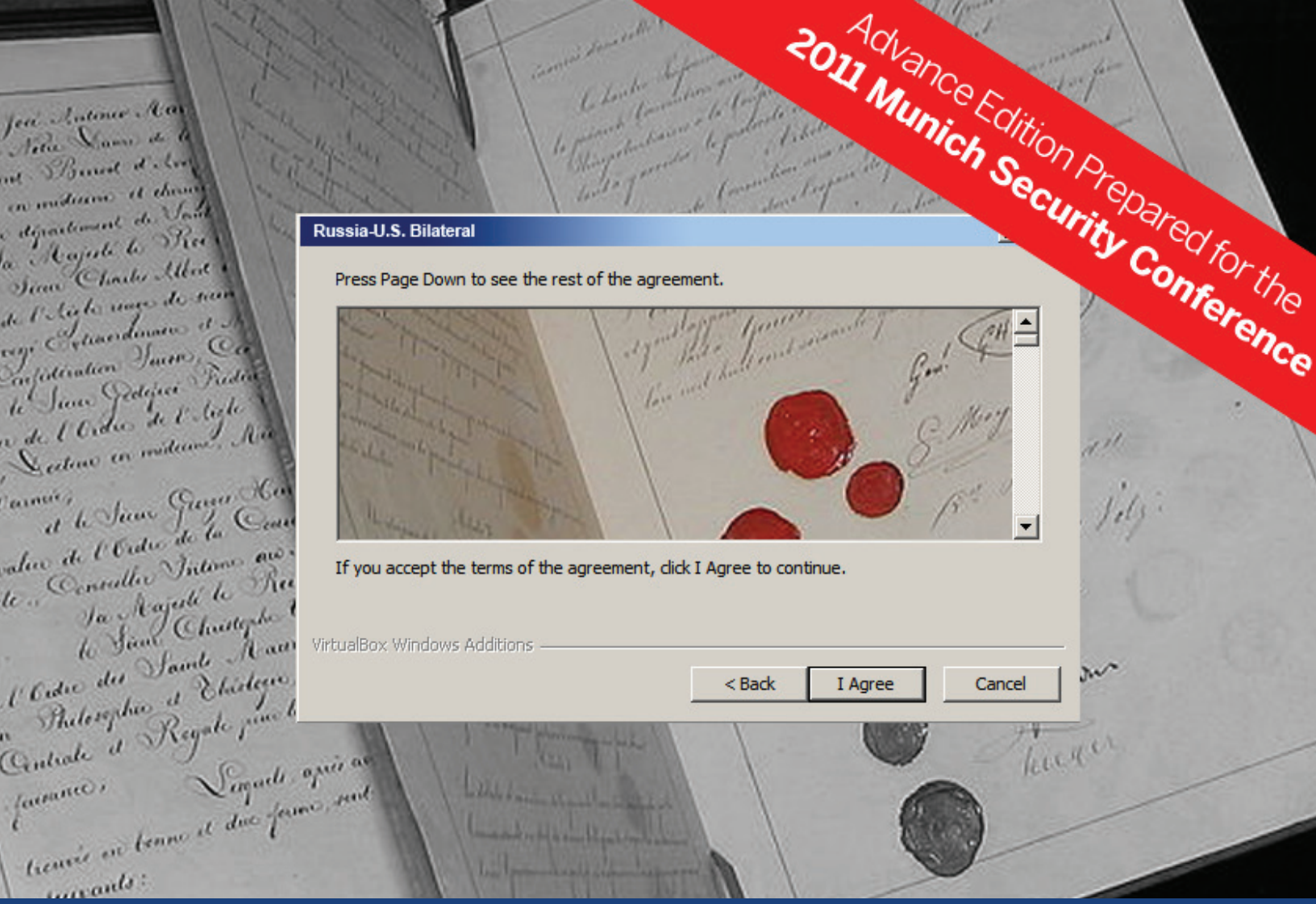


RUSSIA-U.S. BILATERAL ON CRITICAL INFRASTRUCTURE PROTECTION

Working Towards Rules for Governing Cyber Conflict

Rendering the Geneva and Hague Conventions in Cyberspace

EastWest Institute
Forging Collective Action for a Safer and Better World

30 YEARS

The Russia-U.S. Bilateral on Critical Infrastructure Protection
Working Towards Rules for Governing Cyber Conflict
Rendering the Geneva and Hague Conventions in Cyberspace
Issue 1

An advance publication of this paper was presented at the Munich Security Conference, February 4-6, 2011.

The principal authors of this document are:

Karl Frederick Rauscher, EastWest Institute
and
Andrey Korotkov, Moscow State Institute of International Relations of the Ministry of Foreign Affairs of Russia

Cover art work by Dragan Stojanovski.

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

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info,
For inquiries regarding this report, request referral to Franz Stefan-Gady or Andrew Nagorski

www.ewi.info

RUSSIA-U.S. BILATERAL ON CRITICAL INFRASTRUCTURE PROTECTION

Working Towards Rules for Governing Cyber Conflict

Rendering the Geneva and Hague Conventions in Cyberspace

By KARL FREDERICK RAUSCHER & ANDREY KOROTKOV

January 2011

EastWest Institute
Forging Collective Action for a Safer and Better World

Dedication

To those whose suffering was the impetus for the Conventions.
May future generations have wisdom absent such impetus.

Посвящение

Посвящается тем, чьи страдания стали побуждающим мотивом принятия конвенций
о законах, обычаях и защите жертв войны.
Пусть же у будущих поколений хватит мудрости не допустить подобных страданий.
.

Contents

Foreword

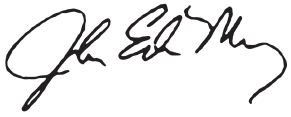
Over the last three decades, strategic dialogue between Russia and the United States has been an essential part of the drive for a safer and better world. The resulting series of significant nuclear arms agreements - most recently, the New START Treaty - represent tangible evidence of progress for people everywhere.

Cybersecurity is the new challenge for continued cooperation between Russia and the United States as well as the entire international community. This is an area where there is precious little trust or international cooperation, and no real agreed norms for behavior. At the same time, countries everywhere are increasingly concerned about the intentions and capabilities of non-state actors. Yet the globe's netizens, businesses and public officials rely on the fact that some complex system they don't understand will keep functioning. The global economy itself is now completely dependent on digital tools, which means it is increasingly vulnerable to disruption by state or non-state actors. This is a dangerous situation. There's an urgent need for international cooperation on this most strategic of issues. If we fail in this task, global stability could be as threatened as it would be by a nuclear exchange.

For thirty years, the EastWest Institute has served as an intellectual convener on the most significant strategic challenges that face our world. As part of its Worldwide Cybersecurity Initiative, EWI has created the 'Cyber 40' group of nations to tackle these issues, with the aim of delivering joint reports that build trust and help lay the basis for new international agreements.

The Russian-American cooperation that led to this joint report challenges the conventional wisdom that these cyber issues are too sensitive and complex for international agreement. We wish to thank the technical, business and policy experts who produced the report for their highly effective, hard work. Their success in driving this study and its recommendations shows what can be done if there is political and personal will. We urge the private and government sectors on both sides to be diligent in building on this cooperative cybersecurity effort. We also look forward to receiving the insights and reactions of our readers. The EastWest Institute has rigorous plans to build on this study and welcomes readers' contributions. We trust that this work will help catalyze a movement across boundaries to make effective international cooperation in cyberspace a reality.

HARRY D. RADUEGE, JR
Honorary Chair of the EWI Worldwide Cybersecurity Summit
fmr. Director, Defense Information Systems Agency
and Manager, National Communications System
Lt. General (ret.), U.U.S. Air Force



JOHN EDWIN MROZ
President and
Chief Executive Officer,
EastWest Institute

Preface

Herein are 5 joint recommendations for the private sector and governments. Some are bold. Each is actionable and, if implemented, will provide some measure of breakthrough for international policy in the arena of governing cyber conflict. Further, we submit that given the potential consequences of the current course, consideration of the guidance provided herein should be taken up with urgency.

We introduce this paper as one confronting a grave matter for all mankind in the information age. The Geneva and Hague Conventions on war have drawn the last lines of protection for civilians when all else is failing. Preserving the viability and feasibility of these principles is of solemn relevance to billions of this generation and those to come. As our world is rapidly being re-wired and integrated with cyberspace, their preservation is neither automatic nor straightforward. Cyberspace is now an integral part of every aspect of our personal lives, the operation of private businesses and the administration of governments. In fact, information and communications technology has profoundly transformed the natures of critical infrastructure and its protection, and war and its prosecution. Cybersecurity has quickly emerged as the linchpin of our mutual safety, stability and security. Yet the "rules of the road" for cyber conflict, or even the norms for behavior, are blatantly absent.

This joint analysis was conducted by world-class experts from both our countries with the aim to begin to make meaningful progress in the international arena We here express deep appreciation to our colleagues, who are listed on the next page. Their expertise spans the diverse competencies needed to undertake such a project, and their combined experience exceeds five hundred years. Their personal sacrifice and individual contributions during this intense interactive process that drove this report were indispensible and deserving of recognition and gratitude.

The humanitarian protections of the Conventions are hard-fought gains for civilization. They are hallowed and they are mutually shared. May we mutually resolve to prove ourselves good stewards of the progress made by previous generations.

KARL FREDERICK RAUSCHER
Leader, U.S. Experts
Chief Technology Officer & Distinguished Fellow, EastWest Institute
President, Wireless Emergency Response Team
Bell Labs Fellow

New York City, USA

ANDREY KOROTKOV
Leader, Russia Experts
Department Head & Professor
Moscow State Institute of International Relations of the Ministry of Foreign Affairs
First Deputy Minister,
Ministry of Telecommunications and Informatization of Russia (2002-2004)

Moscow, Russia

Contributors

Russian Federation

Artyom Adjemov, Moscow Technical University of Communications and Informatics
Vladimir Ivanov, EastWest Institute
Victor Minin, Civil Advisory Committee on Science and Technology Aspects of Information Security
Boris Slavin, Union of Chief Information Officers of the Russian Federation
Leonid Todorov, Coordination Center for Top Level Domains for Russia
Elena Zinovieva, Moscow State Institute of International Relations

United States of America

Charles (Chuck) Barry, National Defense University
John S. Edwards, Digicom, Inc.
J. B. (Gib) Godwin, RADM (ret.), Northrop Grumman
Stuart Goldman, Bell Labs Fellow (ret.)
Paul Nicholas, Microsoft Corporation
James Bret Michael, U.S. Naval Postgraduate School
Jack Oslund, George Washington University (ret.)
Thomas C. Wingfield, George C. Marshall European Center for Security Studies

Expert Reviewers

Ramses Martinez, VeriSign
General (ret) T. Michael Moseley, USAF; Perot Distinguished Fellow, EWI

Acknowledgements

Special recognition and sincere appreciation is here expressed

to Wolfgang Ischinger
for integrating this paper in the 2011 Munich Security Conference. [1]

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

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

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

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

to Anatoly Safonov, Vladislav Sherstyuk, Andrey Krutskikh, Sergey Kislyak,
William Burns, Michael McFaul, John Beyrle and John Edwin Mroz
for their innovation, encouragement and foresight.

and finally, to our wider community of respective stakeholder
confidants in Moscow and Washington, D.C.
whose appreciation for innovation in Track 2 engagements ensures their long term value.

1 An advance publication of this paper was presented at the 2011 Munich Security Conference (February 4-6).

1. Executive Summary

In the spirit of the reset of relations between Moscow and Washington, Russian and U.S. security and cyber experts undertook to model new cooperative behavior for dealing with the most challenging security topic of our age: cybersecurity. Until now, the conventional wisdom has been that setting the "rules of the road" for cyber conflict would be both tedious and extraordinarily difficult. In this first effort, the joint team demonstrated that progress can be and is being made. This paper presents five joint recommendations that are immediately actionable and, if implemented, would be effective in preserving key humanitarian principles of the Laws of War. The progress demonstrated here can serve as a catalyst for further progress to achieve that goal.

This joint paper presents the consensus findings of the Russian and U.S. experts on the Rendering of the Geneva and Hague Conventions in Cyberspace. The work is a product of a Track 2 bilateral program that seeks to open dialogue, build sustainable trust and have a positive impact in the most difficult, most critical areas for international security.

In recent history, Russia and the United States have had an outsized influence on international issues. When these two countries can agree on a common approach to any particular problem, other countries are prone to listen seriously. For that reason, top experts from Russia and the United States agreed to tackle the problem of cybersecurity together. The hope is that other countries will join in this process.

One of the most highly regarded accomplishments of this broader community of nation-states in the last century and a half is the cooperation that has led to the Conventions that uphold the dignity and respect for human life. Proceedings from The Hague and Geneva have drawn important lines that effectively say: "You may go this far but no further when fighting for a cause or in mounting a defense." While these lines admittedly protect only the most basic aspects of humanity, they nevertheless tower in their significance as an accomplishment of civilization. For in the midst of an all out clash of ideas and force, they maintain the principle that "we can agree on this."

This paper is not about law. Instead, we are treating these highly regarded common principles of the Geneva and Hague Conventions as our departure point. Of course, today's information and communications technology (ICT) revolution has dramatically transformed the world we live in, which means that the practical application of some Convention principles is no longer as straightforward as it once was.

Unique Characteristics

Because questions about how the Geneva and Hague Conventions relate to cyberspace have been a general concern for some time, a considerable amount of analysis and opining has been offered about this subject. Much of this has focused on the legal issues, political significance, or extreme scenarios that could play out. In contrast, this paper's focus is on the areas of strategic convening based on first principles, applying advanced methods from the technical domain, and seeking action-oriented recommendations.

The unique aspects of this joint analysis start with the fact that this is a bilateral program of two cyber superpowers. Other aspects include the integration of multiple core competencies required for the subject matter (Section 3), the dispensational treatment of the complex landscape of challenges, the utilization of advanced analysis methods in the technical domain (i.e. the Eight Ingredient (8i) Framework and Intrinsic Vulnerability approach) (Section 3), and most importantly, the presentation of specific, actionable, consensus recommendations, that, if implemented, will be effective in preserving the humanitarian critical infrastructure protection principles that can be observed in the Conventions (Section 4).

Joint Recommendations

The following recommendations are presented with essential information to foster their implementation. This information includes essential background information, the required commitments, the benefits of implementation, the alternatives and their consequences, next steps and measures of success. Each recommendation is summarized here from Section 4.

"The hardest thing to explain is the glaringly evident which everybody had decided not to see."

- Ayn Rand, Russian born American writer

"Education consists mainly of what we have unlearned."

- Mark Twain, American writer

"Knowledge is of no value unless you put it into practice."

- Anton Chekhov, Russian playwright and master of the short story

RECOMMENDATION 1. Detangling Protected Entities in Cyberspace

The Geneva Convention provides some measure of protection for purely humanitarian-focused entities and personnel, under qualifying conditions, during war. However, protected and non-protected entities are intermingled in cyberspace, placing the protected entities in jeopardy. Until now, most analyses of this situation have been at the national level. This recommendation will be a major cooperative effort, starting first at the bilateral level, and later extending to the multilateral level.

Russia and the U.S., along with other willing parties, should conduct an evaluation of the present state of the intermingling of protected, humanitarian critical infrastructure with non-protected infrastructures in order to determine whether existing Convention and Protocol articulation is sufficient and whether significant detangling of essential humanitarian critical infrastructures is feasible.

The result of implementing this recommendation will be a bilateral or multilateral determination that will advise as to whether the Convention-provided protections of humanitarian entities are still viable, are substantially degraded, or are substantially degraded and not recoverable with current trends in cyberspace. This advice will promote the preservation of the observed principles of the Conventions that protect humanitarian critical infrastructure and civilians. The effective implementation of this recommendation will require private sector companies from both countries to lend technical expertise and business experience. In addition, Russian and U.S. government stakeholders must support this collaboration with their respective experts; international humanitarian aid non-government organizations (NGOs) must also provide their insights.

RECOMMENDATION 2. Application of the Distinctive Geneva Emblem Concept in Cyberspace

A belligerent party's ability to recognize a declared protected entity is vital to compliance with the Conventions. The Geneva and Hague Conventions direct that protected entities, protected personnel and protected vehicles be marked in a clearly visible and distinctive way. Further, the Conventions establish specific standards for the distinctive emblem itself (i.e. Red Cross, Red Crescent), instruction for its application, and consequences for its misuse. However, there are no distinctive, clearly visible, markers in cyberspace for entities, personnel or related assets. Without such markers, the humanitarian interests intended to be shielded by the Conventions are in jeopardy. This recommendation proposes analogous markers in cyberspace to designate protected entities, personnel and other assets.

Russia and the U.S., along with other willing parties, should conduct a joint assessment of the benefit and feasibility of special markers for zones in cyberspace that can be used to designate humanitarian interests protected by the Conventions and Protocols of War.

The benefit of implementing this recommendation is that it will provide for the clear recognition of a protected entity, person or other asset in cyberspace. A belligerent's ability to identify such protected entities is vital to preserving the Conventions that deal with the protection of humanitarian interests. The effective implementation of this recommendation will require private sector companies lending their expertise, Russian and U.S. government stakeholders supporting the collaboration with their respective experts, and Internet governance organizations supporting the implementation of measures to achieve the distinctive emblem principle in cyberspace.

RECOMMENDATION 3. Recognizing New Non-State Actor and Netizen Power Stature

The digital revolution has created new "territory" in cyberspace. The occupation and control of territory has historically been the chief issue of contention among ethnic groups and political powers engaged in war, and it follows that the Convention signatories have been nation-states. The digital revolution has unleashed non-state actors and individuals to occupy, control and operate in cyber territory. This creates new power asymmetries and magnifies the clout of new participants who can violate Convention principles on a massive scale.

Russia, the U.S. and other interested parties, should assess how best to accommodate Convention principles with the new reality that cyber warriors may be non-state actors.

This joint assessment will provide shared insights of the new emerging dynamic in cyberspace and the growing dangers flowing from it. It also will anticipate the needs of this new multifaceted cyber community in regards to instruction and training about the Geneva and Hague protections for civilians and critical civilian infrastructure. To achieve these benefits, governments must be open to new paradigms of respect, dialogue, cooperation and trust with Non-State Actors (NSAs), such as Non-Government

Organizations (NGOs) and Multi-National Companies (MNCs). In addition, governments and a critical mass of both NSAs and Netizens must be able to demonstrate some new, minimal, to-be-defined level of cooperation in cyberspace.

RECOMMENDATION 4. Consideration of the Geneva Protocol Principles for Cyber Weaponry

With modern civilization's utter dependence on ICT and cyberspace, there are increasing concerns about the potential consequences of cyber weapons, which have the ability to introduce new sorts of aggression, multi-degree cascading effects, and social and economic devastation. Cyber weapons can deliver, in the blink of an eye, wild viral behaviors that are easily reproduced and transferred, while lacking target discrimination. These attributes, combined with a belligerent cause, are an understandable reason for concern. For humanitarian reasons, the Conventions have established a precedent for prohibiting certain weapons.

Military forces charged with ensuring decisive battle space advantage recognize the strategic value of secrecy. This legitimate security concern understandably has stalled progress in international cooperation around weapon analysis. By focusing on Information and Communications Technology (ICT) intrinsic vulnerabilities that are already recognized in the public domain, this recommendation introduces an innovative approach that significantly mitigates those concerns.

Russia, the U.S. and other interested parties, should conduct a joint analysis of the attributes of cyber weapons in order to determine if there are attributes analogous to weapons previously banned by the Geneva Protocol.

The benefits of successfully completing such an assessment include "breaking the ice" among cyber powers for discussions on the new frontier of conflict, creating an international framework for understanding cyber weapon attributes, and curtailing the proliferation of weapons that can have devastating effects on civilians and critical civilian infrastructure. The successful implementation of this recommendation will require experts to be open to discussing weapon types based on publicly available information. Russian and U.S. governments must be open to the possibility that some weapon attributes may be unacceptable because they are offensive "to the principles of humanity and from dictates of public conscience."[1]

RECOMMENDATION 5. Examination of a Third, 'Other-Than-War' Mode

There is no clear, internationally agreed upon definition of what would constitute a cyber war. In fact, there is considerable confusion. Senior government leaders from the same country have incompatible opinions about the most basic aspects of cyber war – its existence now, its reality or likely impact in the future. The current ambiguity is impeding policy development and clouding the application of existing Convention requirements. It is possible that the binary peace vs. war paradigm is too simple for the complexities of the Internet Age. In this recommendation, the joint analysis team offers a fresh approach for a path forward.

Russia and the U.S., along with other willing parties, should explore the value of recognizing a third, 'other-than-war' mode in order to clarify the application of existing Conventions and Protocols.

The value of considering a third mode is that the ensuing discussion will bring much needed clarity and structure to a very complex and confusing discussion. Equally beneficial would be its rejection, after appropriate consideration, to clarify why the current two modes are preferred and what contours and parameters are essential to their definition. The effective implementation of this recommendation will require Russian and U.S. national security stakeholders to acknowledge that the current uncertainty about the definition for cyber war is unacceptable. In addition, Russia, the U.S., and other interested parties, must explore new frameworks to categorize conflict, and they must be devoted to open analysis and consideration of new options for managing behavioral norms in cyberspace.

1 Protocol Additional I, 1949, Article 1. The Geneva Conventions of August 12, 1949, International Committee of the Red Cross, Geneva, http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp .

Summary Statistics

A survey of this joint paper is outlined as follows:

5	Joint Recommendations to preserve the principles of the Geneva and Hague Conventions
10	Joint Observations for the Laws of War, humanitarian protections and cyberspace
16	Subject matter experts formed the combined Russian-U.S. analysis team
30	Meetings held to conduct analysis and develop the recommendations
79	Intrinsic vulnerabilities of cyberspace recognized
754	Convention articles considered in the analysis

Joint Observations

The joint team made many observations. These ten are highlighted because of their central role in supporting the joint recommendations. The following observations are summarized from Section 3:

1. Protected and non-protected critical infrastructure entities are intermingled in cyberspace.
2. Protected humanitarian critical infrastructure lacks markers to designate its protected status.
3. Discrimination between military and civilian targets is more difficult in cyberspace.
4. ICT can be an enabler for better implementation of Convention principles concerning humanitarian needs.
5. Non-State Actors and Netizens can wield elevated power in cyberspace.
6. Cyber weapons have attributes not previously seen with traditional weapons nor considered during the development of the current Laws of War.
7. Military forces will have distinct interests in keeping cyber weapons secret.
8. The complexity of ICT and cyberspace propagates mystery about its nature and limits.
9. A cyber operation may take place undetected and attribution is problematic.
10. The ambiguity surrounding cyber war suggests a different approach.

Next Steps

The suggested next steps for each recommendation are specified in detail in the presentation of each recommendation (Section 4, "Next Steps" headings).

Next steps also include engaging the parties and organizations that should be involved in these discussions. At the program level, the EastWest Institute continues to serve as a strategic convener for Russia-U.S. trust-building in cybersecurity. In addition, the Institute's priorities include its Worldwide Cybersecurity Initiative (WCI), in which it partners with the world's leading thinkers, companies, NGOs and governments in fashioning breakthroughs for international Agreements, Standards, Policies and Regulations (ASPR).

2. Introduction

This section provides background for the joint analysis, establishing the importance of the undertaking, outlining its objectives, defining its scope, and describing its approach.

2.1 Importance

Consideration of the implications on critical infrastructure protection from rendering the international war conventions in cyberspace is of grave importance. While it may seem self-evident that the phrase ***critical infrastructure*** carries significance, a concise survey is offered here.

Critical infrastructure is vital to public safety, economic stability, and national security of Russia, the United States, and other developed countries. The essential sustenance, functioning shelter and basic welfare of the civilian populations require the operation of these systems. Likewise, routine business transactions, the operation of private enterprises and the security interests of nation-states are inseparable from their reliance on critical infrastructures. A subset of the critical infrastructures is recognized as having purely humanitarian interests (Table 1).

Further, the protection of critical infrastructure is a heavy obligation of governments. It is also a basic business affair of the private sector, where ownership often resides. Protection is a rising concern for two primary reasons. First, it is a rising concern because of the dramatically increasing consequences of infrastructure failure as these

systems carry ever-bigger loads for societies.[2] Second, it is a rising concern because these systems, in their rapid ascent in sophistication and power, have become much more difficult to manage in their complexity, and in some ways more vulnerable to compromise or impairment.[3]

The Geneva and Hague Conventions on war have drawn the last lines of protection for civilians when all else fails. Preserving the viability and feasibility of these principles is of solemn relevance to billions of this generation and those to come. As our world is being re-wired in cyberspace, the preservation of these principles is neither automatic nor straightforward. Cyberspace is now an integral part of every aspect of our personal lives, the operation of private business and the administration of governments. As a result, cyberspace has dramatically changed the natures of both critical infrastructure and warfare in profound ways.

Finally, the cooperation of Russian and U.S. experts on this project brings immediate weight to its conclusions. These countries are two of the world's real "titans" in cyberspace, yet the two also have well-recognized differences in culture, ideology and interests. Thus, agreements among their experts and stakeholders are momentous.

2.2 Objectives

Three objectives were set for this bilateral engagement. The first was to open genuine dialogue between subject matter experts and stakeholders from both countries. The second was built on the first and was to develop deeper understanding of each other's perspectives. The third was to establish consensus around critical issues that could serve as an enabler for eventual formal, agreements between the two countries, and as a reference for other nation-states.[4] The first two objectives were met as is evidenced from the contents of this report. Time is needed to determine the achievement against the third objective.[5]

2.3 Scope

There are four parameters that best define the boundaries of this discussion. These are i) the parties involved, ii) the qualifying infrastructure, iii) the specific international agreements, and iv) the nature of protection.

Parties Involved

This analysis 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 part of 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 exceeded five hundred years and included the broad range of expertise needed for an examination of the subject matter. Their knowledge spanned science, engineering, war fighting, humanitarian aid, law, policy development, government administration, business and academic research. Their experiences included combat, military policy, emergency response, international policy development, and critical infrastructure design, operation and protection. In addition, the current roles of the participants represent interests of both the private sector as well as government, including military.

In addition to these experts, EastWest Institute staff served in the capacity of trusted convener, neutral facilitator, process architect and resource mobilizer.[6] The normal path for the Institute is to transfer the momentum of a bilateral Track 2 initiative to official government (i.e. Track 1) channels and to transfer the insights and value to a multilateral process, as appropriate.

2 "It is the policy of the United States (1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States," Critical Infrastructure Act of 2001, USA Patriot Act, Section 1016 (c), 2001. http://www.fincen.gov/statutes_regs/patriot/.

3 "Congress makes the following findings: (1) The information revolution has transformed the conduct of business and the operations of government as well as the infrastructure relied upon for the defense and national security of the United States. (2) Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors." Ibid., Section 1016 (b).

4 e.g., Track 1.

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

6 Institute staff played a neutral facilitation role. The five staff members involved were nationals of Armenia, Austria, Australia, Russia and the U.S.

Table 1. Critical Infrastructures of Russia[7] [8] [9] and the U.S.[10] [11] [12] [13] [14] [15] [16]

CRITICAL INFRASTRUCTURES		
Russian Federation	United States of America	Remarks
Health Care	Public Health	Humanitarian
-	Emergency Services	Humanitarian
-	National Monuments and Icons	Humanitarian
Agriculture	Agriculture and Food	Dual
Water Supply	Water	Dual
Government	Government	Dual
Very Large Information Systems	-	Dual
Information and Telecommunications	Information and Telecommunications	Dual
Energy	Energy	Dual
Utility including Warming Systems	-	Dual
Financial and Banking System	Banking and Finance	Dual
-	Transportation and Shipping	Dual
Transportation Systems[17]	-	Dual
Industry	Chemical Industry & Hazardous Materials	Dual
-	Critical Manufacturing	Dual
-	Post	Dual
Municipal Services	-	Dual
Civil Defense	-	Dual
-	Defense Industrial Base	Target
Defence	-	Target

7 Russian Federation, The National Security of Russia. http://www.scrf.gov.ru/documents/sections/3/.

8 Russian Federation Law on Security, March 5, 1992, N 2446-I, as amended 1992 – 2007. http://www.scrf.gov.ru/documents/20.html.

9 Russian Federation,Strategy of the National Security of the Russian Federation Until 2020, Presidential Decree No. 537, May 12, 2009. http://www.scrf.gov.ru/documents/99.html.

10 Executive Order 13010, Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.

11 White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No.63.

12 Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council, , Federal Register, Vol. 66, No. 196, (October 8, 2001).

13 USA PATRIOT Act, 2001. The Homeland Security Act of 2002 reiterates the PATRIOT Act definition.

14 U.S. Department of Homeland Security, The National Strategy for Homeland Security, , July 16, 2002.

15 White House, Executive Office of the President, The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, (February, 2003).

16 Homeland Security Presidential Directive 7, HSPD-7, December, 2003.

17 Includes pipelines.

Qualifying Infrastructure

Infrastructures are the assets, systems, personnel and procedures that are essential to providing the general functioning of a society. The scope of this analysis includes infrastructures that are critical and national, and that are qualified by meeting requirements of the Conventions for special protection.

Critical

Critical infrastructures are distinguished as those infrastructures whose continued operation is essential for sustaining life, economic stability and continuation of government, to include national security. International standardization of critical infrastructures has been attempted; however, there exists wide variation of lists of

what comprises critical infrastructure and these often vary between countries.

> Variations between countries can be explained by differences in conceptualizations of what is critical, but also by country-specific peculiarities and traditions. Socio-political factors as well as geographical and historical preconditions determine whether or not a sector is deemed to be critical.[18]

In the United States, the 2001 Patriot Act defined critical infrastructure as:

> . . . systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[19]

There is no similar formalized definition in Russia for critical infrastructure or critical infrastructure protection, although there are several references to the importance of specific systems in Russia that are critical to national security, economic stability, and public and social safety.[20]

Table 1 provides lists of critical infrastructures in Russia and the U.S. Note that a few of these are utilized for purely humanitarian interests, and a few are likewise utilized for military objectives, but that most have dual use.

National

The team's critical infrastructure protection bilateral engagement began with a discussion of the options to address national policies affecting international critical infrastructures or international policies affecting national critical infrastructures. Serious consideration was given to international infrastructure as the focus. Such a path would explore "international infrastructure" such as the Domain Name Server (DNS) elements of the worldwide web, communications satellites, or Global Undersea Communications Cable Infrastructure (GUCCI). The later of which was being addressed in part through the implementation of recommendations from an IEEE Report.[21]

After considerable discussion, the focus was brought to bear on international policies affecting national critical infrastructures due primarily because of (a) the strength of the starting position of an internationally accepted convention, (b) the relative perceived lack of progress in this arena, and (c) the sensed need from both sides for urgency in this undertaking.[22] The other areas remain potential subject matter for subsequent collaborative efforts.

Qualified

The term 'critical infrastructure' is not the language of the Conventions. However the concept of certain assets and personnel being vital to civilian and humanitarian interests is well established in numerous articles. The Conventions have historically provided strict qualifications for assets and personnel to afforded protection:[23]

- "compromise only a small part of the territory …"
- "be thinly populated in relation to the possibilities of accommodation"
- " far removed and free from all military objectives, or large industrial establishments"
- " not situated in areas … important to the conduct of war"
- "communications and means of transport … shall not be used … for military personnel or material"
- "in no case defended by military means"
- " marked by means of red crosses (red crescents, red lions and suns) …"
- "all necessary steps must be taken to spare … buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes"
- "submarine cables connecting an occupied territory with a neutral territory …"

18 Elgin M. Brunner and Manual Suter, International CIIP Handbook, An Inventory Of 25 National And 7 International Critical Information Infrastructure Protection Policies, Center for Security Studies (CSS) (Zurich:Center For Security Studies,2009). p.529.

19 USA Patriot Act, Section 1016 (e), October 2001.

20 Brunner, CIIP Handbook, pp. 527-528.

21 Karl F. Rauscher, Reliability of Global Undersea Communications Cable Infrastructure-The Report, Institute of Electrical and Electronics Engineers (April, 2010), www.ieee-rogucci.org.

22 A 'Treaty on Cyber Warfare' is needed now or is overdue" – response of 71% of participants, Participant Summary Results, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EWI,(May 6,2010).

23 For examples see Geneva Convention I, 1949, Annex I, Articles 1-13; Hague Convention IV, 1907, Articles 27-28, 54.

Table 2. Outline of the Geneva and Hague Conventions

Component	Title	Dates	No. of Articles	Words (English) Approx.
Geneva Convention	Amelioration of the Condition of the Wounded on the Field of Battle	1864	10	660
Hague Conference II	Laws and Customs of War on Land	1899	60 (55 in Anx)	3,960
Hague Conference IV	Laws and Customs of War on Land	1907	64 (56 in Anx)	4330
Geneva Protocol	For the Prohibition of the Use in War of Asphyxiating Gas, and for Bacteriological Methods of Warfare	1928	-	400
Geneva Convention I	For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field	1864, rev. 1949	77 (13 in Anx)	8,600
Geneva Convention II [24]	For the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea	1949	63	6,795
Geneva Convention III	Relative to the Treatment of Prisoners of War	1929, rev. 1949	143	20,246
Geneva Convention IV[25]	Relative to the Protection of Civilian Persons in Time of War	1949	180 (21 in Anx)	21,373
Geneva Convention	Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on Their Destruction	1975	15	1,700
Protocol I	Relating to the Protection of Victims of International Armed Conflicts	1977	102	21,779
Protocol II	Relating to the Protection of Victims of Non-International Armed Conflicts	1977	28	3,376
Protocol III	Relating to the Adoption of an Additional Distinctive Emblem	2005	17	1,934

Further discussion of infrastructures is provided in Section 3, Systematic Analysis.

International Agreements

Of the existing treaties, conventions, and agreements that make up the "Laws of War," a subset was selected to be the area of focus. The criteria were the relationship to addressing civilians and civilian assets. The joint team introduced the term 'Conventions' in this paper to refer to this subset. The scope of the joint analysis included articles of the Geneva and Hague Conventions listed below:

- Geneva Convention (1864)
- Hague II (1899)
- Hague IV (1907)
- Geneva Convention (1928)
- Geneva Convention I (1949)
- Geneva Convention II (1949)
- Geneva Convention III (1949)
- Geneva Convention IV (1949)
- BW Convention (1975)[26]
- Protocol Additional I (1977)
- Protocol Additional II (1977)
- Protocol Additional III (2005)

24 Successor of Hague Convention X, 1907.

25 Based on parts of the Hague Convention IV respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, The Hague,18 October, 1907, http://www.icrc.org/ihl.nsf/intro/195?OpenDocument.

26 Biological Weapons Convention.

Some of these agreements were selected because they addressed prohibited weapons that could affect the personnel element of critical humanitarian infrastructure (i.e. Geneva Conventions of 1928 and 1975).

> The Fourth Geneva Convention of 1949 ("Fourth Geneva Convention") provides specific requirements for the treatment of civilians in the course of war. Although the Fourth Geneva Convention relates mainly to particular classes of civilians, it does provide some general protections to civilians as a whole. The 1977 Additional Protocol I ("Additional Protocol I") to the Geneva Conventions contains much more extensive protections for civilians, including highly detailed provisions regarding the targeting of civilian populations. The Fourth Geneva Convention and Additional Protocol I have been widely ratified, and apply to "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."
>
> Article 51(4) of Additional Protocol I prohibits parties to a conflict from engaging in indiscriminate attacks, being attacks that: are not directed at a specific military objective; employ a method or means of combat which cannot be directed at a specific military objective; or employ a method or means of combat the effects of which cannot be limited as required by Additional Protocol I, and that are, therefore, of a nature to strike military objectives and civilians or civilian objects without distinction. Article 51(4) may be regarded as a residual protection, because engaging in indiscriminate attacks as defined would likely breach other rules of Additional Protocol I.[27]

The Conventions in scope combine for 759 articles that are fleshed out with just over 93,200 words. Many of the articles are repetitive, capturing some of the same principles in a different context.

The analysis team agreed that in its simplest sense, the criteria for what designates some infrastructure as "critical," is its essential role in the safety of human life, economic stability, and national security with the first priority being human life. Though critical infrastructure protection is not a term of the Geneva and Hague Conventions, the safety of human life is directly related to portions of the Geneva Conventions, particularly those sections dealing with noncombatants, i.e. civilians[28]\

Table 2 synthesizes the Convention articles that were the primary source of reference for this analysis, which sum to 295.

Nature of Protection

The scope was further bounded to the types of protection currently or potentially offered by the Conventions. This protection includes being excluded from being an "object of an attack" and being at "at all times respected and protected."[29] There are also provisions for being granted a "due warning" if protection is to cease.[30] Qualifying vehicles are afforded "free passage."[31]

The protections afforded such assets and personnel are forfeited if the assets or personnel operate outside of the strictly specified parameters.[32]

> While IHL stipulates that civilians be protected against direct attack, "unless and for such time as they take a direct part in hostilities", neither the Geneva Conventions nor their Additional Protocols spell out what conduct constitutes direct participation in hostilities. In its efforts to redress this situation and to protect the civilian population from erroneous or arbitrary targeting, the ICRC initiated an informal process of research and consultation with the aim of clarifying three key questions: (1) Who is considered a civilian for the purposes of conducting hostilities? (2) What conduct amounts to direct participation in hostilities? (3) What modalities govern the loss of civilian protection against direct attack?[33]

It is noted here that "critical infrastructure protection" is a phrase often used by governments and the private sector owners and operators to refer to their efforts. This type

27 Tania Voon, "Pointing The Finger: Civilian Casualties Of NATO Bombing In The Kosovo Conflict", American University International Law Review, Vol. 16, No.4, April, 2001, pp. 1091- 1095.

28 See Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Geneva, 1949. http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/index.jsp.

29 Geneva Convention IV, 1949, Articles 18, 22.

30 Ibid. Article 19.

31 Ibid. Article 23.

32 Geneva Convention, 1864, Article 1-3, 27; Hague IV, 1907, Articles 27-28, 54; Geneva Convention IV, 1949, Articles 15, 19.

33 Nils Melzer, "Clarifying The Notion of Direct Participation in Hostilities-Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law", Geneva, ICRC Legal Reference Document, June, 2009. http://www.icrc.org/eng/resources/documents/feature/direct-participation-ihl-feature-020609.htm.

Table 3. Civilian and Humanitarian Critical Assets in the Conventions

Component	Relevant Articles to Scope	No. of Articles
Geneva Convention, 1864	10	10
Hague (II) Conference, 1899	27-28, 55-56	4
Hague (IV) Conference, 1907	27-28, 54-56	5
Geneva Protocol, 1928	-	-
Geneva Convention I. 1949	19 – 44, 1 – 13 in Annex I	58
Geneva Convention II, 1949	22 - 45	44
Geneva Convention III, 1949	-	0
Geneva Convention IV, 1949	1 – 26, Annex Articles 1 – 8	34
Geneva Convention, 1975	15	15
Protocol I, 1977	1 – 34, 48 - 79	70
Protocol II, 1977	1 - 28	28
Protocol III, 2005	1 - 17	17

of protective measure, usually undertaken by infrastructure designers and suppliers and by local governments, is not in scope.

2.4 Principles of Approach

Following are several points of emphasis about the approach used in this joint analysis.

One Team

Russian and U.S. participants of this effort participated on one combined team against the technical policy challenges at hand in cyberspace. Experts looked for common ground on which to build consensus but also were comfortable in articulating and holding to points of distinction.

Track Two

This cooperative dialogue is being led and supported by non-government organizations. The primary affiliation of most of the experts is a private sector company or academic institution. Both sides provided periodic briefings to their respective government stakeholders in Moscow and Washington, D.C.

Four Dispensations

The joint analysis concluded that there are four distinct dispensations to be managed simultaneously in the application of the Conventions' principles today. These are discussed in more detail in Section 3 (Figure 1). They are:

- *Traditional* weapons targeting *legacy* critical infrastructure
- *Traditional* weapons targeting *networked* critical infrastructure
- *Cyber* weapons targeting *legacy* critical infrastructure
- *Cyber* weapons targeting *networked* critical infrastructure

Advanced Methods

Advanced methods of technical analysis were referenced when understanding the limit and potential for cyberspace and when charting the course for future opportunities for cooperation. These methods include the 8i Framework for ICT and the Intrinsic Vulnerability approach.

3. Systematic Analysis

This section presents conclusions of the joint analysis that was conducted by the Russian-U.S. expert team. The nature of this analysis was to examine the implications of applying the observed principles of the Geneva and Hague Conventions regarding protections for qualified humanitarian assets and personnel to cyberspace with the aim of (a) understanding what, if any, challenges there may be in preserving the long and highly regarded humanitarian principles of these "Laws of War", (b) identifying aspects of ICT that are potential enablers for promoting the principles of the Geneva Convention, and (c) identifying issues that need further consideration.

In conducting the analysis, the team observed four distinct dispensations needing to be managed simultaneously in the application of the Conventions' principles today.[34]

These four dispensations are defined around the two parameters of infrastructure type and weapon type, and are spatially illustrated in Figure 1.

Infrastructure Type

For the purpose of this analysis, the two categories are intended to be mutually exclusive. While the distinction is primarily one between generations, there are specific characteristics for each. Legacy Infrastructures are those existing prior to the emergence of the Internet as a widely adopted connective fabric, while Networked Infrastructures represent the current state of modern systems. The transition from the former to the latter was a gradual process, and for the purpose of this analysis, specifying the exact conversion is not necessary.[35]

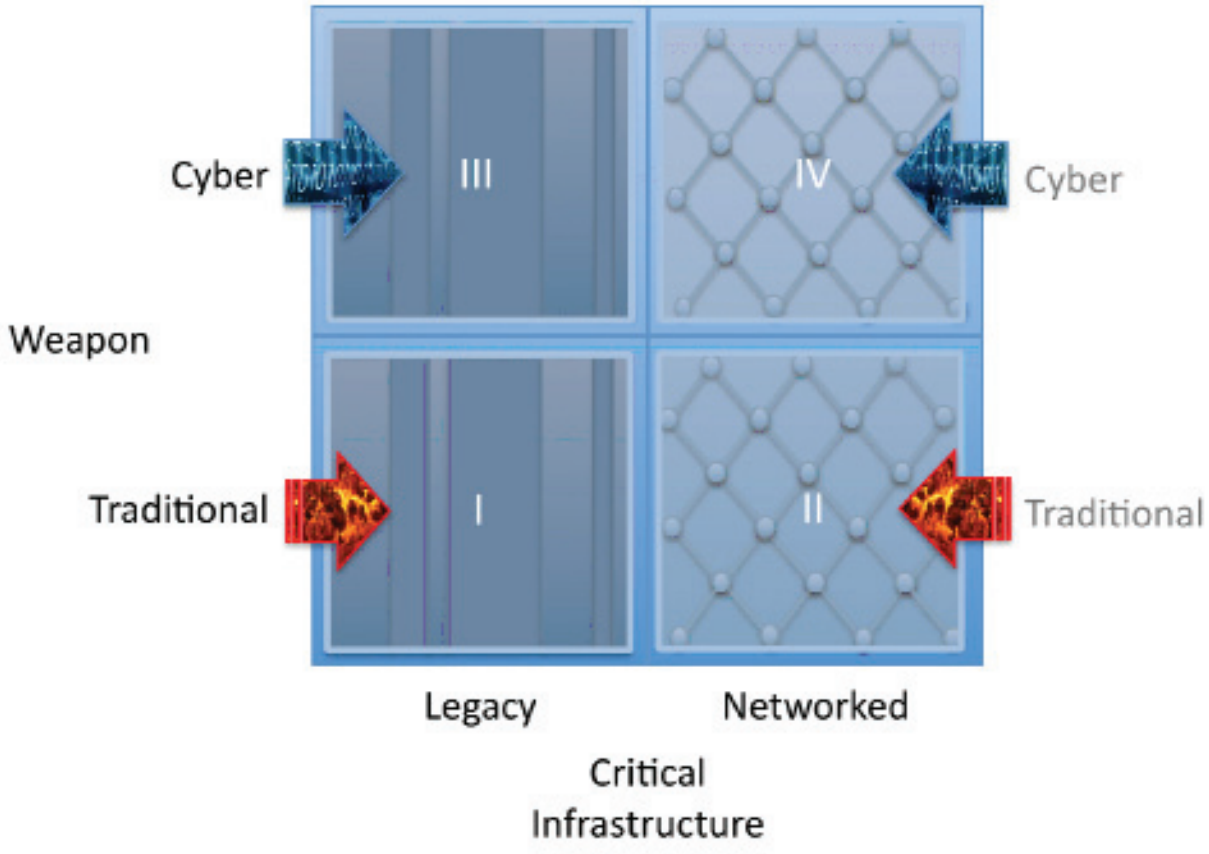


Figure 1. Four Dispensations for the Laws of War in Cyberspace

34 The team employs the term "dispensation" here because of its combined meaning as a distinct but related category and for having a special set of rules for which it should be administered.

35 The authors recognize the complexity of generational transition is non-trivial. However, the details of such complexity are not a factor in the current discussion. Transitional hybrids can be upgraded to the more advanced generation.

We recognize that both types of infrastructure exist today in the world but that the overwhelming global trend is for economic development to be accompanied by the introduction of networked infrastructures.

The key differentiating characteristics of the two infrastructure types are captured below. In addition, several examples are provided for illustrative purposes.

- Legacy Critical Infrastructures are differentiated by:
  - human supervision and control during operation
  - human management of inter-infrastructure interfaces
  - downward trends in utilization

Examples of legacy critical infrastructures include power plants and distribution facilities managed primarily with forecasts, hospitals with paper records and expertise limited to on-site staff, best estimate logistics for shipping, paper-based financial markets, and air traffic control based on radio contact and manual coordination with radar.

- Networked Critical Infrastructures are characterized by:
  - real-time reliance on software controlled operation (e.g., artificial intelligence)
  - inter-infrastructure interfaces that are highly interdependent and complex
  - an upward trend in utilization
  - more relied upon for basic sustenance by civilians, especially in urban areas

Examples of networked critical infrastructures include power grids with real-time "smart" feedback intelligence, hospitals utilizing electronic medical records with unlimited access to specialists via telemedicine, just-in-time inventory management via Radio Frequency Identification (RFID)-tagged parcels, electronic intra-day financial settlements, and variably automated air traffic control systems.

A fitting question at this stage is, "Are networked critical infrastructures better or worse than the legacy systems they have replaced?" The answer from the perspectives we are most familiar with – personal lifestyle, business operation, government administration, etc. – is a resounding "better!" We can do more and be faster with less effort.

Fortunately, the principles of the Conventions on War are not something many of us deal with on a daily basis. Adherence to the Conventions can be strengthened with the use of ICT,[36] but some new challenges need to be addressed.

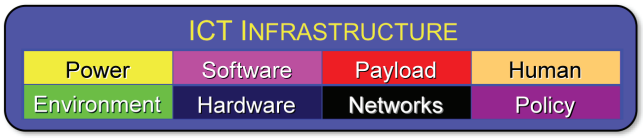


Figure 2. The Eight Ingredient (8i) Framework[37]

Each of the differentiating characteristics above is directly or indirectly the result of the integration of ICT. It is very useful to consider the Eight Ingredient (8i) Framework here, as it provides a complete picture for both ICT and less advanced elements of cyberspace (Figure 2). The 8i Framework can be used to systematically review the intrinsic vulnerabilities of each of these ingredients.[38] Unlike the threat side of the equation, where the possible permutations of threats make their number practically infinite, the number of intrinsic vulnerabilities of each of these ingredients, and thus for the cyberspace fabric of networked critical infrastructure, is finite.[39]

Weapon Types

For the purpose of this analysis, the two categories used here are intended to be mutually exclusive. The first describes weapons existing during the time of the writing of the conventions, while the latter represents the types of arms that are emerging today that make use of information and communications technology. Like the infrastructure transformation, the transition from the former to the latter was not discrete. Although both types of weapons exist today, there is great impetus for the development of advanced weapons that are either enhancements of tra-

36 See Section 3.5, Joint Observation 4.

37 ATIS Telecom Glossary; Bernando Rancho, Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop,; Karl F. Rauscher., Protecting Communications Infrastructure, Bell Labs Technical Journal, Special Issue: Homeland, Security, Vol. 9, No. 2, July, 2004; Next Generation Networks Task Force Report, The President's National Security Telecommunications Advisory Committee,(March 28, 2006), Background and Charge; Annual Report 2002, ATIS Network Reliability Steering Committee (NRSC).

38 Karl F. Rauscher et al. Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal Homeland Security Special Issue, Vol. 9, No. 2, April, 2006.

39 See Appendix G, Next Generation Networks Report, The President's National Security Telecommunications Advisory Committee (March, 28, 2006).

ditional weapons or altogether new forms of cyber-based capabilities.[40]

The key differentiating characteristics of the two weapon types, as well as examples, are outlined below.

- Traditional Weapons are those that are characterized by: [41]
  - the use of force (including kinetic, electromagnetic field and nuclear), biological contaminants, or chemical hazards
  - the immediate target is physical
  - assets are usually specially designed for armed conflict
  - access for the most advanced is very restricted
  - the most basic are inexpensive while the most advanced are very expensive

Examples of traditional weapons include firearms, grenades, bombs, artillery, nuclear missiles, etc.

- Cyber Weapons are characterized by:
  - the use of logic
  - the target is information or control
  - assets often have civilian applications
  - the threshold for access is low and getting lower
  - can be relatively cheap[42]

Examples of cyber weapons in cyberspace include worms, viruses, remote manual control, and key loggers. Examples of traditional weapons that are enhanced with ICT include GPS-enabled guidance systems, remotely controlled vehicles, and networked soldiers and battlefield equipment.

In order to be effective, a weapon needs to be able to exercise one of the intrinsic vulnerabilities of information and communications technology. Again, the 8i Framework is constructive as it provides a systematic approach for addressing intrinsic vulnerabilities that a weapon would have to make use of (Figure 2). The full spectrum of cyber weapons would be all of those that could exercise the intrinsic vulnerabilities.

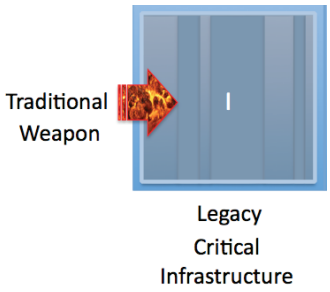
3.1 Dispensation I. Traditional Weapons in Legacy Infrastructure

This dispensation is similar to the environment that existed during the development of the last major Convention revision in 1949. The critical infrastructure architectures, the nature of interdependencies, and the reliance on manual operation characterize them as legacy. Similarly, the weapons here utilize the transfer of energy for impact.

Examples of what takes place in this dispensation include:

- a mobilized armored vehicle (i.e. tank) firing high caliber explosives at an oil refinery
- a submarine using an explosive torpedo to sink a shipping vessel
- a jet bomber striking an airport runway

For Dispensation I, the team concluded that the original intent of the Conventions directly apply as is. Thus the rendering of the Geneva and Hague Conventions for critical infrastructure protection concerns here is straightforward.



3.2 Dispensation II. Traditional Weapons in Networked Infrastructure

This dispensation is similar to the environment of 1949 in terms of the types of weapons it comprises, but dissimilar in that the critical infrastructure it comprises is networked, i.e. characterized by intense interdependencies, automated control, and high complexity.

---

40 "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." U.S. Department of Defense U.S. Cyber Command Fact Sheet, (May, 25 2010).

41 It is important to note that traditional weapons are being enhanced with ICT to enable remote operation, automate functions, enhance decision support, improve precision, augment function, etc. Hybrids can be upgraded to the more advanced generation.

42 " But there is one big difference between [nuclear and cyberweapons]. Cyberweapons are very cheap, almost free of charge," Vladislav Sherstyuk, quoted in David Talbot, Russia's Cyber Security Plans, MIT Technology Review Blog, http://www.technologyreview.com/blog/editors/25050/, (posted April 16, 2010).

Examples of what takes place in this dispensation include:

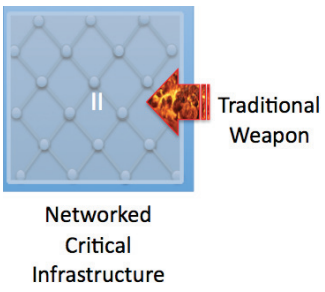
- a rocket-propelled grenade (RPG) firing high caliber explosives at a mobile communications radio tower
- an amphibious assault vessel and crew attacking and destroying an undersea cable landing station with small arms and explosives
- a jet bomber striking a smart grid concentration node

Networked infrastructure includes all of the physical elements of legacy infrastructure, plus the advanced ingredients, like software. Note that the cyberspace ingredients susceptible to traditional weapons are the environment that will house network equipment, the power generation and distribution equipment, the electronic hardware, networks and the operational personnel. Software, payload and agreements, standards, policies and regulations (ASPR) are not hard targets and thus could be affected indirectly, but not directly with traditional weapons.

The effective administration of this environment recognizes that the impact of critical infrastructure impairment is now much farther reaching in terms of the cascading effects on other systems, much more likely to be impactful on civilians and more likely to result in confusion.[43] That is, because of the complexity of critical infrastructure interactions, it is likely that some failure modes or effects are unknown, even for those societies that are the most advanced in their planning.

With all of the talk about cyber weapons, the existing arsenal should not be forgotten. It will certainly be expanded and used. A well-targeted conventional weapon now has richer target options.

Joint Observations 1 through 4 are key to managing this dispensation (Section 3.5). The first three deal with the ability to distinguish protected entities from non-protected entities. The fourth acknowledges the many ICT benefits offered in the application of Convention principles.



43 There are also time sensitivities that can further complicate system operation, i.e. if other systems are unavailable.

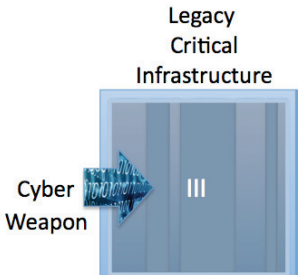
3.3 Dispensation III. Cyber Weapons in Legacy Infrastructure

This dispensation is similar to the environment of 1949 in terms of the types of infrastructure being attacked, but dissimilar in that cyber weapons are being used. Note that since the target is not cyberspace-integrated infrastructure, we are here mostly dealing with ICT-enabled weapons.

Examples of what takes place in this dispensation include:

- a Global Positioning System (GPS)-guided missile attacking a transportation hub
- a networked combat soldier attacking an in-transit target with satellite video support
- a remotely operated unmanned aerial vehicle (UAV, i.e. drone) transmitting coordinates to offshore naval artillery for a mechanized infantry unit target

Note that the infrastructure ingredients of legacy information and communications systems do not include the advanced ingredients like software. Such systems are susceptible to ICT-enhanced traditional weapons in their physical interface. This is because the weapons are primarily kinetic. Thus the target ingredients are environment that will house network equipment, the power generation and distribution equipment, the electronic hardware, networks and the operational personnel. On the other hand, the ICT-enhanced weapon is itself susceptible to each of the eight ingredients.



Mastering the administration of this environment recognizes that the effectiveness, extension and operational complexity of an arsenal can be greatly increased. Weapons can be more accurate when charged with making a surgical strike.

Joint Observations 4 through 6 and 10 are key to managing this dispensation (Section 3.5). Number 4 ac-

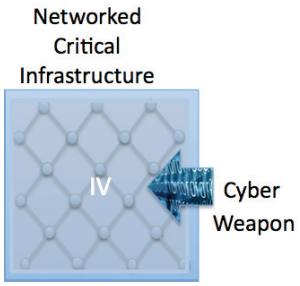
knowledges the many ICT benefits offered in the application of Convention principles. For example, it follows that accountability for accurate decisions and execution can be increased because the ability to discriminate between valid and prohibited targets can be greatly enhanced. Observation 5 draws attention to the enhanced status of individuals and other organizations. Eventually, it would be expected that there would be an increasing availability of advanced ICT-enhanced weapons. Observations 6 and 7 acknowledge that while the specific types of advanced weapons can legitimately remain secret, the attributes of how they can be effective are based on well-established, public domain scientific information. Finally, Observation 10 observes that the introduction of such weapons has complicated historical understanding of armed conflict, though this observation is more predominant in Dispensation IV.

3.4 Dispensation IV. Cyber Weapons in Networked Infrastructure

This dispensation is the intersection of cyber weapons and cyber targets. It is the breeding ground for many weapons that are yet to be envisioned. Likewise, from all indications of the path ahead for the role of the ICT in society, business, government and military, targets will grow exponentially. The mastery of this domain is seen as vital for those nation-states who seek to have military dominance going forward.

Examples of what takes place in this dispensation include:

- a small international interest group uses a packaged malware application to corrupt the data on the computer network of a government
- a home nation-state of a popular communications network equipment supplier remotely activates a hidden software feature that causes the equipment in the target country to crash and remain unstable for days
- a sophisticated, undetectable hack into the controls of a combat operation randomly alters coordinates and personnel designation information causing sporadic 'friendly fire'



In this dispensation, all of the eight ingredients of cyberspace are susceptible to cyber weapons, which are likewise susceptible to each.

Among other concerns, the administration of this environment recognizes that there are still yet to be defined "rules of the road," that this is an emerging field with huge commercial and strategic significance, and that critical infrastructures are increasingly exposed as cyber weapons proliferate and as society becomes increasingly dependent upon ICT for its many benefits.

Each of the ten Joint Observations are important to understanding and managing Dispensation IV. Discussion is made here regarding those observations not previously discussed in Sections 3.1 through 3.3. Observation 3 raises the concern that both sides had about the difficulty of distinguishing Convention-protected targets from legitimate targets. In Observation 8 the team discerns that, while there is great complexity, rapid change and other factors that make cyberspace incomprehensible, there are also fundamental scientific, engineering and mathematical limits and rules that can be better utilized for the administration of this dispensation. Finally, Observation 9 points out that a cyber event can take place without any awareness of the affected party at the time, if ever.

3.5 Joint Observations

The following ten observations were selected from many that were produced by the analysis. They were generated during the analysis of the articles of the Laws of War and by the examination of distinctions among the dispensations.

Joint Observation 1: Protected and non-protected critical infrastructure entities are intermingled in cyberspace.

Table 4. Summary of Joint Observations

	Dispensation				Ingredient							
Joint Observation	**I**	**II**	**III**	**IV**	**Environ.**	**Power**	**Hardware**	**Software**	**Network**	**Payload**	**Human**	**ASPR**
1. Protected and non-protected critical infrastructure entities are intermingled in cyberspace.		II		IV								
2. Protected humanitarian critical infrastructure lacks markers to designate its protected status.		II		IV								
3. Discrimination between military and civilian targets is more difficult in cyberspace.				IV								
4. ICT can be an enabler for better implementation of Convention principles concerning humanitarian needs.	I	II	III	IV								
5. Non-State Actors and Netizens can wield elevated power in cyberspace.			III	IV								
6. Cyber weapons have attributes not prev. seen with traditional weapons nor considered during the dev. of the current LoW.			III	IV								
7. Military forces will have distinct advantages in keeping cyber weapons secret.			III	IV								
8. The complexity of ICT and cyberspace propagates mystery about its nature and limits.		II		IV								
9. A cyber operation may take place undetected.				IV								
10. The ambiguity surrounding cyber war suggests a different approach.		II	III	IV								

Accepting this observation is a necessary step toward the preservation of principles of the Conventions that protect civilians. The protected entities will be harmed if they are impaired as a result of an attack on non-protected entities. Collateral damage is a long understood consequence of war. However the extent to which collateral damage (including impaired function) can occur now is greatly multiplied.

First, we observe the principle of protection from the Conventions. There are at least four distinct aspects relating to civilians and critical civilian infrastructure.[44]

Protected Populations: The Conventions establish protection for the "whole of the populations of the countries in conflict …"[45]

Protected Areas: The Conventions enable parties to establish "in occupied areas, hospital and safety zones and localities so organized to protect from the effects of war …"[46] "Civilian hospitals … may in no circumstances be the object of attack but shall at all times be respected and protected …"[47]

Protected Personnel: The Conventions establish protection for "Persons regularly and solely engaged in the operation and administration of civilian hospitals …"[48]

44 While it is the obvious context, the Conventions nevertheless make it clear that " …military objectives, or large industrial or administrative establishments" are legitimate targets. Geneva Convention IV, 1949 Annex 1, Article 4.

45 Ibid. Article 13.

46 Ibid. Article 14.

47 Ibid. Article 18.

48 Ibid. Article 20.

Protected Infrastructures: The Convention establishes that various modes of transportation dedicated to humanitarian missions "be respected and protected in the same manner ..."[49] "It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as food-stuffs, agricultural areas for the production of food-stuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive."[50]

Second, we observe the obligation to establish separation. In the context of 1949, this was physical separation.

Separated: The Conventions direct that protected entities "be situated as far as possible from ..." potential military targets.[51]

There is an abundance of commentary on the interpretation and application of the referenced articles. The point here is not to draw a fine line, but rather to establish that there is some measure of protection instituted.

Today's highly interdependent, life-sustaining infrastructures require electricity and communications network connectivity for their basic function. Modern societies have lost the ability to survive without them. This is especially a concern for urban areas, which in this sense are especially delicate. The proliferation of just-in-time inventory management further exacerbates this problem.

Modern hospitals are highly networked facilities, dependent on telemedicine, and continuous retrieval of geographically remote information that is most likely stored in a data center that also houses other industrial and administrative data, and possibly even defense-related data. Maintaining the function of such a facility requires protection of the information and communications infrastructure dependencies. The equivalent target prohibition is substantially augmented in this environment (distributed computing and storage, co-location, other factors), making compliance much more difficult.[52] Detangling would likely be very costly and is contrary to current infrastructure architecture trends that are taking advantage of just-in-time availability of data storage capacity and computer processing cycles.[53]

Recommendation 1 addresses this concern (Section 4).

Joint Observation 2: Protected humanitarian critical infrastructure lacks markers to designate its protected status.

The Conventions direct that protected entities "shall be marked ...,"[54] and that markers should be "distinctive" and "clearly visible."[55] They further direct that qualified personnel to "bear the emblem provided for ..."[56] Finally, the Conventions direct various modes of transportation to "be marked ..."[57]

Modern medical data is often in electronic form and resides in, or is transported through, cyberspace. This includes patient records, research sources, operational controls and billing information. Such humanitarian assets are seldom separated from other non-protected infrastructure. The reasonable argument could be made that only basic medical care is what is protected and modern medicine is an excessive demand and therefore off limits. However, the Convention vision does recognize that there are "ever-increasing requirements of civilization" and "the ever progressive needs of civilization."[58] [59]

Recommendation 2 addresses this need (Section 4).

Joint Observation 3: Discrimination between military and civilian targets is more difficult in cyberspace.

This observation is based on Joint Observations 1 and 2. It is significant because discrimination is an important obligation of an attacker.[60] "One of the existing restrictions of International Humanitarian Law (IHL) that may

49 Ibid. Articles 21, 22.

50 Ibid. Article 54.

51 Ibid. Article 18.

52 Further to this point, the constraint of Geneva Convention IV Annex 1 Article 4: "Hospital and safety zones shall fulfill the following conditions: (c) They shall be far removed and free from all military objectives, or large **industrial or administrative establishments**." [emphasis added].

53 Distributed network processing and storage, or so-called 'cloud computing.'

54 Ibid. Article 18.

55 Ibid. Article 18.

56 Ibid. Article 20.

57 Ibid. Articles 21, 22.

58 Hague II, 1899, Preamble.

59 Hague IV, 1907, Preamble.

60 The four factors influencing an attack decision include discrimination, necessity, proportionality and chivalry, see part III.Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace (Falls Church: Aegis Research, 2000).

be seen as applying to cyberspace concerns the responsibility of an attacker to seek military targets."[61]

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[62]

It is noted that it is incumbent upon the asset owner to mark his property. This observation is incorporated in Recommendations 1 and 2 (Section 4).

Joint Observation 4: ICT can be an enabler for better implementation of Convention principles concerning humanitarian needs.

ICT can also improve the implementation of various requirements of the Conventions. Examples include tracking individuals, enabling family communications, and supporting basic cultural, educational and spiritual needs.

> The Parties to the conflict shall take the necessary measures to ensure that children under fifteen, who are orphaned or are separated from their families as a result of the war, are not left to their own resources, and that their maintenance, the exercise of their religion and their education are facilitated in all circumstances. Their education shall, as far as possible, be entrusted to persons of a similar cultural tradition.[63]

> They shall, furthermore, endeavour to arrange for all children under twelve to be identified by the wearing of identity discs, or by some other means.[64]

> All persons in the territory of a Party to the conflict, or in a territory occupied by it, shall be enabled to give news of a strictly personal nature to members of their families, wherever they may be, and to receive news from them. This correspondence shall be forwarded speedily and without undue delay.[65]

Other benefits include those afforded to prisoners of war with regard to spiritual and family communications. The benefits of ICT-enabled humanitarian critical infrastructure, or ICT otherwise applied, include efficiency and speed, enhanced compliance monitoring, and an improved quality of what could be offered. Online cyber schools are an emerging trend that demonstrates how educational needs could be met virtually for youth populations when provided with Internet access.

Joint Observation 5: Non-State Actors and Netizens can wield elevated power in cyberspace.

The technological expertise and financial backing required to have a state-of-the-art arsenal of traditional weapons is very high. Being able to achieve these levels is, in part, what has defined a superpower. But the international power stature is yet another arena revolutionized by ICT. For now, "Cyber threats come from a vast array of groups and individuals with different skills, motives, and targets."[66] "We face nation states, terrorist networks, organized criminal groups, individuals, and other cyber actors with varying combinations of access, technical sophistication and intent."[67] The reality for nation-states is that Non-State Actors (NSAs) and individuals can use computers built for non-military applications in powerful ways against them.[68]

---

61 For example, additional rules include prohibition against indiscriminate attacks andthe need to minimize collateral civilian damage .Knut Dörmann, "Computer Network Attack and International Humanitarian Law", 19-05-2001 Cambridge Review of International Affairs "Internet, State and Security Forum",Cambridge, May, 2001.

62 Protocol I Additional to the Geneva Convention, 1977, Article 48.

63 Geneva Convention IV, 1949, Article 24.

64 Ibid.

65 Ibid., Article 25.

66 Robert, S. Mueller, III, Federal Bureau of Investigation (FBI) Director Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, DC, (March 17, 2010).

67 Dennis C. Blair, Director of National Intelligence Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, Washington DC, (February 2, 2010).

68 There are no generally agreed international definitions for Non-State Actors (NSA's) or Non-Governmental Organizations (NGO's). As a result, any organization that is not an Intergovernmental Organization (IGO) is considered an NSA. However, the International Law Association's Committee on Non-State Actors in International Law has established a working definition to start sorting out the various actors. The Hague Conference: First Report of the Committee on Non-State Actors in International Law: Aims, Approach and Scope of Project and Legal Issues, International Law Association, The Hague, 2010. Three criteria for identifying non-state actors were established: (1) bodies comprised of and governed or controlled by States or groups of States, such as IGOs and groups of States such as the Group of 7, were excluded; (2) NSAs were defined in terms of what they actually do and how they behave; and (3) actors were defined in terms of whether the functions they actually perform in the international arena have real or potential effects on international law. Expressly excluded as non-state actors were the Mafia, Al-Qaeda and pirates, the commonality of each being its criminality.

The challenges attached to this issue are substantial and varied. They include dealing with the loss of distinction between uniformed combatants and non-uniform combatants, the gap of educating the population of netizens, the profound reality of numbers on the order of billions of computers and online users, and asymmetric relationships in terms of what is at stake to be lost.

Recommendation 3 considers this challenge.

Joint Observation 6: Cyber weapons have attributes not previously seen with traditional weapons nor considered during the development of the prevailing Laws of War.

Cyber weapons focus on information, logic, and control. Relative to traditional weapons, their attributes can seem relatively extreme, as they can (a) be delivered on the order of a second from around the world, (b) have viral-like behavior in spreading, (c) have artificial intelligence that enables them to learn and adapt, (d) be produced relatively cheaply, and (e) be easily copied and transferred. While these attributes may be extreme from a weapons standpoint, they are also the same attributes of the ICT and networks that we use everyday in our personal lives and in our businesses. However, when combined with an aim toward destruction, they have a very different demeanor.

The Conventions have long ago set precedent for prohibitions of weapons of mass destruction. Chemical and biological weapons serve as the examples of types of weapons outlawed. They have been "justly condemned by the civilized world" and otherwise prohibited by international law.[69] [70] The joint team concluded that the exploration of the attributes of cyber weapons based on public domain information, would be a highly useful endeavor.

Recommendation 4 incorporates this observation.

Joint Observation 7. Military forces will have distinct interests in keeping cyber weapons secret.

The number of distinct cyber weapons is likely to be very large in a very short period of time. Those nations that are developing the most advanced weapons have a strong interest in being able to protect the intelligence surrounding such capabilities. Advantages include the ability to surprise an adversary who is unaware of a capability, or to make the source and actual nature of an attack unknown, or to develop an awareness of what is possible and therefore strengthen one's own defenses.

Recommendation 4 factors in this constraint.

Joint Observation 8: The complexity of ICT and cyberspace propagates mystery about its nature and limits.

The complexity of ICT is impenetrable for all practical purposes. In addition, true mastery of the technology requires a solid grounding in the core competencies of physics, electrical engineering, mathematics and computer programming skills. There are too few in the policy community with such skills, which tends to cultivate discussions around the uncertain aspects or latest concern, as opposed to leveraging known reference points. We therefore have a mindset of computers being a "magical black box" where we do not know what is inside and only understand our inputs and outputs. Focus of media, intelligence, military, and even the business community tends to be heavily oriented on the threats. As a result, there are many policy developers and other decision makers influencing cyberspace with re-circulated and other-than-firsthand information. The scientific and engineering community has the advantage of understanding the component building blocks of critical infrastructure and is therefore able to understand the intrinsic vulnerabilities of its ingredients.[71] Integration of all of the relevant expertise is essential to making progress.

This observation is integrated into Recommendation 4.

Joint Observation 9: A cyber operation may take place undetected and attribution is problematic.

How do you know that you have observed a cyber operation? Attacks or other operations in cyberspace can be unobservable. Awareness of the event may be delayed or may never happen. Further, their cascading effects may be more significant at the second or third order, and the relationship between the first and subsequent orders may be unknown.

---

69 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, (The Geneva Protocol), 1925.

70 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (The Chemical Weapons Convention), 1992.

71 Karl F. Rauscher et al.Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal Homeland Security Special Issue, Vol. 9, No. 2, April, 2006.

Similarly, how do you know who has launched an attack? The mutability of message headers, ability to cloak origination information and other factors make absolute confidence in attribution fundamentally problematic.[72]

Joint Observation 10: The ambiguity surrounding cyber war suggests a different approach.

It is essential that the conditions for the application of the Conventions be clarified regarding cyber conflict. However there is currently an extremely wide range of opinions on what constitutes a cyber war. Exemplary of the ambiguity are the quotes shown here.

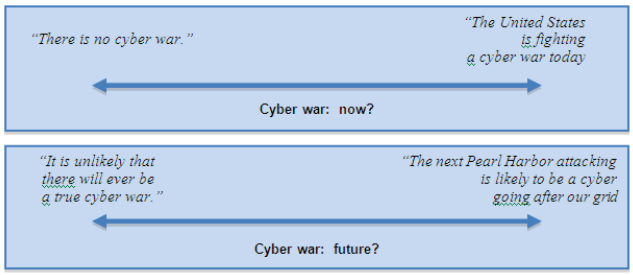


Figure 3. Contrast of Views on Cyber War[76]

In addition to sharp disagreements on the reality of cyber war now and in the future, the impact of an attack is another point of contention.[73] [74] [75] All of this may relate to the starting definitions or understanding of the proper way to view this new form of aggression and weaponry.

> Cyber warfare has never had either a clear definition or any mutually agreed-upon international convention that oversees it; yet it carries both huge incentives and damages for the states that are involved in it. The offenders are often treated leniently because of the lack of international cooperation and jurisdiction; examples can be seen drawn from the Titan Rain.[77]

Regarding computer network attacks, a legal expert from the International Committee of the Red Cross stated that "If CNA is used against an enemy in order to cause damage, it can hardly be disputed that CNA is in fact a method of warfare."[78] It may be that the existing paradigms of peace, war, sabotage, terrorism, and crime need to be augmented.

Recommendation 5 presents a joint recommendation from the team on this subject.

72 The degree of state control and responsibility is different for candidate regimes. Shackelford, Scott, J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Conference on Cyber Conflict Proceedings, Tallinn, 2010.

73 "Today, the opinion prevails in the U.S. and in a number of western countries that the threat of 'information wars' and, above all, the immensity and the consequences of 'information weapons' ... are strongly exaggerated." Alexander V., Fedorov, "International Information Security: the Diplomacy of Peace (Moscow: Moscow Institute of Physics and Technology, 2009), p. 30.

74 ""Cyber War is real. What we have seen so far is far from indicative of what can be done." Richard Clarke, Cyber War – The Next Threat to National Security and What to do about it, (New York: Harper Collins Publishers, 2010), p. 21.

75 "It is an area of warfare, cyber warfare, that I think needs to be one on which we focus greatly and has devastating potential on the downside." Admiral Mike Mullen, Chairman of the Joint Chiefs of Staff, quoted in, Lalit Kha Jha, "Cyberwarfare has devastating potential: Mullen", MSN News (January 13, 2011), http://news.in.msn.com/international/article.aspx?cp-documentid=4797248.

76 Quotes used above are:
[Upper left quote] Continuing: ". . . I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment." Howard Schmidt, quoted from Ryan Singel, "White House Cyber Czar: There is no Cyber War", Wired Magazine, March 4 2009. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/.
[Uper right quote] Continuing: "... and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking." Former Director of National Intelligence, Mike McConnell, Washington Post, February 28, 2010.
[Lower left quote] Peter Sommer and Ian Brown, "Reducing Systemic Cybersecurity Risk", OECD-IFP Project on "Future Global Shocks", (January 14, 2011). http://www.oecd.org/dataoecd/57/44/46889922.pdf.
[Lower right quote] Continuing: "... and that can literally cripple this country," CIA Director Leon Panetta, quoted in The New New Internet – The Cyber Frontier, (April 21, 2010), http://www.thenewnewinternet.com/2010/04/21/panetta-warns-cyber-attack-could-be-next-pearl-harbor/. Another related quote from Shawn Henry, assistant director of the FBI's cyber division, "Other than a nuclear device or some other type of destructive weapon, the threat to our infrastructure, the threat to our intelligence, the threat to our computer network is the most critical threat we face," "Terrorist groups are working to create a virtual 9/11, "inflicting the same kind of damage on our country, on all our countries, on all our networks, as they did in 2001 by flying planes into buildings." quoted in Homeland Security Newswire,(January 6, 2009). http://homelandsecuritynewswire.com/fbi-us-facing-cybergeddon.

77 Maya Tao,"Law Brief on Cyberwarfare", The Maya Tao Blog, http://mayatao.com/wp-content/uploads/2010/11/Law-Brief-on-Cyber-Warfare.pdf, (accessed, January 21, 2011).

78 Knut Dörmann, "Computer Network Attack and International Humanitarian Law", 19-05-2001 Cambridge Review of International Affairs "Internet, State and Security Forum",Cambridge.May, 2001.

4. Joint Recommendations

This paper submits five joint recommendations. Each is vital to the preservation of the humanitarian-related critical infrastructure principles provided by the Conventions. Each recommendation is also actionable and, if implemented, can be effective in breaking through a present obstacle. The experts from both sides urge timely consideration and action for each of these recommendations.

The Laws of War have been revised over time. Sadly, history tells us that the motivation for such change has been unprecedented treacherous acts of mankind against each other. The resulting condemnation "of the general opinion of the civilized world" has resulted in the development of "the ever increasing requirements of civilization."[79] [80] Each of these recommendations seeks to harmonize concepts of modern, networked critical infrastructure with those of the Geneva and Hague Conventions and Protocols.

The recommendations below are applicable to the four dispensations as shown in Figure 4. Each of the recommendations address the particular major concerns identified in each dispensation.

The implementation of these recommendations will require both leadership and support from governments, the private sector, and NGOs. Table 5 portrays the landscape of the required leadership and source of expertise. It should be observed that the primary roles are often shared with the private sector or NGOs.

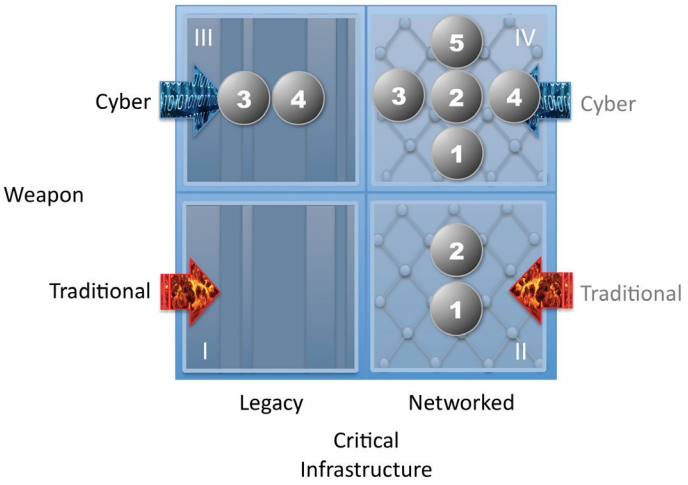


Figure 4. Application of the Recommendations

This perhaps is a surprise to many who expect government leadership as the natural and only default. This is an example of private sector led *private*-public partnership.[81] This is an important emphasis given the private sector's advanced expertise, operational knowledge, and ownership regarding ICT and ICT infrastructure.

Each recommendation is presented in a concise manner in order to support critical decision-making, to maintain the momentum from the report development and to mobilize resources toward action. The outline of the recommendation presentation is as follows:

- **Title** for identification and a summary
- **Background** to provide the essential elements of the context of the issue being addressed
- **Recommendation** to identify who should do what
- **Required Commitments** crisply outlines the requirements from critical parties for success
- **Benefits** encapsulates the value proposition for implementing the recommendation
- **Alternatives and Their Consequences** outlines the other options and likely outcomes
- **Next Steps** offers suggestions for keeping the momentum and focus
- **Measures of Success** provides means to objectively evaluate performance.

79 Geneva Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 1925.

80 Hague II, 1989, Preamble.

81 *P*PP, to emphasize the role of the private sector leadership; a phrase coined by the author in keynote speech prepared for the European Union Ministerial Conference on Critical Information Infrastructure Protection, Tallinn, 27-28 April 2009.

Table 5. Leadership Posture and Expertise Sourcing for Recommendation Implementation

	Leadership			Expertise		
Recommendation	Government	Private Sector	NGOs	Government	Private Sector	NGOs
1. Advise on the Commingling of Protected and Unprotected Critical Infrastructures in Cyberspace	Supporting	Primary	Primary	Supporting	Primary	Primary
2. Application of the Distinctive Emblem Principle in Cyberspace	Primary	Supporting	Primary	Supporting	Primary	Primary
3. Recognizing New Non-State Actor and Netizen Power Stature	Primary	Supporting	Primary	Primary	Primary	Primary
4. Consideration of the Geneva Protocol Principles for Cyber Weaponry	Primary	Supporting	Supporting	Primary	Primary	Supporting
5. Research and Analysis of a Third, 'Other-Than-War' Mode	Primary	Supporting	Primary	Primary	Primary	Supporting

Key	
	Primary Role
	Supporting Role

4.1 Detangling Protected Entities in Cyberspace

Background

The Geneva Convention provides for some measure of protection for purely humanitarian-focused entities and personnel, under qualifying conditions, during war.[82] However, protected and non-protected entities are intermingled in cyberspace, placing the protected entities in jeopardy.[83]

How the protected entities have arrived here is understandable. The benefits of embracing ICT are tangible. They include enhanced capabilities, improved efficiency and reduced costs. Further, with a prevailing peacetime mindset, the rapid development of technology and an often competitive environment, it is not surprising that there has been a lack of deliberate planning to ensure a continued equivalent protection from the consideration of the Laws of War.

Until now, most analyses of this situation have been at the national level. This recommendation provides guidance for a major cooperative effort, starting first as a bilateral effort, and then extending to a multilateral one.

This recommendation directly addresses the intense interdependence and complexity of cyberspace that is a characteristic for both Dispensation II and Dispensation IV (Section 3, Figure 1).

RECOMMENDATION 1

Russia and the U.S., along with other willing parties, should conduct an evaluation of the present state of the intermingling of protected, humanitarian critical infrastructure with non-protected infrastructures in order to determine whether existing Convention and Protocol articulation is sufficient and whether significant detangling of essential humanitarian critical infrastructures is feasible.

Required Commitments

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

- Private sector companies from both countries must lend technical expertise and business experience.
- Russian and U.S. government stakeholders must support the collaboration with their respective experts.[84] [85]
- International humanitarian aid non-government organizations (NGOs) must provide their insights.
- Each of these parties must be committed to an objective analysis and exploration of available options.

82 Geneva Convention IV, Relative to the Protection of Civilian Persons in Time of War, 1949, Articles 13, 14, 18, 20-22, 54.

83 See Joint Observation 1, Protected and non-protected critical infrastructures are intermingled in cyberspace, Section 3.2. There is an abundance of commentary offered on the application of the referenced Convention Articles. The point here is not to draw a fine line, but rather to establish that there is some measure of protection afforded.

84 The major tasks of military policy in the sphere of ensuring international information security will be ... the arrangement of conditions for equitable and reliable international information exchange based on the universally acknowledged norms and principles of international law ...",Alexander V., Fedorov, International Information Security: the Diplomacy of Peace (Moscow: Moscow Institute of Physics and Technology, 2009), p. 30.

85 "... strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity." – Point 7 of Near-Term Action Plan, White House, Executive Office of the President, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure (May 29, 2009),http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . resulting in decreased civilian protection from Geneva and Hague Conventions.
- Deliberately wait for time to pass and learn from lessons of first tragedies that occur . . . accepting responsibility for a result that may include unacceptable loss of life and property.
- Accept inability of the Conventions to transfer into cyberspace . . . resulting in loss of the humanitarian protections in times of conflict.

Benefits

The result of implementing this recommendation will be a bilateral or multilateral determination that will advise as to whether the Convention-provided protections of humanitarian entities is still viable, is substantially degraded, or is substantially degraded and not recoverable facing the current trends in cyberspace. The implementation of this recommendation promotes the preservation of the principles of the Conventions that protect basic humanitarian interests – both qualified civilians and assets, and that therefore make up a vital part of critical infrastructure. Ultimately, the value of maintaining the ability to distinguish protected zones can be immeasurable, as the value of human life is immeasurable. In addition, the objectives promote the protection of other humanitarian interests.

Next Steps

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

- 1-1 Convene experts from Russia, the U.S. and other willing parties to determine if the current levels of entanglement and likely consequences are acceptable.
- 1-2 Prepare a summary of the findings from the above analysis.
- 1-3 If significant guidance is developed as a product of the steps above, implement a joint trial to measure the feasibility of the proposal.
- 1-4 Make appropriate recommendations based on steps above.

Measures of Success

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

- Bilateral consensus, followed by subsequent multilateral consensus, on the acceptability of the current state of entanglement.
- The successful conducting of a trial for proposed recommendations.
- De-entanglement of protected humanitarian critical infrastructure, or enlargement of protection to cover selected entanglement conditions.

4.2 Application of the Distinctive Emblem Principle in Cyberspace

Background

The Geneva and Hague Conventions direct that protected entities, protected personnel and protected vehicles be marked in a clearly visible and distinctive way.[86] Further, the Conventions establish specific standards for the distinctive emblem itself, instruction for its application, and consequences for its misuse.[87] A belligerent's ability to recognize a declared protected entity is vital if they are to comply with the Conventions. Thus, the disciplined use of the designated marker is essential for the protection principles to be maintained. Humanitarian-related critical infrastructure has been infused with ICT and fully integrated into cyberspace. The result is that there are no "distinctive," "clearly visible," "markers" in cyberspace for entities, personnel or related assets. Without such markers, the humanitarian interests intended to be shielded by the Conventions are in jeopardy.[88]

As an example, the joint team offers for consideration the introduction of markers in cyberspace to designate protected entities, personnel and other assets. One possible example of such a marker may be the introduction of a top-level domain (TLD) extension, such as ".med" or ".+++" or ".nsz" for "no strike zone," similar to ".com" or ".org."[89] Great care must be given to avoid conflict with an existing country's or organization's domain. This recommendation directly addresses the need for guideposts in cybersecurity that is characteristic for both Dispensation II and Dispensation IV (Section 3, Figure 1).[90]

It is noted here that related exiting principles, such as the obligation of the asset owner to be diligent in appropriately marking, and for integrity in application, need also be included in proposed solutions.[91]

RECOMMENDATION 2

Russia and the U.S., along with other willing parties, should conduct a joint assessment of the benefit and feasibility of special markers for zones in cyberspace that can be used to designate humanitarian interests protected by the Conventions and Protocols of War.

Required Commitments

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

- Private sector companies must lend their expertise to understanding the options for establishing designations in cyberspace.
- Russian and U.S. government stakeholders must support the collaboration with their respective experts.
- Internet governance organizations must support the implementation of measures to achieve the distinctive emblem principle in cyberspace.

86 Joint Observation 2, Protected critical infrastructure lacks markers to designate its protected status, Section 3.2.

87 Geneva Convention I, Articles 38-44, 53, Annex I Article 6; Geneva Convention IV, Articles 18, 20, 21, Annex I Article 6.

88 As with the physical world, an unintended consequence of marking protected sites is that they can be identified by an attacker, e.g., a terrorist.

89 There may be one mark or multiple marks, but each must be recognized across systems.

90 The significance for Dispensation II regards reconnaissance.

91 Geneva Convention IV, Article 18.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . resulting in a continued reliance on the Conventions as is, with potential increased vulnerability of protected entities, or potential increased risk of inadvertent destruction of protected entities, or uncertain ability to recognize protected entities, personnel and other assets in cyberspace.
- Deliberately wait for time to pass and learn from lessons of first tragedies that occur . . . accepting responsibility for a result that may include unacceptable loss of life and property.
- Accept inability of the Conventions to transfer into cyberspace . . . resulting in loss of the humanitarian protections in times of conflict.

Benefits

The benefit of the implementation of this recommendation is that it will provide for the clear recognition of a protected entity, person, or other asset in cyberspace. The ability for a belligerent attacker to be able to identify such protection status is vital to being able to preserve the Conventions that deal with the protection of humanitarian interests. The day after a protection domain is established, qualifying organizations can start benefiting with this unique identification.

Next Steps

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

- 2-1 Russian, U.S. and other willing parties should convene to develop the objectives for a proposal to apply the distinctive emblem principle in cyberspace.
- 2-2 Representatives of the forum described in the (2-1) should present this proposal to the appropriate international standards development organizations (SDOs).[92]
- 2-3 Based on feedback from the above steps, a trusted neutral entity should address the political and financial arrangements needed to support the implementation of the agreement.

Measures of Success

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

- Bilateral consensus on a proposal for the application of the Geneva and Hague Convention distinctive emblem principle.
- The adoption and support of markers to designate protected entities, personnel and other assets in cyberspace.
- The ability for belligerent attackers to be able to clearly identify protected entities, personnel and other assets in cyberspace.[93]

92 For example, a "Birds of a Feather" (BOF) session at the Internet Engineering Task Force (IETF) to propose a Request for Comments (RFC).

93 Automated detection by systems should be a component of this achievement.

4.3 Recognizing New Non-State Actor and Netizen Power Stature

Background

One of the most fundamental, underlying assumptions for agreements to the Laws of War is that nation-state powers constitute the sufficient signatures.[94] Historically, wars have been waged between ethnic groups or political entities (e.g., nations, kingdoms). The chief contention has been the occupation and control of territory. Cyberspace introduces new 'territory.'[95] [96] Another new reality is that cyber weapons are a revolutionizing enabler. They can elevate Non-State Actors (NSAs) and Netizens to high statures of power.[97] Attention must be given to this new, asymmetric power structure.[98] Non-government organizations (NGOs) and non-nation-state actors – including individuals – now have the potential to wield the power to have devastating effects on public safety, economic security or national security.[99]

In seeking to harmonize the Convention principles that protect civilians and civilian infrastructure with this new reality, a wide range of issues become evident. Just one of these issues is raising awareness about the Convention requirements among citizens, or better here, netizens. The Conventions hold that "The High Contracting Parties undertake, in time of peace as in time of war, to disseminate the text of the present Convention as widely as possible in their respective countries, and, in particular, to include the study thereof in their programs of military and, if possible, civil instruction, so that the principles thereof may become known to the entire population …" Thus, the concept of priority for civilian awareness (in order to perform some function) in the implementation of the Conventions is not a novel one.

94 See the Geneva and Hague Convention signatures.

95 Mary Ann Davidson, The Monroe Doctrine in Cyberspace, Testimony of Oracle Chief Security Officer before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, March, 2009.

96 This reality is key to the administration of Dispensations II and IV.

97 This reality is part of the administration of Dispensations III and IV.

98 See Joint Observation 5, Non-State Actors and Netizens can wield elevated power in cyberspace, Section 3.3.

99 Existing international law recognizes three categories: uniformed military forces of a state, organized armed groups, and civilians. Each of these can be targeted under different circumstances. Other measures exist within law enforcement and intelligence operations regimes that provide instruments for characterizing 'bad actors' in cyber space.

RECOMMENDATION 3

Russia, the U.S. and other interested parties, should assess how best to accommodate Convention principles with the new reality that cyber warriors may be non-state actors.

Required Commitments

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

- Governments must be open to new paradigms of respect, dialogue, cooperation and trust with Non-State Actors (NSAs).
- Non-Government Organizations (NGOs) and Multi-National Companies (MNCs) must offer insights and vision for new workable solutions.
- Governments and a critical mass of both NSAs and Netizens must be able to demonstrate some new, minimal, to-be-defined level of cooperation in cyberspace.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . resulting in continued alienation with emerging force in cyberspace.
- Over-react before an assessment by inviting NSAs and Netizens an equal position with nation-states . . . resulting in chaos from the unmanageable numbers and untrained resources.
- Over-react by rejecting a further discussion . . . accelerating the alienation of NSAs.

Benefits

The benefits of conducting this assessment include having more insights into a critical growing dynamic, being prepared for the additional risks from the emergence of this new force, and being able to anticipate the needs of this new community in regards to instruction and training regarding the Geneva and Hague protections for civilians and critical civilian infrastructure.

Next Steps

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

- 3-1 Russian and U.S. experts identify and agree on the structure and objectives of the assessment.
- 3-2 Russian and U.S. experts aggregate the data needed for the assessment, inviting other interested parties - especially NSAs - to be part of the analysis.
- 3-3 The combined team prepares the assessment report and presents to critical international government and industry fora.[100]

Measures of Success

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

- The role of NSAs in preserving and implementing the Conventions is better understood.
- The Conventions are confirmed as sufficiently effective in accommodating NSAs and Netizens as is, or are otherwise adjusted to do so.

100 Examples may include the United Nations (UN), Cyber40, Institute of Electrical and Electronics Engineers (IEEE), and the International Chamber of Commerce (ICC).

4.4 Consideration of the Geneva Protocol Principles for Cyber Weaponry

Background

One of the most prominent accomplishments of the Laws of War has been the agreement established for the prohibition "… of the use in war of asphyxiating, poisonous or other gases, and of bacteriological methods of warfare."[101] The use of such was " justly condemned by the opinion of the civilized world."[102] Is the list of weapons that would offend "the conscience" of the nations complete?[103] Some proposed candidates from traditional arsenals include nuclear weapons, cluster bombs, and land mines. More recently, questions have arisen about the emerging cyber arsenal.

With modern civilization's utter dependence upon ICT and cyberspace, there are increasing concerns about the potential consequences of cyber weapons, which have the ability to introduce new sorts of attack, influence and devastation. Indeed cyber weapons themselves can introduce new attributes to an arsenal. Some of these attributes include the potential for viral behavior, with the lack of discrimination and travel at computer speeds. These attributes, combined with a belligerent cause, are an understandable reason for concern.

On the other hand, military enterprises can provide decisive battle space advantage with superior weapons. This is particularly the case when such weapons are unknown and cannot therefore be well defended against.[104] Such concerns are legitimate. However, they do impede international discussions of such weapons. With such constraints, it is understandable why progress in international cooperation is stalled.

An innovative approach that significantly satisfies the concerns above, is one that would (a) avoid compromising military intelligence regarding specific capabilities, and that would (b) operate within the existing Convention principles, and that would (c) operate with discussion on attributes that are well established in the public domain.[105] This recommendation employs such an approach. This recommendation directly addresses the need for anticipating emerging challenges that is characteristic for both Dispensation III and Dispensation IV (Section 3, Figure 1).

RECOMMENDATION 4

Russia, the U.S. and other interested parties, should conduct a joint analysis of the attributes of cyber weapons in order to determine if there are attributes analogous to weapons previously banned by the Geneva Protocol.

Required Commitments

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

- Russian and U.S. experts would need to be open to discuss weapon types based upon publicly available information.
- Russian and U.S. governments must be open to the possibility that some weapon attributes may be unacceptable as they are offensive "to the principles of humanity and from dictates of public conscience."[106]

101 Geneva Protocol,1928.

102 Ibid.

103 Ibid.

104 Publicly available information includes widely published principles physics, electrical engineering and computer programming, and historically experienced malicious code, the 8i and Intrinsic Vulnerability approach is also instructive here.

105 The proposal to apply banned weapons principles to cyberspace is not new. However, proposals tend to pivot the transfer at from the application point (i.e., inspection) as in Kenneth Geers, , Cyber Weapons Convention, Naval Criminal Investigative Service (NCIS), Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn, Estonia, 2010.

106 Protocol Additional I, 1949, Article 1.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . resulting in the possibility of a cyber arms race, or the unleashing of cyber weapons with undesirable affects, or the loss of an opportunity to apply the lessons learned from previous Convention impetus.
- Over-reacting by imposing harmful regulations and restrictions in technology . . . resulting in impediments to innovation, and forcing advanced research and development underground.
- Restrict discussions on cyber weapon attributes . . . with the outcome of a surprise future experience with a weapon type requiring a reaction.

Benefits

The benefits of successfully completing a Russia-U.S. bilateral assessment of Geneva Protocol principles for cyber weaponry, include "breaking the ice" among cyber "titans" for discussions on the new frontier of conflict, creating an international framework for understanding the attributes of cyber weapon attributes, and preventing a cyber weapon that can have devastating effects on civilians and critical civilian infrastructure.

Next Steps

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

- 4-1 Russian and U.S. experts cooperate to develop the objectives and methodology for the study to consider cyber weapons in light of the Geneva Protocol principles on weapons.
- 4-2 Russian and U.S. experts commence analysis of both the Protocol principles for weapons and the attributes of cyber weapons using public domain information.
- 4-3 Russian and U.S. experts prepare a report on their findings and present their conclusions to their respective stakeholders, and make available to other international fora, as appropriate.

Measures of Success

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

- The development of a joint Russian-U.S framework for understanding the Protocol prohibition principles for certain weapon types.
- Russian and U.S. experts conduct a joint analysis of the attributes of ICT-based weapons.
- The resulting joint Russian-U.S. report is used to determine which, if any, attributes of cyber weapons may be similar to types of weapons prohibited by the Geneva Protocol of 1928.

4.5 Consideration of a Third, 'Other-Than-War' Mode

Background

Critical infrastructures are increasingly exposed to cyber threats, the impact of which could be serious loss of life and property. The Conventions provide protections for civilians and critical humanitarian assets that meet strict qualifications.[107] [108] However, the applications of these protections are primarily oriented around war.[109] There is not a clear, internationally agreed upon definition of what would constitute a cyber war. In fact, there is quite a bit of confusion.[110] Figure 3 documents how senior government leaders have incompatible opinions about the most basic aspects – the existence and the reality of cyber war.[111]

The conventional understanding of conflict status begins with a linear continuum placing peace at one end, and war at the other. In between are progressive levels of conflict.[112] [113] [114] Currently, cyber events are seen through this lens with an aim to harmonize them with existing thresholds and frameworks.[115]

There are some fundamental challenges in applying the existing regimes. These include factors such as cyber events having the potential for being unobservable and the attribution of an attack being very difficult to attain with high confidence.[116] In observing the current level of difficulty in this harmonization quest, the team determined that a bilateral engagement devoted to reevaluating the fundamental needs and opportunities in this arena would be very valuable.[117]

RECOMMENDATION 5

Russia and the U.S., along with other willing parties, should explore the value of recognizing a third, 'other-than-war' mode in order to clarify the application of existing Conventions and Protocols.

Required Commitments

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

- Russian and U.S. national security stakeholders must acknowledge that the current uncertainty about the definition for war in cyberspace is not acceptable and be committed to seeking clarity.
- Russia, the U.S., and other interested parties, must convene for the purpose of vigorous exploration of new frameworks categorizing conflict.
- The same must be devoted to open analysis and consideration of new options for managing behavioral norms in cyberspace.[118]

107 First Geneva Convention, Articles 19 – 44, and Articles 1 – 13 in Annex I; Second Geneva Convention, Articles 22 – 45; Fourth Geneva Convention Articles 1 – 26, and Annex Articles 1 – 8; Protocol I, Articles 1 – 34, 48 – 79; Protocol II, Articles 1 – 28; Protocol III, Articles 1 – 17.

108 Team members observed that the authors of the Conventions had in mind that the concept of war was not just a formally declared state, but rather intended to include conflict level of violence.

109 E.g., Geneva Convention IV, Preamble and Articles 1 -3.

110 This is a point that can be easily verified by reviewing media headlines on the subject of cyber warfare.

111 Joint Observation 10, Section 3.5.

112 Existing legal frameworks provide structure that includes the regimes of law enforcement, intelligence operation, and military operation. Each of these has very different criteria for addressing threats, and any given cyber incident may be characterized under two or even all three headings, depending on the situation. So, parts of an intrusion could be investigated and prosecuted, parts could be dealt with immediately (and perhaps violently) by the military, and parts could be handled quietly through an executive order to an intelligence agency.

113 UN Charter Article 39.

114 Definition of Aggression, UN General Assembly Resolution 3314 (XXIX), 1974.

115 Cyber events can be (a) "international peace and security," which is lawful activity; (b) a use of force that is unlawful, but not permitting a forceful response; (c) an armed attack, allowing a unilateral forceful response to a specific incident; and (d) war, being a generalized state of hostilities in which all of the armed forces of one state may lawfully target all of the armed forces of another state. There also exist criteria and methods for movement from a lower level to a higher level in this structure.

116 Joint Observation 9, (Section 3.5).

117 This recommendation attends to an issue that resides in Dispensations II, III and IV. However, it is a prominent feature of the later (Section 3, Figure 1).

118 It is critical that such analysis include core competencies of the scientific and engineering disciplines.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing . . . resulting in continued confusion and disagreement about what constitutes acceptable peacetime behavior and a state of war in cyberspace.
- Reject out of hand the concept of a third mode . . . limiting discussion and alternatives to the current binary war and peace classification options.

Benefits

The value of considering a third mode is that the ensuing discussion will bring much needed clarity and structure to a very complex and confusing discussion. Equally beneficial would be its rejection after appropriate consideration because this would foster understanding about why it is only the current two modes that are preferred, and what contours and parameters are essential to their definition.

Next Steps

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

- 5-1 Russia, U.S. and other willing parties, decompose the current situation back to first principles and reconsider the possible options and attributes of an "other-than-war" mode.
- 5-2 Aggregate the stakeholder concerns for the net value of such a new structure and develop test criteria for each concern that would satisfy the stakeholder interests.
- 5-3 Perform joint analysis of the new structure based on the developed evaluation criteria and prepare a joint report that documents the conclusions.

Measures of Success

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

- A bilateral or multilateral consensus determination is made regarding the benefit of an internationally recognized mode of conflict that is "other-than-war."
- Appropriate follow-up action is taken to i) either implement such a third mode, or ii) effectively dismiss it from further consideration with decisive conclusions.

5. Conclusion

This paper has described the early steps of a Russia-U.S. bilateral process to strengthen both countries positions with regard to the protection of humanitarian critical infrastructure in cyberspace. The joint team began with a solid footing of agreement: the principles of the highly regarded Geneva and Hague Conventions that provide protections for humanitarian interests. In conducting this analysis, a system of four dispensations was introduced for managing the complex and dynamic landscape of issues. Examination of the dispensations gave rise to a focus on key Joint Observations with regard to rendering the Convention principles in cyberspace. The associated concerns from these observations were then addressed in five joint recommendations, which, if implemented, could enhance the preservation of humanitarian critical infrastructure in cyberspace.

The Russia-U.S. bilateral team is committed to continuing this important dialogue on critical infrastructure protection. Ongoing work includes supporting the implementation of the recommendations presented here, advancing bilateral progress to multilateral progress, and extending the dialogue to other areas of importance to both countries in the field of cybersecurity.

BIOGRAPHIES

About the Authors

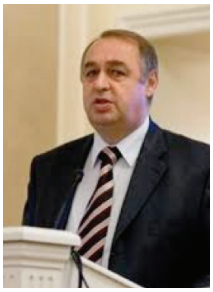
Karl Frederick Rauscher

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

Andrey Korotkov

Andrey Korotkov is the Global Information Processes and Resources Department Head at the Moscow State Institute of International Relationships (University), the BPMS Department Head at the School of IT-management at the Russian Academy of National Economy under the President of the Russian Federation. He is an expert on very large information systems, artificial languages and semiotics. Prof. Korotkov is a member of the High-Level Advisory Group of the UN Global Alliance on ICT for Development. In 2002 he was appointed the First Deputy Minister of the Ministry of Telecommunications and Informatization of the Russian Federation and in this position was responsible for a number of major federal information technology projects in Russia. Among them are the national critical infrastructure elements protection development. He holds a Ph.D. in Philology from Moscow State University and an Ec.D (Dr.Dr.) from the Academy of National Economy under the Government of the Russian Federation, and is a two-time recipient on the all-Russia IT Leader of the Year award (2006 and 2009). He is currently a Principal Researcher at the Institute of Mathematical Problems of Biology.

Contributing Subject Matter Experts



Artyom Adjemov

Artyom Adjemov is a professor of Computer Science and Communications and the Rector of Moscow Technical University of Communications and Informatics. He is an expert in telecommunications. Adjemov is the author of 60 scientific books and textbooks and is a member of both the International Academy of Communications and the International Academy of Open Education.

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, Barry has researched and published work on transatlantic relations, political-military affairs, and operational command and control systems for more than 30 years. He is a member of the Pi Alpha Alpha National Honor Society in Public Administration and a Woodrow Wilson Foundation Fellow. He holds a Doctorate of Public Administration (Information Management) from the University of Baltimore.

John S. Edwards

John S. Edwards has over 51 years of experience in the telecommunications field, spanning design, analysis, and business planning. He successfully established and managed several design groups and founded three companies, one of which was later a billion dollar acquisition by a large corporation. He has held senior-level management positions at a variety of companies, represented Nortel Networks on the Industry Executive Subcommittee of the Presidential National Security Telecommunications Advisory Committee for 25 years, and 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 was granted a PhD in Electrical Engineering from the University of Pennsylvania.

J. B. (Gib) Godwin, Rear Admiral (ret.)

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

Stuart Goldman

Stuart Goldman contributed to the computer and telecommunications industries for 45 years prior to his retirement. During this period he architected a number of communication systems and participated extensively in several national and international standards bodies, in a variety of leadership roles. He has been granted 25 patents and has an additional 53 pending applications. Stuart is a Bell Labs fellow.

Vladimir Ivanov

Vladimir Ivanov is the Director of the EastWest Institute's Moscow Office. Before his current position, he was responsible for managing EWI's Fiscal Transparency Program, including the publication of a series of studies on fiscal flows between the Russian federal budget and the regions. In 2006-2009 he played a leading role in EWI's cooperation with Russia on promoting international *private*-public partnerships to combat terrorism, particularly in the areas of cyber security, critical infrastructure protection and countering illicit trade in precious metals and gemstones. Ivanov currently is involved in all EWI projects with a 'Russia dimension,' particularly the U.S.-Russia bi-lateral dialogue on cybersecurity and Euro-Atlantic Security. His previous professional experience includes work in the fields of social sciences research, business journalism, and public relations.

Ivanov 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.

James Bret Michael

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

Viktor Minin

Viktor Minin is an expert in automatics, telemechanics and social psychology, and has 29 years of experience in information security. During his military career, he was responsible for information security issues at the Special Communication Information Service at the Federal Security Service of Russia. He is a member of the Coordination Council of CIS on Information at the Regional Communications Commonwealth and is the Chairperson of the Civil Advisory Committee on Science and Technology Aspects of Information Security.

Paul Nicholas

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

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

Boris Slavin

Boris Slavin has been the President of the Union of Chief Information Officers of the Russian Federation since 2008. He holds a Ph.D. in Physics from Moscow State University and is the author of several publications on IT governance and information society theory. Slavin has extensive practical experience in IT and has served as CIO of several Russian enterprises.

Leonid Todorov

Leonid Todorov earned his B.A. in management from the University of Copenhagen and his M.A. in Linguistics from Moscow State Pedagogical University. After the onset of the Russian reforms, he served for more than a decade as Chief of Staff to the late PM Yegor Gaidar. He has subsequently worked for a mining sector company and a PR firm, both headquartered in Moscow. In 2008, he joined the coordination center for the .RU top level domain, and serves as Deputy Director for External Relations in Russia's Internet registry. Leonid's focus is on Internet governance, IDNs, international cooperation, and cybersecurity. He has authored and coauthored a number of publications on these issues, and has presented at various national and international events.

Thomas C. Wingfield

Thomas C. Wingfield is a professor of International Law at the George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany, where he lectures on the rule of law, human rights, and the law of war. He is a Research Fellow at NATO's Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, where he is coauthoring a manual for the Law of Armed Conflict in Cyberspace. His research focuses on identifying the international legal standards which characterize the use of force and armed attack in cyberspace. He holds both a J.D. and an LL.M. from Georgetown University Law Center, and is completing an S.J.D. at the Law School of the University of Virginia. He is the former Chair of the American Bar Association's Committee on International Criminal Law, and is the author of THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE.

Elena Zinovieva

Elena Zinovieva graduated with honors from Saint Petersburg State University, studying Applied Computer Science in the humanitarian area with a focus in International Relations. She has also studied at Warsaw State University and at the Faculty of Philology of Saint Petersburg State University. Zinovieva received her Ph.D. in Political Science in 2009 from the Moscow State Institute of International Relations (MGIMO) where she completed a thesis on the role of international institutions and organizations in internet governance. She has published work in the fields of internet governance, ICT and policy, and the technological aspects of international relations, and currently works as a lecturer at MGIMO in the Political Science department.

Acronyms

8i	Eight Ingredient (Framework of ICT Infrastructure)
ASPR	Agreements, Standards, Policies and Regulations
ATIS	Alliance for Telecommunications Industry Solutions
BOF	Birds of a Feather
CCD	Cooperative Cyber Defense
CIP	Critical Infrastructure Information Protection
CIP	Critical Infrastructure Protection
CNA	Computer Network Attacks
COE	Counsel of Europe
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name Server
EWI	EastWest Institute
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
GUCCI	Global Undersea Communications Cable Infrastructure
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGO	Intergovernmental Organization
IHL	International Humanitarian Law
ISP	Internet Service Provider
ITU	International Telecommunications Union
LoW	Laws of War
MED	Symbols proposed for protected designation in cyberspace (Recommendation 2)
MNC	Multi-National Corporations
NATO	North Atlantic Treaty Organization
NGO	Non-Government Organizations

NSA	Non-State Actors
NSTAC	National Security Telecommunications Advisory Committee, The President's
NSZ	No Strike Zone
OECD	Organization for Economic Co-Operation and Development
PC	Personal Computer
*P*PP	Private-Public Partnership
PPP	Public-Private Partnership
RFC	Request for Comment
RFID	Radio Frequency Identification
RPG	Rocket-Propelled Grenade
ROI	Return on Investment
SCADA	Supervisory Control and Data Acquisition
TLD	Top-Level Domain
UAV	Unmanned Aerial Vehicle
UN	United Nations
URW	UnRestricted Warfare
U.S.	United States (of America)
VNSA	Violent Non-State Actors
WCI	Worldwide Cybersecurity Initiative
WWW	World Wide Web
+++	Symbols proposed for protected designation in cyberspace (Recommendation 2)

REFERENCES

Avalon Project, Yale University, avalon.yale.edu.

ATIS Network Reliability Steering Committee (NRSC) 2002 Annual Report, www.atis.org/nrsc .

ATIS Telecom Glossary, www.atis.org, 2007.

Blair, Dennis, C., Director of National Intelligence Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, February 2, 2010.

Brenner, Susan W., Clarke, Leo L., Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, Vol 43.

Brunner, Elgin, M. and Manuel Suter, Manuel, International CIIP Handbook, An Inventory Of 25 National And 7 International Critical Information Infrastructure Protection Policies, Center for Security Studies (CSS), Zurich, Switzerland, 2008/2009.

Charter of the United Nations, The, 1973.

Civil Defense in International Law, Advisory Service on International Humanitarian Law, International Committee of the Red Cross, June 2001.

Confusion on the Cyber-Battlefield – The World Needs Rules of Cyberwar, Science Daily, October 2010.

Clarifying the notion of direct participation in hostilities, ICRC, 2009.

Clinton Administration's Policy on Critical Infrastructure Protection, The, Presidential Decision Directive No. 63, White Paper, May 22, 1998.

Critical Infrastructure Protection, Executive Order 13010, Executive Order 13010, Federal Register, July 17, 1996. Vol. 61, No. 138.

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, White House, 2009.

Davidson, Mary Ann, The Monroe Doctrine in Cyberspace, Testimony of Oracle Chief Security Officer before the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, March 2009.

Definition of Aggression, UN General Assembly Resolution 3314 (XXIX), 1974.

Dion, Maeve, When Cyber Incidents Threaten National or International Security: What is the Law?, The CIP Report, Legal Insights, Volume 9 Number 7, January 2011.

Dörmann, Knut, Computer Network Attack and International Humanitarian Law, 19-05-2001 Article, Cambridge Review of International Affairs, Trinity College, Cambridge, May, 2001.

Dylevsky, I.N., et al., Russian Federation Military Policy in the Area of International Information Security: Regional Aspects, Moscow Military Thought 31, July 2009.

Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228, Federal Register, Vol. 66, No. 196, October 8, 2001.

Fedorov, Alexander V., Terrorism and International Information Security, Yaderny Kontrol, December 2001.

Fulghum, David A., Cyber Attacks No Longer Non-Kinetic, A Defense Technology Bog, September 2010.

Geneva Convention, The, The Geneva Conventions of 1949 and their Additional Protocols, Geneva.

Geneva Protocol, The; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, 1925.

Hague Convention, The Hague Convention of 1899 and 1907 The Hague.

Homeland Security Physical Security Focus Group Final Report, Network Reliability and Interoperability Council (NRIC) VI Issue 3, December 2003.

Homeland Security Presidential Directive 7, HSPD-7, December, 2003.

Hughes, Rex, Towards a Global Regime for Cyber Warfare, Cyber Security Project, Chatham House, London.

International Information Security: the Diplomacy of Peace. Moscow, 2009.

Komov, Sergey A., Korotkov, Sergey, V, Dylevsky, Igor N., Military Aspects of Ensuring International Information Security in the Context of Elaborating Universally Acknowledged Principles of International Law.

Lorents, Peeter and Ottis, Rain, Knowledge Based Framework for Cyber Weapons and Conflict, Proceedings of Conference on Cyber Conflict, CCD COE Publications, Tallinn, Estonia, 2010.

Michael, James Bret, On the Response Policy of Software Decoys: Conducting Software-based Deception in the Cyber Battlespace, IEEE Proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC'0), 2002.

Michael, James Bret, Tikk, Eneken, Wahlgrn, Wingfield, Thomas C., "From Chaos to Collective Defense," IEEE Computer Society, August, 2010.

Michael, James B., Wingfield, Thomas C., Wijesekera, Duminda, Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System, Proceedings of the IEEE Computer Society (27th) Annual International Computer Software and Applications Conference, 2003.

Moteff, John and Parfomak, Paul, Critical Infrastructure and Key Assets: Definition and Identification, CSR Report, October 2004.

Mueller, Robert, S. III, Federal Bureau of Investigation (FBI) Director Statement Before the House Committee on Appropriations, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, DC, March 17, 2010.

National Security of Russia, The. http://www.scrf.gov.ru/documents/sections/3/.

National Strategy for Homeland Security, The, U.S. Office of Homeland Security, July 16, 2002.

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, The, Office of the President, February, 2003.

Next Generation Networks Task Force Report, NSTAC, March 28, 2006.

Nonstate Actors: Impact on International Relations and Implications for the United States, National Intelligence Council, August, 2007.

NSTAC Report to the President on International Communications, The President's National Security Telecommunications Advisory Committee (NSTAC), August, 2007.

Our World. Views from the Field., International Committee of the Red Cross, 2009.

Public Data Network Reliability Focus Group Final Report, Issue 3, NRIC VII October 2005.

Participant Summary Results, Proceedings of the First Worldwide Cybersecurity Summit, Dallas, EWI 2010.

Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating To National Security, OECD, May 2008.

Rauscher, Karl Frederick, Reliability of Global Undersea Communications Cable Infrastructure, The Report, (ROGUCCI) IEEE, 2010. www.ieee-rogucci.org.

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

Rauscher, Karl F., Krock, Richard E., Runyon, James P., Eight ingredients of communications infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal, Volume 11, Issue 3, 2006.

Rauscher, Karl, F., European Commission-Sponsored, Availability And Robustness Of Electronic Communications Infrastructures (ARECI) Report, March 2007.

Rowe, Neil, C., U.S. Naval Postgraduate School , Ethics of Cyberwar Attacks, A chapter in Cyber War and Cyber Terrorism, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.

Russia's Cyber Security Plans, MIT Technology Review, April 2010.

Saunders, Steven Chris, Confusion on the Cyber-Battlefield – The World Needs Rules of Cyberwar, North Carolina Journal of Law and Technology, February, 2010.

Sabadia, Aisha, Austin, Greg, PROTECT! Cilivians and civil Rights in Couner-Terrorism, EWI Policy Paper, 2007.

Scott, James Brown, ed. The Hague Peace Conferences of 1899 and 1907, Vol. 1, The Conferences, The Johns Hopkins Press ,1909.

Schmitt, Michael, N., Hassiaon Dunniss, Heather, A., Wingfield, Thomas C., Computers And War: The Legal Battlespace, Background Paper prepared for Informal High-Level Expert Meeting on Current Challenges to International Humanitarian Law, Cambridge, June, 2004.

Security, Russian Federation Law on March 5, 1992, N 2446-I, as amended 1992 – 2007. http://www.scrf.gov.ru/documents/20.html.

Strategy of the National Security of the Russian Federation Until 2020, Presidential Decree No. 537, Russian Federation, May 12, 2009. http://www.scrf.gov.ru/documents/99.html.

Shanghai Cooperation Organization, The, http://www.sectsco.org/EN/

Shackelford, Scott, J., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, Conference on Cyber Conflict Proceedings, Tallinn, 2010.

Sommer, Peter and Brown, Ian, Reducing Systemic Cybersecurity Risk, OECD Multi-Disciplinary Issues International Futures Program, January 2011.

Suter, Manuel, A Generic National Framework For Critical Information Infrastructure Protection (CIIP), Center for Security Studies, ETH Zurich, August 2007.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), 107th United States Congress, October 2001.

U.S. Army Cyber Operations and Cyber Terrorism Handbook, 1.02, US Army Training and Doctrine Command, Fort Leavenworth, Kansas 2005.

U.S. Cyber Command Fact Sheet, U.S. Department of Defense, May 2010.

Voon, Tania, Pointing The Finger: Civilian Casualties Of NATO Bombing In The Kosovo Conflict, 2001.

Wingfield, Thomas C ., "The Law of Information Conflict : National Security Law in Cyberspace," Aegis Research, 2000.

Wingfield, Thomas, C., Michael, James B., An Introduction to Legal Aspects of Operations in Cyberspace Naval Postgradute School, The, Monterey, California, April 2004.

Wireless Network Reliability Focus Group Final Report, NRIC, VII Issue 3, October 2005.

EWI Board of Directors

EastWest Institute
Forging Collective Action for a Safer and Better World

OFFICE OF THE CHAIRMAN

Francis Finlay (U.K.)
EWI Co-Chairman
Former Chairman,
Clay Finlay LLC

Ross Perot, Jr. (U.S.)
EWI Co-Chairman
Chairman, Hillwood Development Company, LLC;
Member of Board of Directors, Dell, Inc.

Armen Sarkissian (Armenia)
EWI Vice-Chairman
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President and CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee of EWI Board of Directors
Senior Fellow, Harvard Business School

R. William Ide III (U.S.)
Counsel and Secretary
Partner, McKenna Long & Aldridge LLP

Leo Schenker (U.S.)
EWI Treasurer
Senior Executive Vice President, Central National-Gottesmann, Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former President of Finland

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Thor Bjorgolfsson (Iceland)
Chairman
Novator

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

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

Mark Chandler (U.S.)
Chairman and CEO
Biophysical

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

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

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

Adel Ghazzawi
Managing Director
BV Group

Melissa Hathaway (U.S.)
President
Hathaway Global Strategies, LLC;
Former Acting Senior Director for Cyberspace
U.S. National Security Council

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

Emil Hubinak (Slovak Republic)
Chairman and CEO
Logomotion

Wolfgang Ischinger (Germany)
Chairman
Munich Security Conference

Haifa Al Kaylani (U.K.)
Founder & Chairperson
Arab International Women's Forum

Donald Kendall, Jr. (U.S.)
Chief Executive Officer
High Country Passage L.P.

Sigrid R. v. C. Kendall (U.S.)

Zuhal Kurt (Turkey)
CEO
Kurt Enterprises

James A. Lash (U.S.)
Chairman
Manchester Principal LLC

Christine Loh (China)
Chief Executive Officer
Civic Exchange, Hong Kong

Ma Zhengang (China)
President
China Institute of
International Studies

Michael Maples (U.S.)
Former Executive Vice President
Microsoft Corporation

Francis Najafi (U.S.)
Chief Executive Officer
Pivotal Group

Frank Neuman (U.S.)
President
AM-TAK International

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

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

John R. Robinson (U.S.)
Co-Founder
Natural Resources Defense Council

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

Ramzi H. Sanbar (U.K.)
Chairman
Sanbar Development Corporation, S.A.

Ikram Sehgal (Pakistan)
Chairman
Security and Management Services

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
Chief Executive Officer
Bud Smith Organization, Inc.

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

William Ury (U.S.)
Director
Global Negotiation Project
at Harvard Law School

Pierre Vimont (France)
Ambassador
Embassy of the Republic of
France in the United States

Alexander Voloshin (Russia)
Chairman of the Board of Directors
OJSC Uralkali

Charles F. Wald (U.S.)
Former Deputy Commander
U.S. European Command

Zhang Deguang (China)
President
China Foundation for
International Studies

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

NON-BOARD COMMITTEE MEMBERS

Marshall Bennett (U.S.)
President
Marshall Bennett Enterprises

John A. Roberts, Jr. (U.S.)
President and CEO
Chilmark Enterprises L.L.C.

J. Dickson Rogers (U.S.)
President
Dickson Partners, L.L.C.

George Sheer (U.S.)
President (retired)
Salamander USA & Canada
Founder & CEO
International Consulting Group, USA

CHAIRMEN EMERITI

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

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

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

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

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

Ira D. Wallach* (U.S.)
EWI Co-Founder

DIRECTORS EMERITI

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

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

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

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

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

William E. Murray* (U.S.)
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)
Former Minister of Foreign Affairs of Norway

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

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

* Deceased

Founded in 1980, the EastWest Institute is a global, action-oriented, think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe, and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) non-profit organization with offices in New York, Brussels and Moscow. Our fiercely-guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
Belgium
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka Street 7/5,
Building 1, 6th Floor
Moscow, 125009
Russia, +7-495-2347797

EWI New York Center
11 East 26th Street
20th Floor
New York, NY 10010
U.S.A. 1-212-824-4100

www.ewi.info