

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 State University (MSU) in 2003. The Institute's main aim is to coordinate the research activity on information security at MSU. 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

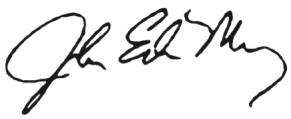
Foreword

In June 2013, Presidents Vladimir Putin and Barack Obama signed a historic agreement to begin cooperation on cybersecurity. The mutual understanding developed through previous work by our institutions to define critical terminology for cyber conflict helped prepare the way for that agreement. There is increasing international attention to the importance of ongoing definitional work in cyber, including that of the 2012 United Nations Group of Governmental Experts (GGE).

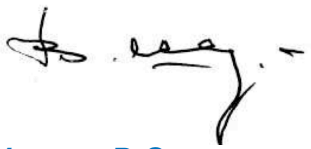
Since our first report was issued, both countries and the world have witnessed an increasing need for new "rules of the road" for cyberspace. Ultimately, the essential building blocks for any international agreements are words that convey the same meaning to each party involved. The challenge of cyberspace is unlike any other in history in the degree of its complexity, the speed of its advance and the number of key concepts that are often beyond the grasp of non-technically trained diplomats.

Our institutions were fortunate to once again have at the helm for this study a world-class team of science, technology, engineering and mathematics (STEM) professionals integrated with stakeholders with military, policy and legal training. This report, based on work from our nations' superb teams in a Track 2 process, has yielded another 20 terms.

We present this report as a small but important step in making the world a safer place for all of us.



John Edwin Mroz
President & CEO
EastWest Institute



Vladislav P. Sherstyuk
Director, Information Security Institute
Moscow State University

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

Preface

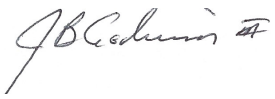
With the increasing frequency of cyber incidents, unattributable accusations within and outside of borders, and expanding use of networks to probe systems worldwide, there is an ever growing need to check the escalation of these intrusions and establish norms by which we can multilaterally agree. Specifically, the fundamental tenets of a common set of language continued to rise to the surface of any conversation as the worldwide rhetoric has continued to escalate in the cybersecurity domain.

In 2011, the EastWest Institute together with the Information Security Institute of Moscow State University took an initiative and led a much needed discussion. As a result, 20 terms were established through our initial bilateral negotiations and publication in April 2011. Building on then-established collaborative relationship, the joint team reinitiated the discussion in 2013, to further define critical terms. While the initial negotiations were bilateral in nature, the overriding intent is for these efforts to become multilateral by expanding negotiations to other nations that seek to create a consensus on what has clearly been an ill-defined and unstructured arena.

The two teams have contributed greatly both in their individual compilations, bilateral negotiations, collaborations, and, most importantly, in the ever growing trusting relationship that has developed from our initial efforts in 2011. While this report superficially represents 20 additional agreed terms, the robust, substantive and ongoing nature of these negotiations is building on the foundation, required for recurring bilateral discussions beyond the bounds of terminology to establish accepted worldwide standards in the cyber and information domains.

This set of terms was presented at the fourth World Cyberspace Cooperation Summit in Silicon Valley, USA, in November 2013, as an addendum to the original document. As these terms serve as a foundation and catalyst for multilateral efforts, we welcome and encourage comments, opinions and suggestions that could improve them.

Our intention is to make these efforts an ongoing and expanding universe of agreed terms without defining a scope or set of limitations. Join us in this journey!



RADM (ret.) J.B. Godwin III
Leader, US Experts
President, BriteWerx, Inc.
& Senior Fellow
EastWest Institute

Andrey Kulpin
Leader, Russia Experts
Director, International Center
Information Security Institute
Moscow State University

Contributors[1]

Russian Federation

Vladimir Ivanov, EastWest Institute

Sergey Komov, Information Security Institute*

Andrey Kulpin, Information Security Institute

Alexey Salnikov, Information Security Institute

Anatoly Streltsov, Information Security Institute

Valery Yaschenko, Information Security Institute

United States of America

Merritt Baer, Merritt Rachel Baer, LLC, and EWI Senior Fellow **

Charles (Chuck) Barry, National Defense University

John S. Edwards, Digicom, Inc.*

J. B. (Gib) Godwin III, RADM (ret.), BriteWerx, Inc. and EWI Senior Fellow

Stuart Goldman, Bell Labs Fellow (ret.) and EWI Senior Fellow

Luis Kun, National Defense University**

Paul Nicholas, Microsoft Corporation*

James Bret Michael, U.S. Naval Postgraduate School*

Jack Oslund, George Washington University (ret.)

Karl Frederick Rauscher, former CTO, EastWest Institute and Bell Labs Fellow

*Issue I contributors only
**Issue II contributors only

Special appreciation is expressed here for Nadiya Kostyuk for her broad research and translation support for the team.

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

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 Anatoly Safonov, Vladislav Sherstyuk, Andrey Krutskikh and John Edwin Mroz,
for their foresight and encouragement of such Track 2 Russo-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.

1 Introduction

The time is way over due for clear, agreed-upon cyberspace terms and policies. Indeed, there is unacceptable chaos regarding the meaning of even the most basic terms—cyberspace, cyber war and cyber attack. Given the seriousness of security breaches in cyberspace over the last several years, it is 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 and managing the nuclear tensions of the modern age and interests that promote worldwide stability, prosperity and peace.

This document is a tangible step forward toward clarifying 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] 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 United States, naming international cooperation as its seventh point

[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] For instance, 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 First Worldwide Cybersecurity Summit, Dallas, May 2010.

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: [...] 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, but to build confidence, genuine understanding and momentum for creating more expansive efforts in the arena of "rules of the road." While these terms have no binding effect, they provide a platform where stakeholders from around the world can engage in a broader conversation on this important and timely issue. This first step is indeed significant because it is tangible progress that was born of the Russo-American collaboration.

Discussion Disagreements: Information and Cyber

There were two disagreements in the bilateral discussions. Specifically, the Russian view of information security emphasizes the holistic span of information, where cyber is one component along with others. The Russians see information as being either natural or artificial. The latter is cyber, seen as the technical representation of information. Natural information, on the contrary, includes one's thoughts and information from books and documents. Therefore, the Russians originally wanted to lead the discussion about information and not just its subset, such as cyber. Another hurdle was over the security of information. Specifically, 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 (i.e. cyber). Moreover, this view considers the protection of population from terrorism and censorship to be an essential aspect of "information security."[8]

The Americans were more interested in addressing data in the emerging electronic infrastructures. They acknowledged that other information exists outside of the "cyber" arena, but understood that this was not where the focus should have been at the time. In the bilateral effort, they wanted their 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

[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] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *A/65/201. General Assembly*. United Nations, July 30, 2010. http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

[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.

population's awareness. The reasoning behind this is the belief 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 to influence its citizens' views and perceptions.

After acknowledging these differences in perspectives, an agreement was reached to restrict discussion to "cyber" as a subset of "information"; this agreement was acknowledged by the combined team. 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: (i) the initial parties—Russia and the U.S.[9]; (ii) the focus being "information and cybersecurity," 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.

Frameworks

Information and Communications Technology (ICT) and cyberspace are complicated and could benefit from the use of appropriate frameworks. This must be done with caution, however, as an inaccurate framework can actually make a situation more complicated by introducing confusion. The following two frameworks were utilized in this discussion.

Eight Ingredient Framework

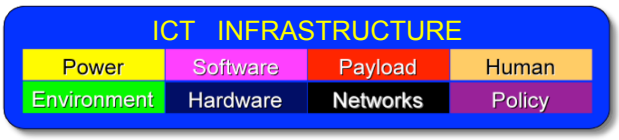


Figure 1. Eight Ingredient (8i) Framework[10]

The 8i Framework introduces the complete set (i.e. eight) of ingredients that are needed for cyberspace.

> The 8i Framework is a systematic and comprehensive framework that a) consists of the ingredients that make up communications infrastructure, b) includes all of these ingredients, c) specifies the 8 ingredients of environment, power, hardware, software, network, payload, ASPR (Agreements, Standards, Policy and Regulations; abbreviated

[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.

[10] Karl Rauscher, *Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop*, Rancho Bernardo, CA, USA, 2001; Karl Rauscher, *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

as Policy) and human. This framework is used for understanding and mastering vulnerabilities, identifying disciplines, decomposing attributes, preparing for new technologies; and other studies that support network, security and emergency preparedness.[11]

Four Dispensations for the Laws of War in Cyberspace

A Russia-U.S. Track 2 bilateral on *Rendering the Geneva and Hague Conventions in Cyberspace* introduced a framework that recognized a weapon as being either enabled by ICT (i.e. cyber) or not, as well as critical infrastructure assets as being ICT or not. While not the conventional use of cyber, it was more consistent in its treatment of the ICT presence. This consistency is important in definitions.

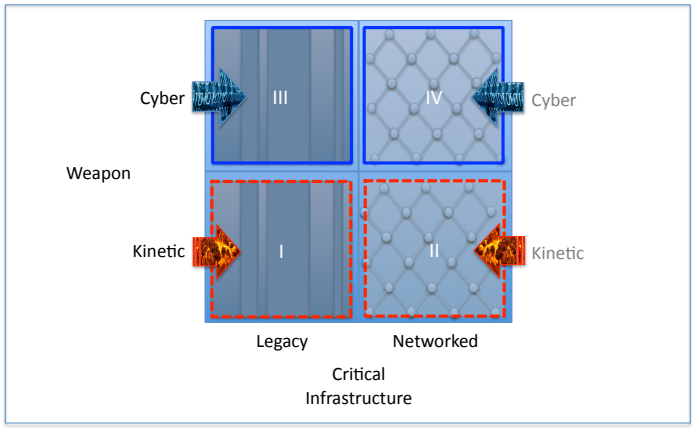


Figure 2. Four Dispensations for the Laws of War in Cyberspace[12]

[11] ATIS Telecom Glossary, www.atis.org.

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

2 Consensus Definitions

This section presents 40 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 Theater, The Modes of Aggravation and The Art.

The Theater

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

New Terms

- Information Space
- Cyber Entity
- Cyber Asset
- Cyber Forces
- Cyber Warrior

The Modes of Aggravation

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

New Terms

- Information Operation
- Information War
- Information Conflict
- Cyber Penetration
- Cyber Threat
- Cyber Exfiltration
- Cyber Espionage
- Cyber Operation

The Art

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

New Terms

- Information Superiority
- Information Operation
- Information Operations Dominance
- Information Security
- Cyber Weapon
- Cyber Vulnerability
- Cyber Intelligence

2.1 The Theater

This section presents consensus definitions for 11 terms, namely: cyberspace, cyber infrastructure, cyber services, critical cyberspace, critical cyber infrastructure, critical cyber services, information space, cyber entity, cyber asset, cyber forces and cyber warrior.

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 11 definitions are presented here.

Cyberspace[13]

is [a]an electronic medium through which [b]information is [c]created, [d]transmitted, [e]received, [f]stored, [g]processed and [h]deleted.

Киберпространство

[а]электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация [б]создаётся, [в]передаётся, [г]принимается, [д]хранится, [е]обрабатывается и [ж]уничтожается.

[13] ***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 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, air and space. However, as these four are 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, 92-93. (CJCS CM-0363-08)

Cyber Infrastructure[14]

is [a]the aggregation of people, processes and systems [b]that constitute cyberspace.

Киберинфраструктура

[а]совокупность людей, процессов (в том числе управляющих), и систем, [б]составляющих киберпространство.

[14] ***Commentary***

Important considerations for this term include the following:

The **cyber infrastructure** consists of the eight essential ingredients: 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, complied 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). Karl Rauscher, "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 networks, thus becoming more integrated with **cyberspace**.

Known definitions were consulted during this process.

Cyber Services[15]

are [a]a range of data exchanges in cyberspace [b]for the direct or indirect benefit of humans.

Киберсервисы (услуги, службы)

[а]различные виды обмена данными в киберпространстве [б]для прямой или косвенной пользы людям.

[15] ***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 to be created (i.e. IPv6 potential to have a vastly larger number of connected entities).

Known definitions were consulted during this process.

Critical Cyberspace[16]

is [a]cyber infrastructure and cyber services that are vital to [b]preservation of [c]public safety, [d]economic stability, [e]national security and [f]international stability.

Критически важное киберпространство

[а][часть (элементы)] киберинфраструктуры и киберуслуг, которые необходимы для [б]осуществления жизненно важных функций поддержания [в]общественной безопасности, [г]экономической стабильности, [д]национальной безопасности и [е]международной стабильности.

[16] ***Commentary***

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

Known definitions were consulted during this process.

Critical Cyber Infrastructure[17]

is [a]the cyber infrastructure that is essential to [b]vital services for [c]public safety, [d]economic stability, [e]national security, [f]international stability and [g]for the sustainability and restoration of critical cyberspace.

Критически важная киберинфраструктура

[а]киберинфраструктура, которая необходима для [б]осуществления жизненно важных функций [в]поддержания общественной безопасности, [г]экономической стабильности, [e]национальной безопасности, [ж]международной стабильности, а также для поддержания [з]работоспособности и функций эффективного восстановления критически важного киберпространства.

[17] ***Commentary***

Important considerations for this term include the following:

The most critical infrastructures are often those providing communications, energy, transportation, financial services and continued governmental activities. 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 due to increased sophistication and the loss of a low-tech back-up option.

Known definitions were consulted during this process.

Critical Cyber Services[18]

are [a]cyber services that are vital to [b]preservation of [c]public safety, [d]economic stability, [e]national security [f]and international stability.

Критически важные киберсервисы (услуги, службы)

[а][часть (элементы)] киберсервисов (услуг, служб), которые необходимы для [б]осуществления жизненно важных функций, поддержания [в]общественной безопасности, [г]экономической стабильности, [д]национальной безопасности и [е]международной стабильности.

[18] ***Commentary***

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

Known definitions were consulted during this process.

Information Space[19]

is [a]any medium, through which [b]information is [c]created, [d]transmitted, [e]received, [f]stored, [g]processed or [h]deleted.

Информационное пространство

[а]любая среда, в которой [б]информация [в]создается, через которую [г]передается, [д]принимается, в которой [е]хранится, [ё]обрабатывается и [ж] уничтожается.

[19] ***Commentary***

Known definitions were consulted during this process.

Cyber Entity[20]

[a]any [b]distinct [c]thing or [d]actor [e]that exists within [f]the cyber infrastructure.

Киберобъект

[а]любой [б]индивидуальный [в]объект или [г]субъект, [д]существующий в [е]киберинфраструктуре.

[20] ***Commentary***

A thing can be a person, network, etc.

Known definitions were consulted during this process.

Cyber Asset[21]

a [a]cyber entity [b]with value.

Кибератив

[а]киберобъект (киберсубъект), [б]обладающий ценностью.

[21] ***Commentary***

The owner of the asset determines its value.

Known definitions were consulted during this process.

Cyber Forces[22]

[a]cyber assets [b]organized for [c]conducting cyber operations.

Киберсилы

[а]кибератривы, [б]организованные для [в]проведения кибероперации.

[22] ***Commentary***

Known definitions were consulted during this process.

Cyber Warrior[23]

[a]a person [b]skilled and [c]directly engaging in [d]cyber warfare.

Кибербоец

[а]человек, [б]обладающий специальными навыками и [в]непосредственно вовлеченный в [г]кибервойну.

[23] ***Commentary***

Known definitions were consulted during this process.

2.2 The Modes of Aggravation

This section presents consensus definitions for 13 terms, namely: cyber crime, cyber terrorism, cyber conflict, cyber war, cybersecurity, information operation, information war, information conflict, cyber penetration, cyber threat, cyber exfiltration, cyber espionage and cyber operation.

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 13 definitions are presented here.

Cyber Crime[19]

is [a]the use of cyberspace [b]for criminal purposes [c]as defined by national or [d]international law.

Киберпреступление

[а]использование киберпространства [б]в преступных целях, [в]которые определяются в качестве таковых национальным или [г]международным законодательством.

[19] ***Commentary***

Important considerations for this term include the following:

Given the 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 the 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 Terrorism[20]

is [a]the use of cyberspace [b]for terrorist purposes [c]as defined by national or [d]international law.

Кибертерроризм

[а]использование киберпространства [б]в террористических целях, [в]которые определяются в качестве таковых национальным или [г]международным законодательством.

[20] ***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 this 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 a person, organization or other entity in the third country.

Known definitions were consulted during this process.

Cyber Conflict[21]

is a [a]tense situation [b]between and/or among nation-states and/or organized groups [c]where unwelcome cyber attacks [d]result in retaliation.

Киберконфликт

[а]напряженная ситуация [б]между и/или среди государств и/или политически организованных групп, [в]при которой враждебные (нежелательные) кибератаки [г]провоцируют (приводят) к ответным действиям.

[21] ***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.

Cyber War[22]

is [a]an escalated state [b]of cyber conflict [c]between or among states [d]in which cyber attacks are carried out by state actors [e]against cyber infrastructure [f]as part of a military campaign

[g](i) Declared: that is formally declared by an authority of one of the parties.

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

Кибервойна

[а]высшая степень [б]киберконфликта [в]между или среди государств, [г]во время которой государства предпринимают кибератаки [д]против киберинфраструктур противника, [е] как часть военной кампании;

[ё](i) может быть объявлена формально одной (всеми) конфликтующими сторонами, или

(ii) не объявляться формально и быть de facto.

[22] ***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 this 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 Karl Rauscher & Andrey Korotkov, *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].

Cybersecurity[23]

is [a]a property of cyberspace [b]that is an ability to resist [c]intentional and/or unintentional threats [d]and respond and recover.

Кибербезопасность

[а]свойство киберпространства (киберсистемы) [б]противостоять [в]намеренным и/или [г]ненамеренным угрозам, а также [д]реагировать на них и [е]восстанавливаться после воздействия этих угроз.

[23] ***Commentary***

Important considerations are included in the "Discussion Disagreements: Information and Cyber" discussion presented in Section 1.

The Russian word for "security" connotes protection. No additional meanings, such as the means to provide this protection, are implied by the Russian word for "security," whereas the English term "security" includes such means.

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*.

Information Operation[24]

[a]organized activities to [b]gather, [c]prepare, [d]disseminate, [e]restrict or [f]process [g]information [h]to achieve a goal.

Информационная операция

[а]организованная деятельность по [б]сбору и накоплению, [в]подготовке, [г]распространению, [д]ограниченю в доступе, или [е]обработке [ё]информации [ж]для достижения поставленной цели.

[24] ***Commentary***

Known definitions were consulted during this process.

Information War[25]

is [a]an escalated state [b]of information conflict [c]between or among states [d]in which information operations [e]are carried out by state actors [f]for politico-military purposes.

Информационная война

[а]высшая степень [б]информационного конфликта [в]между государствами, [г]когда информационные операции [д] проводятся государственными структурами для [е]достижения военно-политических целей.

[25] ***Commentary***

Known definitions were consulted during this process.

Information Conflict[26]

is [a]a tense situation [b]between or among nation-states or organized groups [c]where information operations [d]result in retaliation.

Информационный конфликт

[а]напряженная ситуация [б]между государствами или оранизованными группами, в которой [в]проведение информационых операций [г]приводит к ответным действиям.

[26] ***Commentary***

Known definitions were consulted during this process.

Cyber Penetration[27]

[a]unauthorized [b]entry [c]into a cyber entity.

Киберпроникновение

[а]неавторизованный [б]доступ [в]к киберобъекту (киберсубъекту).

[27] ***Commentary***

Known definitions were consulted during this process.

Cyber Threat[28]

[a]a danger, whether [b]communicated or sensed, [c]that can exercise [d]a cyber vulnerability.

Киберугроза

[б]обнаруженная или установленная [а]угроза [в]использования [г]киберуязвимости.

[28] ***Commentary***

Known definitions were consulted during this process.

Cyber Exfiltration[29]

[a]a type of cyber operation [b]that involves copying or removing any [c]data.

Киберэксфильтрация

[а]тип кибероперации, [б]связанный с копированием или изьятием каких-либо [в]данных.

[29] ***Commentary***

Known definitions were consulted during this process.

Cyber Espionage[30]

[a]a cyber operation [b]to obtain [c]unauthorized [d]access to [e]sensitive information [f]through covert means.

Кибершпионаж

[а]кибероперация по [б]получению [в]неавторизованного [г]доступа к [д]чувствительной информации [е]скрытыми методами.

[30] ***Commentary***

The authorization is associated with the entity that owns the information. Espionage is potentially a crime.

Known definitions were consulted during this process.

Cyber Operation[31]

[a]organized activities in cyberspace to [b]gather, [c]prepare, [d]disseminate, [e]restrict or [f]process [g]information [h]to achieve a goal.

Кибероперация

[а]организованная деятельность в киберпространстве по [б]сбору и накоплению, [в]подготовке, [г]распространению, [д]ограничению в доступе, [е]обработке [ё]информации [ж]для достижения поставленной цели.

[31] ***Commentary***

Known definitions were consulted during this process.

2.3 The Art

This section presents consensus definitions for 16 terms, namely: cyber warfare, cyber attack, cyber counter-attack, cyber defensive countermeasure, cyber defense, cyber defensive capability, cyber offensive capability, cyber exploitation, cyber deterrent, information superiority, information operation, information operations dominance, information security, cyber weapon,[32] cyber vulnerability and cyber intelligence.

The 16 definitions are presented here.

[32] The EWI Russia-U.S. Bilateral on Critical Infrastructure Protection recently offered considerable definition of a cyber weapon 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 Karl Rauscher and Andrey Korotkov, *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 Warfare[33]

is [a]cyber attacks [b]that are authorized by state actors [c]against cyber infrastructure [d]in conjunction with a government campaign.

Боевые действия в киберпространстве

[а]кибератаки, [б]проводимые государствами (группами государств, организованными политическими группами), [в]против киберинфраструктур [г]и являющиеся частью военной кампании.

[33] ***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 Attack[34]

is [a]an offensive [b]use of a cyber weapon [c]intended to harm a designated target.

Кибератака

[а]наступательное [б]использование кибероружия [в]с целью нанесения вреда определенной цели.

[34] ***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 as a **cyber weapon** against a non-cyber asset or as a cyber asset. But a **cyber attack** is *not* a non-cyber weapon against a non-cyber asset or cyber asset (See framework on page 13). See the previous footnote for additional insights and reference material.

The combined team could not resolve whether the following acts would constitute an attack: propaganda, website 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, 2-C-12. This definition is the only use of the word "cyber" in the mentioned above NATO publication. In compliance with the request of the custodian of the publication, a written notification of the use of this definition here has been provided to the NSA.

Cyber Counter-Attack[35]

is [a]the use of a cyber weapon [b]intended to harm a designated target [c]in response to an attack.

Киберконтратака

[а]использование [б]кибероружия с целью нанесения вреда определенной цели [в]в ответ на атаку.

[35] ***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**, a cyber counter-attack is defined by a weapon type and not the nature of the target.

Known definitions were consulted during this process.

Cyber Defensive Countermeasure[36]

is [a]the deployment [b]of a specific cyber defensive capability [c]to deflect [d]or to redirect [e]a cyber attack.

Оборонительные средства противодействия в киберпространстве

[а]развертывание [б]особых оборонительных средств противодействия [в]для отражения, [г]или перенаправления [д]кибератаки.

[36] ***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 a 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 Defense[37]

is [a]organized capabilities [b]to protect against, [c]mitigate from and [d]rapidly recover from [e]the effects of cyber attack.

Кибероборона

[а]организованная совокупность средств и действий [б]для защиты, [в]смягчения [г]и эффективного восстановления [д]от враждебных воздействий [д]кибератак.

[37] ***Commentary***

Important considerations for this term include the following:

Cyber defense refers to actions taken by a party to protect its interests 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 Capability[38]

is [a]a capability [b]to effectively protect [c]and repel [d]against a cyber exploitation or [e]cyber attack [f]that may be used as a cyber deterrent.

Оборонительные возможности в киберпространстве

[а]возможность [б]эффективно защитить [в]и отразить [г]кибератаку, предотвратить киберконфликт, [д]предупредить использование противником преимуществ в киберпространстве, [е]которая может быть использована в качестве средства сдерживания в киберпространстве.

[38] ***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 Capability[39]

is [a]a capability [b]to initiate [c]a cyber attack [d]that may be used [e]as a cyber deterrent.

Наступательные возможности в киберпространстве

[а]возможность [б]начать [в]кибератаку, [г]которая может быть использована [д]в качестве средства сдерживания в киберпространстве.

[39] ***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, 92-93 (CJCS CM-0363-08).

Cyber Exploitation[40]

is [a]taking advantage [b]of an opportunity [c]in cyberspace [d]to achieve an objective.

Использование преимуществ в киберпространстве

[а]использование в своих интересах [б]имеющихся возможностей [в]в киберпространстве [г]для достижения поставленной цели.

[40] ***Commentary***

Important considerations for this term include the following:

The advantage here may be either the acting party's strength or 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, 2-C-12. This definition is the only use of the word "cyber" in this NATO publication. In compliance with the request of the custodian of the publication, a written notification of the use of this definition here has been provided to the NSA.

Cyber Deterrent[41]

is [a]a declared [b]mechanism [c]that is presumed effective [d]in discouraging cyber conflict [e]or a threatening activity [f]in cyberspace.

Средства киберсдерживания

[а]признанный [б]механизм, [в]который считается действенным [г]для препятствования киберконфликту, [д]или угрожающей деятельности [е]в киберпространстве.

[41] ***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.

Information Superiority[42]

[a]having better [b]or more [c]information.

Информационное превосходство

[а]обладание информацией [б] лучшего качества, или [в]в большем объеме.

[42] ***Commentary***

Known definitions were consulted during this process.

Information Operation[43]

[a]organized activities to [b]gather, [c]prepare, [d]disseminate, [e]restrict or [f]process [g]information [h]to achieve a goal.

Информационная операция

[а]организованная деятельность по [б]сбору и накоплению, [в]подготовке,[г]распространению, [д]ограниченю в доступе или [е]обработке [ё]информации [ж]для достижения поставленной цели.

[43] ***Commentary***

Known definitions were consulted during this process.

Information Operations Dominance[44]

[a]overwhelming [b]capability in information operations, [c]leading to a position of control.

Доминирование в информационных операциях

[а]подавляющее [б]превосходство при проведении информационных операций, [в]приводящее к состоянию контроля над всей ситуацией.

[44] ***Commentary***

Known definitions were consulted during this process.

Information Security[45]

is [a]property [b]of information space [c]that is an ability [d]to resist threats and [e]respond and [f]recover.

Информационная безопасность

[а]свойство [б]информационного пространства [г]противостоять угрозам, [д]реагировать на них и [е]восстанавливаться (после нанесения ущерба).

[45] ***Commentary***

This also applies to all of its subspaces as well.

Known definitions were consulted during this process.

Cyber Weapon[46]

[a]software, [b]firmware or [c]hardware [d]designed or applied [e]to cause damage [f]through the cyber domain.

Кибероружие

[а]программное, [б]аппаратное обеспечение, или [в]прошивки микросхем, [г]разработанные или применяемые [д]для нанесения ущерба [е]в киберсфере.

[46] ***Commentary***

Consequential harm can be caused to the physical domain as well. Also see the quad chart of physical and cyber attributes (see page 13).

Known definitions were consulted during this process.

Cyber Vulnerability[47]

[a]property of [b]a cyber entity [c]that is susceptible to exploitation.

Киберуязвимость

[а]свойство [б]киберобъекта, [в] которое в потенциале может быть использовано для проведения кибероперации.

[47] ***Commentary***

Cyber vulnerability can be known or unknown.

Known definitions were consulted during this process.

Cyber Intelligence[48]

1. [a]information of value [b]collected and [c]processed through [d]cyber operations,

2. [a]information of value [b]collected about [c]cyber assets of [d]another entity.

Киберразведка

1. [б]сбор и [в]обработка [а]ценной информации с использованием [г]киберопераций,

2. [б]сбор [а]ценной информации о [в]киберактивах [г]другого субъекта/ объекта.

[48] ***Commentary***

Cyber intelligence can be military, political, economic, industrial, environmental, diplomatic, etc.

Known definitions were consulted during this process.

3. Recommendations

This section presents five recommendations, which if implemented, would enable more meaningful international agreements in the critical emerging area of cyber conflict. Each recommendation is presented with critical information to support decisions regarding its implementation. This information includes the following nine elements:

1. Title—to identify and summarize.
2. Purpose—to state the intent in a straightforward manner.
3. Background—to provide the essential elements of the context of the issue being addressed.
4. Recommendation—to identify who should do what.
5. Required Commitments—to outline the requirements from critical parties for success.
6. Benefits—to encapsulate the value proposition for implementing the recommendation.
7. Alternatives and Their Consequences—to outline the other options and likely outcomes.
8. Next Steps—to offer suggestions for keeping momentum and focus.
9. Measures of Success—to provide means to objectively evaluate performance.

3.1 Advocacy for Use of Agreed Terminology

Purpose

This recommendation calls on stakeholders to promote the deliberate use of terminology with agreed definitions in order to enhance the quality of international agreements.

Background

The value of agreements made between parties in the context of international affairs is determined by several factors. One of the most critical factors is the extent to which the agreements are commonly understood, so that expectations for behaviors can be accurate. This recommendation advances understanding with the aim of impacting developing agreements.[49]

It is quite challenging to achieve any agreement regarding cyberspace as this field of study is rapidly developing and its key concepts are not well understood by the policy community, which is generally not scientifically or otherwise technically trained in essential principles of information and communications technology.

Recommendation No. 1

Russian and United States stakeholders should advocate the utilization of commonly defined terms in order to enhance the meaningfulness and quality of international agreements to achieve peace and stability in cyberspace.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Stakeholders from Russia must actively advocate the use of terms with agreed upon definitions in international agreements related to cyberspace.
- ☐ Stakeholders from the United States must actively advocate the use of terms with agreed upon definitions in international agreements related to cyberspace.

[49] Note that this recommendation encourages the use of well-defined terms in agreements with regard to cyberspace, but does not limit this advocacy to only the terms presented in this document.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Develop agreements with limited agreed upon vocabulary . . . resulting in agreements with reduced understanding.

- Russian or U.S. stakeholders advocate the adoption of unilaterally-defined terminology with implicit ideological undertones . . . resulting in delays in reaching the agreements.

Benefits

The implementation of this recommendation will 1) enhance the meaningfulness and quality of the agreements, 2) be an enabling factor for agreements; and 3) increase the speed and efficiency of the agreement development process.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

1-1. Russian and U.S. stakeholders advocate the use of agreed terminology for policy development regarding conflict in cyberspace.

1-2. Agreed terminology is used in the agreement development process for international diplomacy.

1-3. International agreements for conflict in cyberspace make use of the agreed terms.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Russian and U.S. stakeholders are advocating the use of agreed terminology.

B. Agreed terminology is actually used in policy development for cyber conflict policy.

3.2 Military Academy Usage

Purpose

This recommendation calls on military academies to adopt terminology with agreed definitions in order to elevate the precision of education dealing with cyber conflict policies.

Background

Military academies play a critical role in the transfer of key concepts and broader frameworks. Training with regard to international policies for cyber conflict can be enhanced when they integrate terminology with agreed definitions.

Recommendation No. 2

Military academies and other educational institutions devoted to international affairs should include commonly defined terms into their educational processes.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Military academies in Russia must integrate terminology with agreed definitions into educational processes that deal with cyber conflict.
- ☐ Military academies in the United States must integrate terminology with agreed definitions into educational processes that deal with cyber conflict.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Limit discussion of international cyber conflict policy to vocabulary that is unilaterally defined . . . yielding an understanding of policy that is limited to a single-nation context.

- Utilize definitions agreed to separately by Russian or U.S. stakeholders . . . resulting in propagation of divergent definitions in discussions with the need to carry forward multiple meanings simultaneously.

Benefits

The implementation of this recommendation will elevate the precision of educational discussions by enabling strong reference points to be established in the context of very complex and evolving material. Faculty and students can have increased confidence that they know what the other country also understands about the key concepts in international policy agreements. This relatively stronger foundation will make future agreements possible.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

2-1. Russian and U.S. military academies and other educational institutions dealing with international affairs become aware of these and other international definitions.

2-2. Russian and U.S. military academies and other educational institutions dealing with international affairs integrate these and other international definitions into their curriculum, as appropriate.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Russian and U.S. military academies make use of the commonly defined terms.

B. The agreed terms are used to enhance mutual understanding of faculty and students in regard to future policy development.

C. The agreed terms enable faculty and students to propose new international agreements with regard to cyber conflict.

3.3 Multilateral Terminology Refinement

Purpose

This recommendation calls on Russian and U.S. stakeholders to engage other interested nation-states to join in enhancing existing definitions and in building additional definitions for critical terms.

Background

Achieving agreements on the critical terminology definitions for cyber conflict by two countries like Russia and the United States is a breakthrough as the East-West bridge did not previously exist. It is also significant because it suggests that if agreements could be achieved with such disparity of cultural and political perspectives, then it is likely that the definitions will be used by other countries with diverse cultures and political views.

Recommendation No. 3

Russian and United States stakeholders for peace and stability in cyberspace should proactively engage other interested nation-states to expand international participation in the refinement and utilization of the commonly defined terms.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Russian stakeholders must participate in outreach to other nation-states.
- ☐ U.S. stakeholders must participate in outreach to other nation-states.
- ☐ Other nation-states must contribute expertise and be willing to cooperate in refining definitions and building a glossary of critical terms.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Limit discussion of terminology for international cyber conflict policy to Russia and the United States . . . missing the opportunity for more rigorous exposure and thus improvements.
- Do not prioritize outreach to other nation-states . . . resulting in low visibility of these and other terms with internationally agreed definitions.

Benefits

The implementation of this recommendation will enhance the quality of the already agreed definitions. The implementation will also build confidence to the extent that the other countries agree on their utility.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

3-1. Russian and U.S. stakeholders invite other countries to comment on the existing list of terms, selected and agreed definitions.

3-2. Russian and U.S. stakeholders engage in rigorous discussions for each term in order to confirm the existing definition or adjust it with improvements.

3-3. Stakeholders from Russia, the U.S. and other countries propose the next list of terms for which international agreement on definitions is needed.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Russian and U.S. stakeholders conduct outreach to other countries.

B. The number of countries that engage in outreach.

C. Feedback on existing definitions is provided.

D. Feedback on existing definitions is considered and used to enhance existing definitions, as appropriate.

E. The number of countries that become involved in suggesting new terms for future definitions.

3.4 Taxonomy of Terms Critical to Cyber Diplomacy

Purpose

This recommendation calls on Russian and U.S. stakeholders to develop an organized structure that clarifies which terms are essential for diplomacy in cyberspace.

Background

Cyberspace is a vast, complex and ever-changing arena, with new terms introduced as often as new services and applications are (e.g., cloud, tweet, honeypot, etc.). Diplomacy in cyberspace suffers from a lack of understanding of the landscape and its changing dynamics. Ideally, diplomatic efforts would be supported by not only well-defined terms, but also by an organized structure that presents the relationship between these terms. This recommendation provides guidance to create such a taxonomy. The first issue of this document Critical Terminology Foundations introduced a simple structure for 20 terms that consisted of "The Theater," "The Modes of Aggravation" and "The Art." This taxonomy is used in this issue as well.

Recommendation No. 4

Russian and United States stakeholders, along with other interested parties, should create and maintain a taxonomy of terminology that is critical to diplomacy in cyberspace.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Subject matter experts from Russia, the United States and other interested parties must collaborate in developing a common taxonomy of critical terminology.
- ☐ Subject matter experts from Russia, the United States and other interested parties must agree on the future priorities for diplomacy in cyberspace.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Continue to define terms but do not provide an organized structure . . . reducing the potential clarity that is possible when relationships between terms are confirmed.

- Do not consider the relationship between terms . . . increasing the likelihood for contradictions to arise among terms, causing conflict in policy developed using these terms.

Benefits

The implementation of this recommendation will provide a framework for understanding available terms that can be utilized in developing policy recommendations. It will also help in identifying the additional terms that require definition.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

4-1. Stakeholders from Russia, the United States and other interested parties agree on a structure for the existing terms with agreed definitions.

4-2. Stakeholders from Russia, the United States and other interested parties agree on methods of identifying which terms are needed in the future to support cyber diplomacy.

4-3. Stakeholders continuously revise the taxonomy to maintain its optimum utility for cyber diplomacy.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. A taxonomy is agreed to for the existing terms.

B. The taxonomy is used to identify missing terms requiring definitions.

C. The taxonomy is useful in cyber diplomacy.

3.5 Maintain Taxonomy of Terms Critical to Cyber Diplomacy

Purpose

This recommendation calls on Russian and United States stakeholders to define addition critical terms as needed.

Background

It is envisioned that critical terminology taxonomy for cyber diplomacy will require ongoing revision for the foreseeable future. New terms will emerge and require definitions to fill gaps in the devolving taxonomy.

Recommendation No. 5

Russian and United States stakeholders, along with other interested parties, should monitor gaps in the existing taxonomy of commonly defined terms and continue the development of critical terminology to address these gaps.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Subject matter experts from Russia, the United States and other interested parties must collaborate in developing definitions for emerging critical terminology.
- ☐ Subject matter experts from Russia, the United States and other interested parties must seek agreements for these new terms, as with the previously defined.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Develop a taxonomy but do not provide for its maintenance . . . reducing the value of the taxonomy as it is not current.
- Do not monitor for gaps in terminology . . . increasing the likelihood that the taxonomy will become outdated.

Benefits

The implementation of this recommendation will ensure an updated set of critical terms for international cyber diplomacy.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

5-1. Stakeholders from Russia, the United States and other interested parties agree on a method of monitoring for gaps in terms.

5-2. Stakeholders from Russia, the United States and other interested parties identify existing gaps in terminology that require definitions.

5-3. Stakeholders develop definitions for the identified terms.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. A continuous monitoring process is in place.

B. A process for identifying gaps is supported bilaterally.

C. The process identifies gaps and fills them with new definitions.

D. The quality of the process improves over time.

4 Conclusion

This joint paper presents 40 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 to create a Russian-U.S. glossary of cyber terms for more than a decade. They have stalled for some of the reasons discussed here. This is the first to bear the intended fruit. This joint team has created a taxonomy that can be improved in the coming months and years. While 40 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 broadening the discussion to a multilateral one. This means ensuring input from the International Information Security Research Consortium (IISRC) and other forums.

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, and to the benefits it can offer to the world that is wandering in information and cyberspace without much-needed reference points.

About the Authors

Chief Editors

James B. Godwin IIII

Rear Admiral (retired) James Basil Godwin III transitioned from the United States Navy in 2006 after 33 years of service. Rear Admiral Godwin is a decorated Naval Aviator with fleet assignments in both the A-7 Corsair II and the F/A-18 Hornet with more than 4500 flight hours embarked in numerous Carrier Air Wings and Carrier Strike Groups. He is the Founder and President of BriteWerx, Inc., a Service Disabled Veteran Owned Small Business (SDVOSB) providing consulting services in the Aerospace, Information Technology and Cyber Fields. He is currently working with three other small business owners in starting up their businesses and fielding their disruptive cyber, electronic and voice, video and data compression technologies. From 2006 to 2012, he held vice president positions within the defense industry, including Athena Technologies (now Rockwell Collins), Dynamic Analytics & Test and Northrop Grumman Information Systems. From 2004-2006, he served as the Direct Reporting Program Manager, Navy Marine Corps Intranet (NMCI) and then as the first Program Executive Officer, Enterprise Information Systems.

Andrey Kulpin

Andrey Kulpin is the Director of International Center of the Information Security Institute (ISI), Lomonosov Moscow State University. He has also worked with and consulted other United Nations entities, including the United Nations Counter-Terrorism Implementation Task Force on measures to counter terrorist use of the Internet, 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 cyber crime.

Karl Frederick Rauscher

Karl Frederick Rauscher is the former 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. His positions included: Vice Chair of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC) and a leader of the European Commission-sponsored study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI). Moreover, 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). His recent publication is the IEEE Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report. Karl is an inventor with over 50 patents/pending in fields that span artificial intelligence, critical infrastructure protection, emergency communications, energy conservation and telemedicine. Additionally, he 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 February 12, 1947, in the Bryanskiy region in the former USSR. In 1967, he graduated from the Mechanics and Mathematics Department of the Moscow State University named after M.V.Lomonosov. In 1971, he finished his post-graduate studies at the

same Department. From 1971 until 1991, he held different positions at the KGB - Committee of the State Security USSR. In 1991, he retired with the rank of Colonel. From 1991 until 2003, Dr. Yaschenko served as the Vice-Chief of the Mathematical Studies in cryptography laboratory of the Moscow University. Concurrently, he was an advisor to the President of this University and represented him at several Committees of the Security Council of the Russian Federation. Since 2003, Dr. Yaschenko serves as a Senior Vice-Director of the Information Security Institute at Moscow State University. He has a PhD in mathematics (1983).

Contributing Subject Matter Experts

Merritt Baer

Merritt Baer runs a consulting company, merrittrachelbaer.com, which provides strategic guidance on cybersecurity and emerging tech. She translates technological, legislative and legal considerations into business intelligence. She has experience in all three branches of the US government, most recently in the office of U.S. Senator Michael Bennet. She is a Fellow of the Global Cooperation in Cyberspace Initiative at the EastWest Institute, a member of National Defense Industrial Association, the New York Bar Association and the American Bar Association. She has a strong publication record reflecting her commitment to chasing questions on the technology horizon. She is a graduate of Harvard College and Harvard Law School.

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, 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.

Stuart Goldman

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

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 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 U.S.-Russia bilateral 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 Engineering. He holds a doctorate degree in Military Science. He is an author of more than 100 scientific works dedicated to information warfare and information security, including eight certificates of invention authorship. Dr. Komov took part in the development of The Doctrine of Information Security of the Russian Federation. He is a member of the experts group on international information security of the Ministry of Defense of the Russian Federation. He participated at the UN Group of Government Experts (2004-2005), Shanghai Cooperation Organization (2006-2009) and Collective Security Treaty Organization (2008-2009). Currently, he is a Scientific Adviser to the Director of the Lomonosov Moscow State University's Institute of Information Security Issues.

Luis Kun

Dr. Luis Kun is a Professor of National Security Affairs at the William Perry Center for Hemispheric Defense Studies at the National Defense University. Prior to this, he served for eight years as the Senior Research Professor of Homeland Security at the i-College. He is Editor-in-Chief of *Springer's Journal of Health and Technology* and the Chairman of the Global Citizen Safety and Security for the International Federation of Medical and Biological Engineering (IFMBE). He graduated from the Merchant Marine Academy in Uruguay and holds BSEE, MSEE and Ph.D. degrees in Biomedical Engineering from the University of California, Los Angeles. He works at the intersection of Information Technology with Healthcare, Public Health and National Security. At IBM, Cedars Sinai Medical Center, AHCPR, CDC and several U.S. universities, he developed strategies, products and curricula related to these fields where he made numerous seminal contributions. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE) and of the American Institute for Medical and Biological Engineering's (AIMBE). He is the Founding Chair of the IEEE-USA: Critical Infrastructure Protection Committee; the Bioterrorism & Homeland Security WG and the Electronic Health Record and High Performance Computers and Communications WG. He has received many awards and was and continues serving on the Board of Governors or Directors, Advisory board and administrative councils of many organizations, magazines and professional journals. He is a frequent invited speaker and has lectured in over 85 countries.

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 the IEEE's Senior Member and a recipient of the IEEE Reliability Society's Engineer of the Year Award. Dr. Michael holds a Ph.D. in Information Technology from George Mason University.

J. 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 U.S. 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.

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. Additionally, Dr. Oslund was on the international staff at the White House Office of Telecommunications Policy and held senior management positions at the Communications Satellite Corporation. He participated in the National Security Telecommunications Advisory Committee (NSTAC) and has taught as an adjunct professor at George Washington University. Dr. Oslund was a Senior Fellow at the University's Homeland Security Policy Institute.

Alexey Salnikov

Alexey Salinikov is a Vice-Director of Information Security Institute of Moscow State University named after M. V. Lomonosov. He studied at the Technical Department of Highest School of the KGB, where he specialized in mathematics and cryptology, and at the George C. Marshall European Center for Security Studies. From 1990 to 2003, he performed various roles at the KGB, including the Committee of State Security, the USSR; the Federal Agency of Government Communications and Information (FAPSI), the Russian Federation; and the Federal Security Service (FSB), the Russian Federation. He retired with the rank of Colonel. Since 2003, he works at Lomonosov Moscow State University. He is the author of more than 30 articles, and a co-author of a monograph on mathematical issues in cryptology. His current interests are political issues of cybersecurity, Internet monitoring, cryptographic protocols and mathematical problems in cryptology.

Anatoly Streltsov

Anatoly Streltsov is the Vice-Director of Information Security Institute of Moscow State University named after M. V. Lomonosov, a retired head of the Department of the Security

Council of the Russian Federation and a 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 doctorate in Technical Science (1987) and in Juridical Science (2004), and the title of Professor (1994). Dr. Streltsov is a Corresponding Member of the Academy of Cryptography of the Russian Federation (2005).

Nadiya Kostyuk

Nadiya Kostyuk is a Program Coordinator for the Global Cooperation in Cyberspace Initiative at EastWest Institute. She spent the past two years conducting interviews with government officials, academics and journalists researching policy gaps in the current European cybersecurity paradigm. In-country experience in Bosnia and Herzegovina, Estonia, Ukraine, Russia, Serbia, Sweden, Switzerland and the Czech Republic provided her with a better understanding of each country's unique political climate. During the summer of 2013, Nadiya participated in the NATO Summer School, where she joined in interactive workshops and simulations with international security experts, discussing best cybersecurity practices.

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.

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

Karl Rauscher and Andrey Korotkov, 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. United Nations Institute for Disarmament Research.
http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf

In Russian

Федеральный закон от 27 июля 2006г. №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, http://comsec.spb.ru/matherials/gosts/gost50922-96.pdf

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

EastWest Institute Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder and CEO
EastWest Institute

R. William Ide III (U.S.)
Council and Secretary
Chair of the Executive Committee
EastWest Institute
Partner
McKenna Long and Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman and CEO
Southwest Energy (HK) Ltd.

Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
Chairman and CEO
IP Partners

Robert N. Campbell III (U.S.)
Founder and CEO
Campbell Global Services LLC

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Michael Chertoff (U.S.)
Co-founder and Managing Principal
Chertoff Group

David Cohen (U.K.)
Chairman
F&C REIT Property Management

Joel Cowan (U.S.)
Professor
Georgia Institute of Technology

Addison Fischer (U.S.)
Chairman and Co-Founder
Planet Heritage Foundation

Stephen B. Heintz (U.S.)
President
Rockefeller Brothers Fund

Hu Yuandong (China)
Chief Representative
UNIDO ITPO-China

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

John Hurley (U.S.)
Managing Partner
Cavalry Asset Management

Amb. Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference
Global Head of Governmental Affairs
Allianz SE

Ralph Isham (U.S.)
Managing Director
GH Venture Partners LLC
Chairman
Laurus Edutech Pvt. Ltd.

Anurag Jain (India)
Chairman
Laurus Edutech Pvt. Ltd.

Gen. (ret) James L. Jones (U.S.)
Former Advisor
U.S. National Security
Former Supreme Allied Commander
Europe
Former Commandant
Marine Corps

Haifa Al Kaylani (Lebanon/Jordan.)
Founder and Chairperson
Arab International Women's Forum

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

General (ret) T. Michael Moseley (U.S.)
Moseley and Associates, LLC
Former Chief of Staff
United States Air Force

F. Francis Najafi (U.S.)
CEO
Pivotal Group

Amb. Tsuneo Nishida (Japan)
Permanent Representative of Japan to the U.N.

Ronald P. O'Hanley (U.S.)
President,Asset Management and Corporate Services
Fidelity Invesments

Amb. Yousef Al Otaiba (U.A.E.)
Ambassador
Embassy of the United Arab Emirates in Washington, D.C.

Admiral (ret) William A. Owens (U.S.)
Chairman
AEA Holdings Asia
Former Vice Chairman
U.S. Joint Chiefs of Staff

Sarah Perot (U.S.)
Director and Co-Chair for Development
Dallas Center for Performing Arts

Louise Richardson (U.S.)
Principal
University of St. Andrews

John Rogers (U.S.)
Managing Director
Goldman Sachs and Co.

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Amb. Kanwal Sibal (India)
Former Foreign Secretary of India

Kevin Taweel (U.S.)
Chairman
Asurion

Amb. Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Amb. Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President and CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz* (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor and Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman and CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman and CEO
Cargill Inc.

Mark Maletz (U.S.)
Chairman, Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest Institute Policy Report Series

2014

A Measure of Restraint in Cyberspace
Reducing Risk to Civilian Nuclear Assets
Policy Report 2014—1

2013

Afghan Narcotrafficking
A Joint Threat Assessment
Policy Report 2013—1 [EN | RU]

The Path to Zero
Report of the 2013 Nuclear Discussion Forum
Policy Report 2013—2

Threading the Needle
Proposals on U.S. and Chinese Actions
on Arms Sales to Taiwan
Policy Report 2013—3

Measuring the Cybersecurity Problem
Policy Report 2013—4

Frank Communication & Sensible Cooperation to Stem Harmful Hacking
Policy Report 2013—5 [EN | CH]

2012

Bridging the Fault Lines
Collective Security in Southwest Asia
Policy Report 2012—1

Priority International Communications
Staying Connected in Times of Crisis
Policy Report 2012—2

2011

Working Towards Rules for Governing Cyber Conflict
Rendering the Geneva and Hague
Conventions in Cyberspace
Policy Report 2011—1 [EN | RU]

Seeking Solutions for Afghanistan, Part 2
Policy Report 2011—2

Critical Terminology Foundations
Russia-U.S. Bilateral on Cybersecurity
Policy Report 2011—3

Enhancing Security in Afghanistan and Central Asia through Regional Cooperation on Water
Amu Darya Basin Consultation Report
Policy Report 2011—4

Fighting Spam to Build Trust
China-U.S. Bilateral on Cybersecurity
Policy Report 2011—5 [EN | CH]

Seeking Solutions for Afghanistan, Part 3
Policy Report 2011—6

2010

Economic Development and Security for Afghanistan
Increasing Jobs and Income with the Help
of the Gulf States
Policy Report 2010—1

Making the Most of Afghanistan's River Basins
Opportunities for Regional Cooperation
Policy Report 2010—2

The Reliability of Global Undersea Communications Cable Infrastructure
Policy Report 2010—3

Rights and Responsibilities in Cyberspace
Balancing the Need for Security and Liberty
Policy Report 2010—4

Seeking Solutions for Afghanistan, Part 1
Policy Report 2010—5

Building Trust Delivering Solutions

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a **global go-to place for building trust, influencing policies and delivering solutions.**

–

Learn more at **www.ewi.info**

EastWest INSTITUTE

EWInstitute
EastWestInstitute