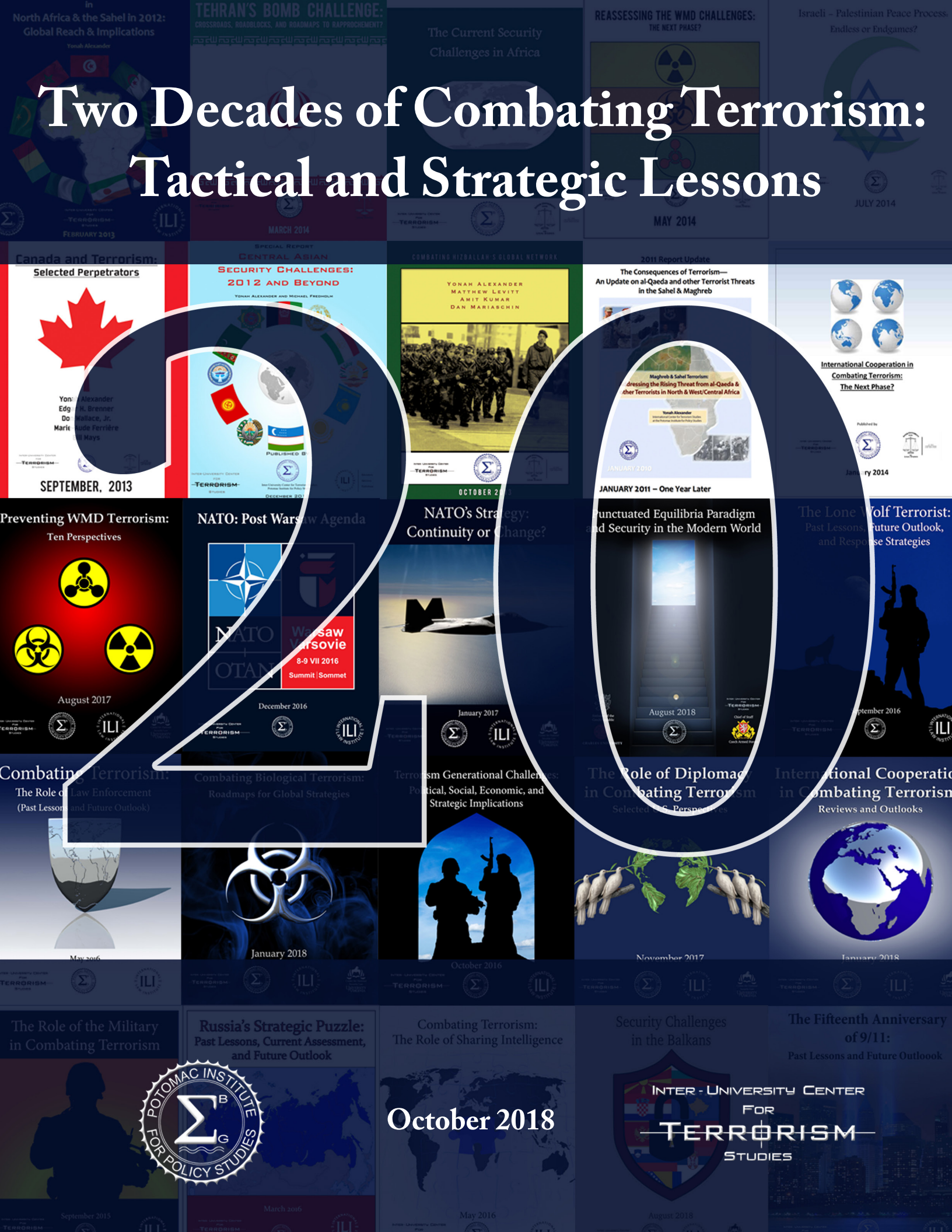
Two Decades of Combating Terrorism: Tactical and Strategic Lessons



October 2018

Potomac Institute for Policy Studies

Inter-University Center for Terrorism Studies

THE INTER-UNIVERSITY CENTER FOR TERRORISM STUDIES

Two Decades of Combating Terrorism: Tactical and Strategic Lessons

October 2018

Table of Contents

DISCLAIMER

The contributors have slightly edited their presentations as recorded in the taped event transcripts. The authors, editors, and research staff cannot be held responsible for errors or any consequences arising from the use of information contained in this publication. The views expressed do not necessarily reflect those of the institutions associated with this report.

Please contact the Inter-University Center for Terrorism Studies at the Potomac Institute for Policy Studies,
901 North Stuart Street, Suite 200, Arlington, VA 22203
Tel. 703-562-4513, 703-525-0770 ext. 237 Fax 703-525-0299
yalexander@potomacinstitute.org www.potomacinstitute.org
www.terrorismelectronicjournal.org www.iucts.org

Cover Design By Alex Taliesen

INTRODUCTION

Professor Yonah Alexander
Director, Inter-University Center for Terrorism Studies and
Senior Fellow, Potomac Institute for Policy Studies

From the dawn of history, humanity has continuously faced two critical security challenges. The first is "natural", or "Mother Nature's", disasters. It includes a wide range of disruptions and destruction to human lives and property. Hurricanes, tornadoes, earthquakes, tsunamis, monsoons, droughts, floods, heat waves, wildfires, and varieties of pandemics arising from biological pathogens, cause some of the most frequent catastrophic costs to individuals, communities, and civilizations.

The second permanent and equally significant security concern consists of "man-made" threats such as technological and economic calamities, ideological and political radicalization and extremism, terrorism, insurgencies, and wars.

Both challenges represent security concerns that include the safety, welfare, and rights of ordinary people; the stability of the state system; the success of national, regional and global economic development; the expansion of liberal democracies; and perhaps, even the survival of civilization itself.

Consider, for example, several landmark historical anniversaries related to the dual-danger from "natural" and "manmade" challenges. First, in 1918 an influenza pandemic, often regarded as the deadliest in modern times, killed an estimated 50-100 million people worldwide. Moreover, the Asian flu originated in 1957-1958 and caused the death of some one to four million individuals. Mention should be made of the deadly Ebola virus that represented a major health security challenge with unprecedented fear and anxiety over public safety around the world. Other current infection challenges include the Zika virus, which causes microcephaly and other birth defects, as well as the cholera epidemic, spread by bacteria from water or food contaminated with feces, which is alarmingly expanding in war-torn Yemen. In short, the expansion of pandemic outbreaks of deadly infectious disease is only a matter of time. The Centers for Disease Control and Prevention recently reported that during the 2015-2017 period, it had already "monitored more than 300 outbreaks in 160 countries, tracking 37 dangerous pathogens in 2016 alone."

Another century-old landmark event occurred on June 28, 1914, when the Archduke Frank Ferdinand, heir to the Austrian-Hungarian throne and his wife, Sophie, were assassinated in Sarajevo. This tragic attack perpetrated by Gavrilo Princip, a young Bosnian terrorist, triggered a series of escalating diplomatic and military moves in Europe and beyond that contributed, at least partly, to the outbreak of World War I. The resulting horrific human and political costs eventually caused the Second World War, with all its unprecedented national and global consequences, and subsequently led to the Cold War and the escalation of terrorism throughout the world. And thus,

in the past four decades, terrorism has evolved further**.** On November 4 1979, Iranian "radicals" seized the U.S. Embassy in Tehran and held the American diplomats captive for 444 days. Also, in 1998 U.S. embassies in Kenya and Tanzania were attacked by al-Qaeda members and on September 11, 2001 bin Laden's operatives perpetrated the most devastating terrorist attack in world history, to name a few key events.

Since this report focuses on "Two Decades of Combating Terrorism: Tactical and Strategic Lessons", a brief overview is provided on some related threats and responses to be followed by an academic context and the selected contributions by colleagues over the past twenty years.

Terrorism: Some Perspectives

Undoubtedly, conflicts emerge from ideological, religious, and national animosities that will continue to make the terrorism challenge a global problem for the remainder of the twenty-first century. Ensuring safety and interests of its citizens at home and abroad will continue to be every government's paramount responsibility in the future. Understanding the methods of operation employed by terrorists, identifying both the present and future threats and specific targets, and becoming fully aware of the damage and consequences that may result from acts of terror, will assist governments in responding effectively to the specter of terrorism nationally and globally.

Once again, terrorism is as old as history itself. In modern times there are four major challenges projected by state and non-state acts of violence that are contrary to the laws of armed conflict and warfare. These concerns relate to the safety, rights, and welfare of individuals and defined communities; the stability of geopolitical structures of nations; sustained health of economic development and prosperity; and the expansion and perhaps even the survival of democracies.

The key question then is whether the international community is capable of crafting adequate responses to terrorism, diffusing expanding conflicts regionally and inter-regionally, engaging in constructive peace processes, and striking a delicate balance between security measures and democratic value systems.

Indeed, the response to this question is most complicated, partly because each state defines "terrorism" unilaterally on the basis of its own unique domestic and foreign relations considerations. There is, however, some universal agreement as to the unlawful nature of attacks directed against non-combatants. Similarly, there appears to emerge a broad consensus among concerned nations regarding a wide range of counterterrorism structures and resources, as well as the implementation of policies and actions. Among the utilized measures frequently mentioned are legislation, law enforcement, intelligence, scientific and technological advancement, economic and military responses, and, finally, diplomacy and international cooperation.

Several general terrorism research findings prior to 9/11 are notable. First, many governments and people have failed to appreciate the magnitude and implications of the terrorist threat. Some countries have tended to regard terrorism as a minor nuisance or irritant. As a result, a large number of states have not yet developed a commitment strong enough to deal effectively with the problem of terrorism.

Second, there are no simplistic or complete solutions to the issue of terrorism. As the tactics utilized to challenge the authority of the state are, and continue to be, novel, so too must be the response of the instruments of the state. We must also be cautious to avoid the kinds of overreaction that could lead to repression and the ultimate weakening of the democratic institutions we seek to protect.

Third, having achieved considerable tactical success during the past three decades, terrorists sometimes find it politically expedient to restrain the level of political violence. These self-imposed restraints will not persist indefinitely, and future incidents may continue to be costly in terms of human lives and property. Certain conditions, such as religious extremism or a perception that the "cause" is lost, could provide terrorists with an incentive to escalate their attacks dramatically.

And fourth, the vulnerability of modern society and its economic infrastructure, coupled with new opportunities for the utilization of sophisticated high-leverage conventional and unconventional weaponry, require nation-states, both unilaterally and in concert, to develop credible responses and capabilities to minimize future threats.

Since 9/11, the following selected counterterrorism strategies need to be adopted or strengthened: develop coherent governmental and intergovernmental policies; establish efficient organizational structures to conduct, coordinate, and implement policies; introduce new legal instruments to close gaps in domestic and international law; produce quality human and technological intelligence and enhance sharing within and among nations; strengthen law enforcement capabilities at all levels to encourage regional and global cooperation; wage an intensified campaign to disrupt the flow of funds to terrorist movements in concert with financial and economic institutions worldwide; prevent the proliferation of weapons of mass destruction to rogue states and terrorist groups; initiate new concepts, doctrines, training, and missions for military forces tasked with combating terrorism in different environments such as urban insurgencies; increase cooperative relationships and alliances with like-minded nations through diplomatic efforts and provide counterterrorism technical assistance to those nations in need of support; and expand the involvement of civic societies, such as religious, professional, and educational bodies, in participating in the battle against terrorism.

The implementation of the foregoing approaches guarantees neither a prompt nor an achievable total victory over terrorism. The challenge facing the international community must be constructed on a long-term, realistic, and integrated war strategy of both weapons and ideas not dissimilar to the twentieth century experiences fighting Fascism, Nazism, and Communism. Whether the post-9/11 world learns the lessons of past and is successful eliminating the globalization and brutalization of modern terrorism requires heeding the advice of Jose Maria Aznar (former Prime Minister of Spain): "Now is the time for us to carry out our duty and to learn the important lessons of our past actions. This is the best way of ensuring that what we do in the future will serve to bring about the final defeat of terrorism."

Since this report on "Two Decades of Combating Terrorism: Practical and Strategic Lessons" is our last publication under the academic framework of the Inter-University Center for Terrorism Studies and the Potomac Institute for Policy Studies during the past twenty years, a brief overview of selected current terrorism threats and relevant responses is in order. Consider the following developments in the United States and abroad as recorded from governmental and non-governmental open sources during October 2018:

- Packages sent to the Pentagon test positive for the deadly poison ricin and a Utah suspect was arrested and confessed to this alleged crime.

- British authorities warned that terrorist attacks involving biological or chemical weapons are getting closer.

- European Union (EU) officials deplored Russian cyber attacks against the Organization for Prohibition of Chemical Weapons (OPCW) in The Hague.

- U.S. urges dialogue to eliminate nuclear weapons.

- Turkey signs a declaration of intent with 12 other NATO allies to cooperate on Maritime Unmanned Systems (drones).

- Israel revealed the existence of a secret nuclear warehouse in Tehran housing documents and equipment from Iran's nuclear weapons program.

- Iranian terrorist plots plan attacks in Europe and elsewhere.

- The Czech Republic's counterintelligence agency, DIS, disrupted a series of servers that Hezbollah was using for recruitment throughout the EU.

- And, the U.S. House Homeland Security Committee reported that the threat of Islamic terrorism in the country continues to be an issue of security concerns.

Three other terrorist-related events that are dubbed by some media coverage as "The October 2018 Surprises" are the following. First, the Saudi Government's kidnapping and murder of journalist Jamal Khashoggi at its Consulate in Istanbul is once again focusing world attention on "terrorism from above" with its serious consequences for regional and global security. Second, a dozen bombs were sent to former U.S. Government officials, elected representatives, a businessman, an actor, and the media and were intercepted without death or injury. A suspect, Cesar Sayoc, was arrested and was reportedly also planning some 100 attacks directed at Democratic leaders and critics of President Donald Trump. This threat, although rather primitive, can still result in undermining the political democratic stability in the U.S. and beyond. And third, Robert Bowers, an Anti-Semitic extremist, targeted a Pittsburgh synagogue on Saturday October 27th killing 11 Jews during prayer services. This incident, considered the most dramatic terrorist attack directed against Jewish targets in American history, also underscores the expansion of hate crimes in the United States and elsewhere around the world.

In sum, in considering the last two decades of terrorism challenges in national, regional, and global dimensions, two critical lessons come to mind. One is the Chinese proverb asserting that "one who studies the past, knows the future" and the second observation, attributed to the philosopher Hegel, that "we learn from history that which we do not learn from history."

An Academic Context

Future historians will probably label the 1990s as the decade of ethnic, racial, religious, and national radicalization and violence. The term "terrorism" will most likely continue to be defined both academically and professionally as the calculated employment of threats and violence by individuals, subnational groups, and state actors seeking to obtain political, social, economic, and strategic objectives in violation of law, intended to create overwhelming fear in a target area larger than the victims threatened or attacked.

Moreover, for the past twenty years terrorists have already introduced into contemporary life a new scale of globalization and brutalization in terms of conventional and unconventional threats, impacts, and responses. We are, indeed, in the midst of a new "Age of Super and Cyber Terrorism" with its serious implications for national, regional, and global security concerns. In addition to biological, chemical, radiological, nuclear challenges, non-explosive weapons will become more effective against technologically developed societies in the future. The key question therefore is whether civilization will survive in the face of these escalating dangers.

It is these strategic concerns that motivated the Terrorism Studies Program at George Washington University and the Potomac Institute for Policy Studies in 1998 to jointly raise the awareness of the threat and to provide alternative response recommendations to governmental, intergovernmental, and nongovernmental bodies on how to reduce the risks of terrorism to manageable levels. To this end, both institutions decided to cooperate initially in co-sponsoring a series of interdisciplinary seminars and research publications.

More specifically, two decades ago, six conferences and seminars were held in the Washington, D.C. area on the following topics: "Cyberterrorism and Information Warfare: Threats and Responses"; "Special Briefing on Terrorism: Current and Future Threats"; "Counterterrorism Strategies: A Future Agenda"; "The Increasing Threat of Contemporary Terrorism"; and "Biological Terrorism: Political and Legal Responses."

Similar activities have been considerably expanded over subsequent years under the administrative structures of the Inter-University Center for Terrorism Studies (IUCTS), and the International Center for Terrorism Studies (ICTS), both of which are based at the Potomac Institute for Policy Studies (PIPS) under the directorship of Professor Yonah Alexander. This academic structure also cooperated with the Inter-University Center for Legal Studies (IUCLS), co-directed by Professor Yonah Alexander and Professor Edgar H. Brenner and located at the International Law Institute (ILI), which was established by the Georgetown University Law Center in 1955 and is chaired by Professor Don Wallace.

Thus, in 1999 some 37 events on terrorism-related topics were organized in the U.S. and abroad such as in London at the International Institute for Strategic Studies; the Centre for Policy Research at the Forum for Strategic and Security Studies and the Institute for Defense Studies and Analysis in New Delhi; the Turkish Economic and Social Studies Foundation (TESEV) in Istanbul; and at Tel Aviv University in Israel; and overall, for the period 1998-2018 a total of 486 seminars and conferences were organized with hundreds more meetings and briefings.

Also, since 1999 a major research project on "Counterterrorism Strategies for the 21st Century: National, Regional, and Global Agenda", and supported with funding from public foundations, has been developed and housed at PIPS. The basic analytical framework for this multi-year and multi-authored project has focused on four major questions. First, in each country analyzed, what are the governmental and public perceptions of the terrorist threat on the primitive, technologically advanced, and mass destruction levels? Second, how successful have governments' policies and actions been in combating both domestic and international terrorism? Third, what factors influence the governments' willingness and ability to cooperate with other nations in combating terrorism? And fourth, what does the counterterrorism performance record of the specific country look like?

In addition to national perspectives, it became necessary to provide regional and global assessments of counterterrorism strategies, consequently resulting in the expansion of the research framework. Moreover, the assessment of successful counterterrorism policies was evaluated on the basis of the following criteria: the reduction in the number of terrorist incidents; reduction in the number of casualties in terrorist incidents; reduction in the monetary cost inflicted by terrorist incidents; reduction in the size of the terrorist groups operating in a country; number of terrorists killed, captured, and/or convicted; protection of national infrastructure (e.g. transportation, communications, economic and political institutions, and security installations and units); preservation of basic national structures and policies (e.g. the rule of law, democracy, and civil rights and liberties); and successes and failures of international cooperation in combating terrorism (e.g. bilateral, regional, and global).

A supplementary funded major research project that was initiated in 2002 (partly undertaken in the aftermath of 9/11), is "Foreign Affinity Terrorism in the 21st Century: How to Combat the International Network in the United States." An advisory panel of scholars and professionals was established at ICTS with Yonah Alexander as project director and principal investigator, to develop an appropriate research protocol to guide future studies in this area. Some of the principal issues included the following questions:

- What are the organizational infrastructures of international terrorist networks in the United States and how are they conducting illegal activities, such as propaganda, fund raising, recruitment, arms purchases, training, and other support for terrorist organizations?

- What policies and legal protection frameworks are available to reconcile security considerations with those liberal democratic values regarding the suspect aliens (e.g., admission and exclusion, civil rights, and extradition of political offenders) and the suspect citizen (e.g., arrest, detention, jury trial)?

- What are counter foreign-affinity terrorism lessons learned and which "best practices" responses should be recommended for more effective strategies in reducing future challenges posed by terrorists to the security concerns of the United States?

- What did the intelligence and law enforcement community know—or what should they have known—about foreign affinity terrorism in the past two decades?

- What changes should be made so that intelligence and law enforcement agencies obtain information about foreign nationals and U.S. national co-conspirators who are suspected of planning to engage in terrorist activities?

- What changes in foreign-affinity counterterrorism coordination need to be made among federal, state, and local officials? What complexities, such as costs, technology, manpower, and legislation, may interfere with such counter-measures?

- What changes need to be made for foreign nationals with respect to immigration and visa applications? Should naturalized U.S. citizens participating in foreign-affinity terrorism be stripped of their citizenship?

- Are keeping citizens alert to potential terrorist threats through special briefings and timely advisories important measures in preventing foreign-affinity terrorism or does it "tip off" foreign-affinity terrorists that intelligence has been gathered on their potential future targets?

- Have the U.S. government's counterterrorism plans gone beyond the legitimate needs of national security and are they infringing on constitutional rights of suspect aliens and suspect citizens in the name of patriotism and security?

Following the above mentioned questions, several books have been published: *Combating Terrorism: Strategies of Ten Countries* (Michigan University Press, 2002), edited by Yonah Alexander with a Foreword by James R. Woosley; *Counterterrorism Strategies: Successes and Failures of Six Nations* (Potomac Books, formerly Brassey's, Inc., 2006), edited by Yonah Alexander with a Foreword by Jose Maria Aznar; and *Terrorists in our Midst: Combating Foreign-Affinity Terrorism in America* (ABC-CLIO Praeger, 2010), edited by Yonah Alexander.

In addition to these three volumes, a total of 54 other books related to different aspects of terrorism and counterterrorism questions were published during 1999-2015. For example, Yonah Alexander and Michael S. Swetnam have written and edited several books, such as: *Osama bin Laden's Al-Qa'ida: A Profile of a Terrorist Network* in 2001, nearly a year before 9/11; *Al-Qa'ida: Ten Years After 9/11 and Beyond* (2012); *Al-Qa'ida's Mystique Exposed: Usama bin Laden's Private Communications* (2015); *ETA: A Profile of a Terrorist Group* (2001); and *Information Warfare and Cyber Terrorism: Threats and Responses* (1999 and 2001), 5 volumes.

Additionally, a series of 15 multi-volume books titled *Terrorism: Documents of Local and International Control—U.S. Perspectives* (Dobbs Ferry, New York: Oceana Publishing), was edited by Yonah Alexander and Donald Musch and published in 1999, 2000, 2001, and 2002. Some of the other notable books published during the past two decades include: *Countering Biological Terrorism in the U.S.* (1999), edited by David W. Siegrist and Janice M. Graham with Yonah Alexander and Donald Musch as General Editors; *Legal Aspects of Terrorism in the United States* (2000), 3 vols. edited by Yonah Alexander and Edgar H. Brenner; *Super Terrorism: Biological, Chemical, and Nuclear"* (2001) edited by Yonah Alexander and Milton Hoenig; *Terrorism and Business: The*

Impact of September 11, 2001 (2002), by Dean C. Alexander and Yonah Alexander; *Evolution of U.S. Counterterrorism Strategy* (2007), 3 vols. edited by Yonah Alexander and Michael Kraft; *The New Iranian Leadership: Ahmadinejad, Terrorism, Nuclear Ambition, and the Middle East Conflict* (2007) by Yonah Alexander and Milton Hoenig, *Turkey, Terrorism, Civil Rights, and the European Union* (2008), co-edited by Yonah Alexander, Edgar H. Brenner, and Serhat Tutuncuoglu Krause; *Terrorism on the High Seas: From Piracy to Strategic Challenges* (2009), edited by Yonah Alexander and Tyler B. Richardson; *Terrorism in our Midst: Combating Terrorism in America* (2010), edited by Yonah Alexander; *The Islamic State: Combating the Caliphate without Borders* (2015), by Yonah Alexander and Dean C. Alexander; and *NATO: From Regional to Global Security Provider* (2015), edited by Yonah Alexander and Richard Prosen.

Other research efforts during the past two decades produced 74 major reports on a broad range of issues such as conventional and unconventional threats (e.g. biological, chemical, nuclear, cyber); perpetrators (e.g. lone wolves, sub-state groups, state-sponsored terrorism); tactics (e.g. kidnapping, assassination, hostage-taking, bombing); regions and countries (e.g. U.S., Europe, the Balkans, the Middle East, Africa, Asia, Latin America); case studies (e.g. Hezbollah, refugees, Jerusalem); and responses (e.g. intelligence, law enforcement, military, and diplomacy). These publications were edited with introductions by Yonah Alexander and published by IUCTS and ICTS at PIPS in cooperation with associated institutions such as the ILI and the Center for National Security Law at the University of Virginia.

For instance, in 1998 the following reports were released: "Cyber-Terrorism and Information Warfare: Threats and Responses" (April, 1998); "Emerging Threats of Biological Terrorism: Recent Developments" (June, 1998); "Terrorism: Current and Future Trends" (August, 1998); and "The Increasing Threat of Contemporary Terrorism" (October, 1998). Two decades later in 2018, four reports were published: "The Role of Diplomacy in Combating Terrorism: Selected International Perspectives" (March, 2018); "Security Challenges in the Balkans" (August, 2018); "Punctuated Equilibria Paradigm and Security in the Modern World" (October, 2018); and "Two Decades of Combating Terrorism: Tactical and Strategic Lessons" (October. 2018).

To be sure, additional reports were published over the past twenty years related to specific joint academic projects between IUCTS, ICTS, and PIPS with other U.S. and international partners. One case in point is a special report titled "Why the Maghreb Matters: Threats, Opportunities, and Options for Effective U.S. Engagement in North Africa" published with the Conflict Management Program (SAIS) at the Johns Hopkins University in March 2009. This effort was chaired by General (Ret.) Wesley Clark and included a panel of distinguished experts such as former U.S. Secretary of State Madeleine Albright, Ambassador Stuart Eizenstat, and Professor I. William Zartman. Seven additional annual reports on "Terrorism in North Africa and the Sahel" were authored by Yonah Alexander and published by PIPS, IUCTS, and the ILI during 2011-2017.

Other notable series reports were released by the Blue Ribbon Study on Biodefense co-chaired by Senator Joseph Lieberman and Governor Thomas J. Ridge. For example, a bipartisan report on "A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts" was published in October 2015 with institutional affiliation of IUCTS and Hudson Institute. A subsequent report published by the panel on "Biodefense Indicators: One Year Later, Events Outpacing Federal Efforts to Defend the Nation" (December 2016) with the institutional sponsors of IUCTS, PIPS, and Hudson. The academic work of the bipartisan panel currently continues with the participation of Yonah Alexander as an ex officio member.

Aside from the publication of books and reports the IUCTS, ICTS, PIPS, and other affiliated institutions in the U.S. and abroad have been involved in a supporting role in producing two academic journals during the past two decades. The first publication is *Terrorism: An Electronic Journal and Knowledge Base*. This effort was initially developed in 1998 as an on-line follow-up to *Terrorism: An International Journal* published in 1977 by Crane, Russak, and subsequently by Taylor and Francis. Yonah Alexander founded these two publications and served as their Editor-in-Chief. Launched again in its current form in August 2012, *Terrorism: An Electronic Knowledge Base* provides continuity to earlier studies on the "Age of Terrorism" and closes research gaps in the growing literature on the manifold aspects of the subject. The new electronic resource focuses on identifying warning signals on conventional and unconventional terrorism in the post-9/11 era and recommends national, regional, and global strategies to confront the potential challenges to all societies.

The second academic effort is *The International Journal on Minority and Group Rights* founded by Yonah Alexander, a former Editor-in-Chief in 1991, which is currently published by Brill/Nijhoff in cooperation with the Raoul Wallenberg Institute at the University of Lund in Sweden. This publication is devoted to interdisciplinary studies of the legal, political, and social problems which minorities and indigenous peoples face in all countries of the world. For the purposes of the *Journal*, the groups are seen as clearly recognizable segments of society, defined by relatively constant factors, such as religion, race, culture, or language. Current developments, not least the spread of violent ethnic and religious conflicts, underline the need for a periodical publication dealing with the rights of persons belonging to minorities and contributions which demonstrate how human rights standards and good governance guidelines can make a better world for all.

The third journal titled *Partnership for Peace* was initiated by NATO's Partnership for Peace Training Center (PFP) in Ankara, Turkey, in cooperation with Yonah Alexander, who served as Editor-in-Chief for several years beginning in 2010. The aim of this interdisciplinary journal is to provide a forum for the exchange of information and expertise among nations in the area of international security, peace studies, and military cooperation-related issues as well as to emphasize the principle that "global problems require global solutions" with the effective contributions of all nations. With this view in mind, the publication sought to establish an up-to-date knowledge

base on peacekeeping operations undertaken by international bodies including NATO, the United Nations, the European Union, and the Organization of African States.

Finally, extensive media coverage by both domestic and international press also resulted in many hundreds of television and radio interviews as well as hundreds of published articles during the past two decades. Selected examples of media outreach include: ABC News, Al-Jazeera, Al-Monitor, Bulgarian International Television, CBS News, *The Chicago Tribune*, CNN, C-SPAN, *Defense Daily*, Hong Kong Phoenix TV, *The Huffington Post, The Jerusalem Post, The Los Angeles Times, The Miami Herald*, Moroccan News Agency, NBC News, *The New York Times*, NHK Japan Broadcasting Corporation, NPR, Reuters News, Sputnik International News (Russia), *The Telegraph*, *The Straits Times*, Voice of America, *The Washington Post*, and *The Washington Times*.

To be sure, the academic agenda of the IUCTS, ICTS, IUCLS, and other affiliated bodies nationally and internationally are looking ahead for further academic activities beyond 2018. Its work agenda includes both previously developed and newly mounted projects. These include the following selected terrorism-related topics: biological, chemical, nuclear, radiological, cyber, space, science and technology, intelligence, law enforcement, military, diplomacy, business, education, the media, and international cooperation.

To implement these and other relevant academic projects the current organizational structures such as the internship program (training the next generation of scholars and professionals), the Inter-Parliamentary Council to Combat Terrorism (headquartered in Brussels), the Diplomatic Forum (involving dialogues with American and foreign ambassadors), and the cooperative arrangements with numerous academic bodies worldwide will be considerably broadened with expected additional foundations support. Hopefully, we will be guided by Goethe's observation that "all intelligent thoughts have already been thought; what is necessary is only to try to think them again."

Acknowledgements

Deep appreciation is first due to the Potomac Institute for Policy Studies for its leadership and support, particularly by Michael S. Swetnam (CEO and Chairman), General (Ret.) Alfred Gray (Senior Fellow and Chairman of the Board of Regents), Dr. Jennifer Buss (President), Gail Clifford (Vice President for Financial Management and Chief Financial Officer), and the late Thomas O'Leary (Executive Vice President and Chief Officer). Many other staff members, such as Alex Taliesen and Sharon Layani, have contributed immensely to our academic mission.

Other extraordinary colleagues elsewhere are Professor Don Wallace Jr. (Chairman, International Law Institute) and both Professor John Norton Moore (Director of the Center for National Security Law and the Center for Oceans Law and Policy, University of Virginia School of Law), who

provided inspiration and continuing cooperation of our academic work. Also, hundreds of academics, diplomats, policymakers, and professionals around the world have participated in our activities over the years.

The research, editorial, and organizational efforts of the International Center for Terrorism Studies interns during the summer and fall 2018 semesters are also appreciated. The participating undergraduate and graduate students include: Talia Andreottola (American University), Jesse Berman (University of Virginia), John Keblish (University of Pennsylvania), Catie Ladas (University of Maryland), David Matvey (Carnegie Mellon University), Dante Moreno (George Washington University), Emily Nestler (College of Brockport, SUNY), Robin O'Luanaigh (University of North Carolina), Lavanya Rajpal (Georgetown University), Linda Rauch (University of Albany, SUNY), Lauren Sasseville (College of William and Mary), David Silverman (George Washington University), and Johnathan Trent (Loyola University in Chicago).

Finally, the generous financial support of private and public foundations in the United States and abroad also deserves our gratitude.

SELECTED REMARKS

Mr. Michael S. Swetnam

Chairman and CEO, Potomac Institute for Policy Studies[1]

I opened the session up earlier today with a discussion about how our national security strategy had evolved in this country over the last 40 years—from one of the Cold War era where we had mutually assured destruction and deterrents to protect this country to one of post-Cold War national security strategy where we talked about fighting MRC's around the world.

Today we talk about dealing with the incidents where the United States is called upon to be the world's policeman. We talk about asymmetric threats from state and non-state actors using weapons of mass destruction that include not just chemical, biological, and nuclear, but sometimes cyber tools to attack the population of the United States. Throughout this Seminar, the discussion has focused on the definitions, and I'd like to note in conclusion that we are still having trouble with the definitions of what national security means in this country.

I'd like to revert back to a definition of national security that preceded the Cold War that dates back to George Washington. President Washington defined national security in the United States as putting together a strategy to guarantee the security of, first the population of the United States, and then second the institutions assembled by that population to do the will of that population.

Remember this is a country by the people and for the people. By that definition national security means first protecting the population of the United States. Civil defense is something that was not discussed much today. It is a term ill or little used today. But in fact, an awful lot of today's discussion and an awful lot of what our national security is going back to, is civil defense.

With that, I'd like to make a comment about a chart that I saw twice—first presented by Mr. Vatis of the FBI and then by General Marsh. And it was a chart that showed the spectrum of the threat from national security to local with shared threats in between. This chart defined national security threats as threats to the intelligence community and threats to the defense establishment.

Terrorist threats were shared, and local threats were defined, in this area as well. I would advocate to you today that in fact the full spectrum of threats are national security threats. That an individual hacker penetrating a system and bringing down the power or electrical grid supporting tens of thousands of people is threating the security, and the well-being of those tens of thousands of people, is in fact involved in a national security attack on the United States of America.

1. Remarks on an event on "Cyber-Terrorism and Information Warfare: Threats and Responses" held at the Potomac Institute for Policy Studies in co-sponsorship with the Terrorism Studies Program at the George Washington University on April 16, 1998.

When approached from that standpoint, the issues brought up by Elizabeth Banker earlier are critical to the discussion that we had today. How do we respond to not so much criminal events, but maybe treasonous, national security events by our citizens or others around the world? That is a critical point that I would like to leave the group with. This is a national security issue of as great an importance today, as the nuclear discussion was during the Cold War.

With that final comment from me, I would like to once again introduce Professor Yonah Alexander. And I want to add to some words that were said about Yonah a few minutes ago, some of my own personal thoughts. This man has led the discussion on terrorism and super terrorism for over two decades in this country. We're able to have a discussion at the level we are today because of his efforts and his colleagues' efforts at The George Washington University. It's an honor to be associated with him.

General (Ret.) Alfred Gray

Twenty-Ninth Commandant of the United States Marine Corps; Senior Fellow and Chairman of the Board of Regents, Potomac Institute for Policy Studies

Part 1[2]

The role of the military is most germane to the discussion of combating terrorism. But, in my humble opinion, there is no such thing as only a military role anywhere in the world, for any reason. It has to be a team effort combining all the elements of national power, influence, and capability – whether it is diplomatic, technological, societal, cultural, or whatever. So, I would ask you to keep that in mind because we are mistaken, in my opinion, when we talk about what can be done exclusively by the military. Clearly, in today's environment, there is a distinct need for what many term "inter-agency"-type processes, cooperation, and working together.

It is important to understand that military type of strategy in action, war, civilian type of strategy in action, national security – or really all the above – are interconnected. This complicated type of operation requires beginning with very clear war or conflict aims and we certainly have to consider how we want this to look when we are done. This is not just from the political, military, economic, or cultural standpoints, but from all of these views and others.

We must also have mechanisms that can translate strategic plans into actions.

Today, in this country, we need to do better in this area. We also need to clearly understand that we must be adaptive along the way, because plans and considerations change.

The subject of whether we, in the United States, are liked or not is crucial in many ways. Fundamentally, you want to understand that if the military serves in a nondomestic environment, there are a couple of basic rules we ought to remember. Do not ever do anything that hurts the people you are trying to help. Soldiers and Marines understand this- they do not need too much in the way of legal advice or anything else like that – this is common sense. There are many lawyers involved in operations, and that bothers me.

During the Eisenhower Administration, William Lederer [with Eugene Burdick] wrote a book called *The Ugly American*. He was talking about the way Americans acted and the way we were viewed by other people around the world – for example, in Laos and places like that. And Eisenhower put the word out to the military. He said, "Start learning about cultures and languages, people and how they live, and start looking at the world through their eyes instead of yours." We

2. Edited introductory and concluding remarks from an event on "The Role of the Military in Combating Terrorism" held on December 5, 2014.

did that pretty well for a while, but I sense we may have drifted away from that slightly. I think that cultural understanding is very, very important.

Part 2[3]

From my personal vantage point, we live in a very challenging world with all of these technologies. But in my experience, over time, there have been countermeasures, counter-counter-measures, and smart people – both civilians and warriors – who figure out ways to operate in these kinds of environments. They figure out how to get to the root cause or challenge of a particular technological advantage or to eliminate, or at least neutralize it. I think that we will maintain that capability because internationally, with our friends and allies, we have the education, the academic background, and the technical expertise. And most of all, any military person operating for the right reasons, in any country, will figure out ways to deal with difficult situations. They have in the past and they will in the future.

What concerns me a little is our propensity to tell everybody – or to lay out ahead of time – our plans. I think we ought to be much more secretive and much smarter about this. There is no need to disclose or advertise what we can or will do. Let them worry about it. Let them think about it. We can really reach out collectively, with our friends and allies, to anywhere in the world, or in space, and pretty much do what we want. We ought to think about this in more of a holistic way and stop revealing so much about doing this and doing that. By the way, I have to tell you that I hate this term "boots on the ground." We should never tell anybody whether or not we are going to put people in there to do what has to be done. Let them worry about it. That is my philosophy on that.

Also, we ought to, geopolitically and through our acts, keep the friends and allies we have. We should talk for a moment about Turkey, for example. Turkey has been a US ally for a long time. Their government has recently undergone some changes – they are moving a little bit away from the secularist position that Ataturk laid out – but Turkey has been a good friend and ally. They have been with us at the 11th hour when they had to be and we ought to cherish those kinds of things. I like people with tough hands – I like people that can fight and they certainly can do that. Having been an artillery forward observer supporting the Turkish brigade in Korea, I have personal knowledge of how they fought. And it is difficult. It is difficult for them with the Kurdish situation and with

3. Edited introductory and concluding remarks from event on "Combating Terrorism: Strategic Assessments, the Military's Role, and International Cooperation" held on May 14, 2015.

all of the other things that are going on – and that is just one country. Each country has these types of challenges. Pakistan has good reason to be wary from time to time about certain things that we do and certain ideas that we have.

As an eternal optimist in life, I believe we have to develop an integrative, adaptive strategy that has the buy-in of all our friends and allies. This strategy must be flexible and must be phased over the long haul. Above all, we have to stay with it. There are no silver bullets with terrorism. The "global war on terrorism" is not a good idea because terrorism is a tactic – it is an ideology. You cannot have a war against tactics. So the idea really is, over the long haul, to make terrorism a bad idea for terrorists – so they are not getting anything out of it. Let it wear itself out. There will always be terrorism. There has been terrorism since history was first recorded, and we will have more in the next 50 years. But the idea is to make terrorism worthless.

Professor Don Wallace, Jr.

Chairman, International Law Institute[4]

As it is always the case with Yonah Alexander's panels, they are very rich and this is no exception. And in some sense, there is too much in them because everything is covered and the question is how do you pull it together? Immediately after 9/11, it was critical that we preserve both our security (and I think we have been pretty successful at home), and our liberties (and I think the courts remain very strong).

We should not mince words: we are talking about radical Islamic terrorism. It is a holy war. Of course not for most Muslims. I lived in the Middle East, in Turkey. Most Muslims are perfectly normal people. We are talking about a specific group with religious fervor. In some ways it may be more than an ideology; it is a faith to some of these people. And unquestionably, it has to be coped with.

When we talk about strategy, we think about looking outwards. For me, a real issue is strategy for ourselves. What do we do? We recognize the problem. How do we cope with it? This is a question for us.

Americans certainly are exceptional; we do tend to exaggerate, but that has also been a great strength. A present risk is to go from doing too much, to doing too little. We hear people say we cannot convert the world to democracy. I think that is true, we cannot convert it, but I do not think we should abandon the cause. But I think it is part of America, this drive that we have, maybe not to save the world but to have an influence on it. And I hope we will not give up. For one thing if we abandon our faith, then others are here to push their faith.

So the question is what do we do? We cannot do everything. We must establish priorities. We do not have resources for everything. Yonah Alexander always begins these programs by reminding us of natural catastrophes and man-made catastrophes, and we have seen a lot of natural catastrophes. We can cope to the extent you can cope with these things. But Mother Nature is pretty damn impressive. We have tremendous challenges; we have national ones, we have the challenge of keeping the Seventh Fleet up-to-date.

We have heard so much about the other forms of terrorism: bio, chemical, etc. We have heard that the battle against ISIS goes beyond knocking out Raqqa. As I noted, I have lived in the Middle East and it is reasonably clear to me that for whatever reason, God has created a group of countries that have a lot of difficulty coping in the modern world.

4. Remarks presented at an event on "Al-Qa'ida" held at the International Law Institute on September 11, 2017.

The challenge for us, for our strategy, is how to sort out our priorities. We Americans think we can do everything. I am of that faith. I think America should always be number one. I do not blame America. In fact, I get very annoyed with the people who do blame America. But it is one thing to not blame it and another thing to be realistic about our abilities. Look at our history, which is basically to take it on. Like many battles of General Grant's, put enough soldiers in there, then you win. At the same time we must continue to grow up. We must look at the facts. We must be analytic. We have to be analytic as hell in distinguishing things, and always putting things in perspective. After all the analysis is done, it does not solve the problem. It is what you do with the facts. But you should not abandon facts. So intelligence is crucial.

SELECTED PERSPECTIVES

General Robert T. Marsh

United States Airforce (Ret.)

Former Chairman, President's Commission on Critical Infrastructure Protection[5]

The topic, obviously, is right down the line of what our Commission was concerned about. But obviously, I've interacted with a whole bunch of you in the room here and you've supported our effort and you know quite a bit about it. But I believe some don't. So those of you that know our Commission well, bear with me, please.

But really what we're here to talk about is what I think are one of the great unsung strengths of the nation and that is our critical infrastructures. They are the very life support systems of the country. And yet, as you know, we take them for granted. We fully expect that when we throw the switch, the lights are going to come on. Turn the spigot and pure water will flow. And when we pick up the phone, we'll get a dial tone and you dial 911 and you'll get emergency assistance early on.

And when you go to the ticket counter in the morning, you are pretty sure you can get to any place in the United States before the day is out. We've taken it for granted. However, that's not likely to be ever so. They are less robust than most people believe. And that's what I'd like to discuss in some more detail. Last October, the Commission did conclude a really intensive 15-month effort of the study of the critical infrastructure. And, of course, my perspective arises from serving on that.

Our report does outline a national policy, an implementation strategy, and recommendations that we believe will serve to better protect the infrastructures from both physical and cyber attack. I'll say more about that later and assure their continued operation. And while we have a pretty good understanding, I think all of us, of the physical threats that are facing the critical infrastructures, the really fast pace of technology renders us always one step behind understanding the cyber threats.

And thus we focused and our report focuses mostly on coping with the evolving cyber threat. To, probably not for this group, but to many I try and give them some perspective on how the Commission faced the challenge. Because imagine if you will that we have a widespread power outage occurring in a major city downtown district shutting down, say thousands of businesses. This happened, incidentally, in Auckland, New Zealand, as you know, just a few weeks ago.

Or the Department of Defense computer systems are invaded and compromised. Telecommunications services in a major financial center in New York City and across the East Coast are temporarily

5. A keynote at an event on "Cyber-Terrorism and Information Warfare: Threats and Responses" held at the Potomac Institute for Policy Studies in co-sponsorship with the Terrorism Studies Program at the George Washington University on April 16, 1998.

out of service. The main Air Traffic Control System at a key airport is shut down, delaying air traffic. And the regional 911 emergency system is disabled because someone has spammed out the phone lines with repeat calls.

Well all of this and perhaps more, let's say, in a relatively short period of time. So what do we do when faced with such situations? Who's in charge? Is it natural or unintended? Or is it a concentrated attack? And should detected intrusions and disruptions be reported? And if so, to whom? And recognizing that most of these systems are privately owned and operated, what can and should be government's involvement?

These are some of the questions that the Commission grappled with and questions to which really there are no easy answers. And questions we that our recommendations will help lay the foundation for addressing. As many of you know, critical infrastructures have long been lucrative targets for anyone wanting to attack another country. Our nation relies on its infrastructures for our life support systems, as I view them -- for national security, for overall public welfare and for our economic strength.

So those who would attack the infrastructures would do so to, say, reduce our ability to act in our national security interest or erode confidence in critical services in order to create public unrest, or reduce American economic competitiveness in one way or another. In the Gulf War, as you all well know, disabling Iraq's infrastructure was one of the keys to our success. A lesson noted with much interest by many countries around the world.

The Commission was established by Executive Order in July of 1996, and it truly was a joint government and private sector endeavor. It was charged to develop, as I said, a national policy, an implementation strategy for protecting from both threats and assuring the continued operation. These are the identified eight infrastructures that we were asked by the President to focus on.

And they are considered vital and we are considered vital because their incapacity or destruction would have a debilitating impact on defense and economic security of the nation. The composition of the Commission was unique. We were truly a public/private partnership with a group of 20 outstanding Commissioners from both the public and private sector. Half were executives from the involved departments and agencies in Washington. The other half were executives from infrastructure companies and organizations.

They came into government full-time to work on this Commission. And so they brought industry experience, expertise and perspective to the Commission. All worked full-time on the Commission. Along with a highly competent staff of approximately 50 personnel, and then we had extensive contract support. Our findings, conclusions, and recommendations are very different from what we anticipated and different from what our stakeholders anticipated, I believe.

Many thought that this was a problem that the government could really address and resolve in a few easy steps. But during the past year, we concluded that really protecting our infrastructures is a public and private undertaking that requires a new kind of partnership. And that protecting our infrastructure is going to take time. It's going to require a long-term effort and a new way of thinking. Our approach recognized that most of the infrastructures operate within an existing framework of government policy and regulation.

But they are also privately owned competitive industries. And as such, protection recommendations should not adversely affect their competitive positions. We recognize that any solution would have to be viable in the market place, as well as the public policy arena. Thus, we adopted the following guiding principles. First, we knew this could not just be another big government unilateral effort.

Government must set the example, but it is the owners and operators who are key to success. They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and know best how to respond to disruptions. Second, while we may be undergoing an information revolution, we concluded that utilizing the best ideas and processes from current structures and relationships was the preferred way to respond.

This means building on existing organizations and relationships, as well as promoting voluntary cooperation. Partnership between industry and government will be far more effective than legislation or regulation. Finally, there is a long-term effort which requires continuous improvement. We must take action in practical increments. There is no magic bullet solution and we must aim not only to protect the infrastructures, but to enhance them.

In the past, broad oceans and peaceable neighbors provided all the infrastructure protection we needed. And that changed during the Cold War. Technology made geography less relevant. We became subject to attack by bombs and missiles, but even then, we knew who the enemy was and where the attack would originate. Now computers and electrons change the picture entirely. The capability to seriously disrupt our infrastructures is widely available at relatively little cost.

And this is the new geography on which the Commission focuses efforts. It's a borderless, cyber-geography whose major topographical features are technology and change. So who is the threat? Well, the bad actors, as I like to call them, are those with the capability and intent to do harm. And while we've not found a smoking keyboard, that is, we do not know who has the specifically focus intent to do harm, we do know a lot about the capability to do serious damage to these systems.

And we characterize capability as a combination of skills and tools. Skills that we found even most teenagers have and dangerous tools that are readily available especially on the internet. In short, the

capability to do harm is widespread and growing. The bad actors who use these tools range from the recreational hacker, who thrives on the thrill or challenge of breaking into another's computer, to the national security threat of information warriors intent on achieving strategic advantage.

Common to all threats is the insider. We could spend millions on technology to protect our infrastructures, but a well-placed insider, whether suborned by an enemy or a disgruntled employee acting alone, could render nearly all protection useless. Hence, the special attention we paid to the insider problem in our report. The new arsenal of weapons of mass disruption in the cyber world would include Trojan horses, viruses, bombs and spamming attacks that can be used to alter or steal data or deny service.

And these tools recognize neither borders nor jurisdictions. They can be used anywhere, any time by anyone with the capability, technology, and intent to do harm. And they offer the advantage of anonymity. And when these tools are used, their effects can be magnified by the growing complexity and interdependence of our infrastructures. Such interdependence creates an increased possibility that a rather minor or a routine disturbance can cascade into a regional outage.

Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs. The Commission was faced with a new geography, new tools, and evolving interdependencies. And in light of these new conditions, we examine the respective roles of the private sector and the federal government. We concluded that the private sector has a responsibility to protect itself from the known established threats, such as individual hackers and criminals, and that the federal government has a large responsibility to protect our citizens from terrorists and nation-state attacks. In short, we found that infrastructure protection is a shared responsibility. Specifically, the private sector must take prudent measures to protect itself from commonplace hacker tools. But, it turns out these same tools will likely be used by the terrorist and the information warrior, albeit, for more dangerous purposes.

So when the private sector protects itself against attack from commonplace hackers, they also will be playing a significant role in national security. It follows then, the federal government must assume responsibility for collecting information about the tools, the perpetrators, and their intent from all sources, including the owners and the operators of the infrastructures. And it must share this information with the private sector so that industry can take the necessary protective measures.

In some respects, our most important finding is that adapting to this new age requires thinking differently about infrastructure protection. We are facing a new and different set of national security challenges as we approach the third millennium. Specifically, we found that we have real and serious vulnerabilities and we have that laid out in spades in the classified report and the addendum to those.

Information sharing between the government and industry is the most immediate need. The federal government has an important role in the new alliance. National awareness of infrastructure threat, vulnerability and interdependency issues must be elevated. Responsibility is shared among owners and operators and government. The existing legal framework is imperfectly tuned to deal with cyber threats. Current research and development efforts are inadequate to the task and infrastructure protection requires a focal point in government.

Protecting our infrastructures into the 21st Century requires a greater understanding of their vulnerabilities and decisive actions to reduce them. After 15 months of consultation, research, assessment, and deliberation, the Commission's fundamental conclusion is that waiting for a serious threat to appear is a dangerous strategy. Now is the time to act to protect our future and this action requires a new partnership to address the risk to our nation's infrastructure.

Outreach was a cornerstone of our effort. In fact, our conclusions and recommendations result directly from the conversations and meetings we had with over 6,000 individuals from industry, academia, science, technology, military, and government. We held five public meetings around the country, participated in numerous conferences, hosted simulations, games, focus groups, and workshops and increased awareness of this effort through the media and our web site.

Before outlining the Commission's recommendations, I'd like to tell you where the report is now. Last October, once the report was completed, an inter-agency working group was formed at the request of the National Security Council to examine the report's recommendations, suggest priorities for implementation, and prepare an inter-agency perspective on the report to forward to the President for action. A transition office was formed from several former Commissioners and the Commission staff to support the NSC staff with the implementation planning.

In conjunction with the inter-agency effort, an advisory committee of private sector CEO's prepared its observations concerning the report and circulated them to the NSC and the Principals Committee. The advisory committee, incidentally, will remain intact and continue to provide executive advice to the Principals Committee.

The Commission's recommendations are the products of much research, discussion, and deliberation. They are founded on shared core principles and they are based on fact. They are aimed at improving coordination and establishing roles for infrastructure protection, fostering partnerships among all stakeholders and coordinating diverse interests. The recommendations fall generally into three categories: actions the federal government must take, actions that the owners and operators of the infrastructures must take, and then actions that have to be taken in partnership by both.

During our extensive outreach efforts, we heard time and again that the owners and operators of the infrastructures needed more information about cyber threats. They said that a trusted

environment must be built so that they can freely exchange information with each other and with government without fear of regulation, loss of public confidence, liability, or tarnished reputation.

The Commission's recommendations lay the foundation for creating a new collaborative environment that includes a two-way exchange of information, not more burdensome regulation. Our recommendations focus on protecting proprietary information and ensuring anonymity when necessary; easy legal impediments to information sharing, such as anti-trust provisions and the Freedom of Information Act; and creating information and sharing mechanisms both within industry and between industry and government.

As to other actions the government should take, we recommended specific steps to ensure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles. Some of our recommendations require that federal agencies play a greater role in developing tools, techniques, and methodologies relating to information assurance, such as, federal agencies offering their expertise to encourage owners and operators to develop and adopt security-related standards with the participation of federal and state agencies, industry associations, and standard groups and the law enforcement and intelligence agencies; the National Institutes of Standards and Technology (NIST), among other agencies, expanding the availability of risk assessment services to the private sector and encourage industry and assisting when necessary to develop risk methodologies.

We also recommended that the U.S. Security Policy Board study and recommend how best to protect private sector information on threats and specific vulnerabilities of private sector critical infrastructures. And finally, that the funding for the Nunn-Lugar-Domenici Domestic Preparedness Program be doubled to expand and accelerate, mitigating the effects of weapons of mass destruction attacks, and expanding it to include the cyber threat.

There's been recent progress in this area. Secretary Cohen recently announced a national strategy for providing military expertise to states who are subject to attack involving chemical, biological, or nuclear weapons. And under this plan, you know, the National Guard and Reserve Force Assessment Teams, or ten of them, will be formed to deploy rapidly and provide medical and technical advice to first responders

The key to the success of these initiatives is educating our citizens about the emerging threats and vulnerabilities in the cyber age. We must change the way of thinking about technology and the resulting threats and vulnerabilities. The Commission's recommendations are aimed at all levels of education, from grammar to graduate school and beyond. They include a series of White House conferences to spur new curricula in computer ethics and intellectual property for elementary and secondary schools; a nationwide public awareness campaign, simulations, and roundtable discussions to educate the general public as well as industry and government leaders; grants by the National

Science Foundation to promote graduate level research and teaching of information network security; and partnership among the Department of Education, other federal agencies and industry to develop curricula and market demand for properly trained information security technicians, managers, and administrators.

Infrastructure assurance is a joint responsibility, but the federal government has an unmistakable duty to lead the effort. Clearly, the federal government must lead by example as it exhorts the private sector, and state and local governments to raise the level of security of their systems. The federal government must aggressively propose the tools, practices, and policies required to conduct business in the cyber age. This includes: improving government information security through developing, implementing, and enforcing the best practices and standards, and then conducting certification and measures against those standards; working with industry to expedite efforts for pilot information security and encryption key management programs; elevating and formalizing information assurance as a foreign intelligence priority; recruiting and retaining adequate numbers of law-enforcement personnel with cyber-skills; and conducting a thorough risk assessment of the National Aerospace System and its plan's sole reliance on the global positioning system.

We examined a full range of legal issues relating to protecting the critical infrastructures with three goals in mind: increasing the effectiveness of government's protection efforts, enhancing the private sector's ability to protect itself, and enabling effective public/private partnership where most needed. We propose revision of specific measure federal legislation as it relates to the critical infrastructures and the cyber threat. Examples are the Stafford Act and the Defense Production Act. We have modest recommendations in the area of criminal law and procedure: specifically, the Federal Sentencing Guidelines to take into account the true harm done by attacks on the critical infrastructures. We call for an expert study group representing labor, management, government, and privacy interest to make recommendations for a long-term reform in the employer/employee relationship while balancing security and privacy.

And we recommend easy legal impediments to information sharing, such as anti-trust provision, federal and private liability, and the Freedom of Information Act. Federal research and development efforts are inadequate to meet the challenge of emerging cyber threats. About 250 million dollars is spent by the government each year on infrastructure assurance-related R&D of which 60 percent or most of that, 150 million, is dedicated to information security, the type of work that the NSA does.

There is very little research supporting a national cyber defense. The Commission believes that real time detection, identification, and response tools are urgently needed. And we concluded that market forces are insufficient to drive the private sector R&D required to meet these needs. Thus, we recommend doubling federal research and development funding for infrastructure protection to 500 million dollars for the next five years.

We recommend this funding target such topics as risk management, simulation and modeling, decision support, and early warning and response. While much of the policy-making apparatus for R&D currently exists, there are other arrangements needed to formulize the public/private partnership necessary for infrastructure protection. The Commission report includes recommended arrangements for information sharing and policy formulation.

At the policy-making level, we recommend an office of National Infrastructure Assurance, located within the White House, to serve as the federal government's focal point for infrastructure protection; a National Infrastructure Assurance Council comprised of selected infrastructure CEO's and Cabinet officials to propose policy and advise the President; and an Infrastructure Assurance Support Office to support both the Council and the National Office.

At the operational level, we recommend private sector Infrastructure Assurance Coordinators or Clearinghouses, if you will, as focal points within each industry infrastructure to share information; and Federal Lead Agencies to be designated to promote and assist in establishing the private sector Coordinators; and an Information Sharing and Analysis Center staffed by both private industry and government to receive and share information about infrastructure threats, best practices, and incidents. And we recommend that it be located out in the private sector.

And finally, a warning center designed to provide operational warning whenever possible of an attack on the infrastructures, either physical or cyber, to be located within the FBI. And you may have noticed Ms. Reno announced the set up of this Infrastructure Protection Center in March. Well, just as the risks are shared between the public and the private sectors, so will the solutions be found. Our national and economic security has become a shared responsibility.

One that will require a new kind of partnership between government and industry. One which encourages information-sharing and one which requires the government to lead by example. And I really appreciate all of your interest. We know that we've only laid the foundation for what we hope will be an ongoing dialogue such as this about how to best address this looming problem. And for those of you who would like to read our report, you can download it from our web site, that's www.pccip.gov.

The Honorable Guy Roberts

Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs[6]

I am particularly appreciative of the work that the Potomac Institute does in facilitating discussions – such as this event – to ultimately develop meaningful policy options to help protect our way of life against the scourge of terrorism. As the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense programs, I lead an organization responsible for ensuring the safety, security, and effectiveness of our nuclear deterrent; developing a spectrum of capabilities to protect the lethality of our forces against the myriad of NBC threats they may encounter in the battle space; and ensuring DoD compliance with nuclear, chemical, and biological defense treaties and agreements.

In the short time I have, I would like to share a general overview of the threat landscape, some thoughts about emerging WMD terrorist threats, and the importance of and challenges to our non-proliferation norms – which one would have thought were strong, durable international norms against the use of such weapons by violent extremist organizations and rogue nations, defined as such by their refusal to accept or comply with those legal prescriptions.

WMD Threat Landscape

As I look at the strategic threat landscape, it is no exaggeration to say that America and her allies face the most complex, demanding international security situation since the end of the Cold War, one fraught with old and new dangers. For example, the rise of ISIS, its evident creation of a CBW program and use of sarin and chlorine weapons; North Korea's use of VX nerve agent at an international airport in Malaysia; Russia's assassination of a former member of their Federal Security Service, who had asylum in the United Kingdom, using plutonium-21 O; and the list goes on. The bottom line is that, WMD threats are real, evolving, and have significantly increased from what they were a decade ago.

The variety of threats is no longer a static list of restricted CBRN materials. Driving this revolution is the concurrent emergence of dual-use technologies and increased access to shared information, which is lowering the expertise required to harness these technologies for illicit purposes. The proliferation of technology, increased ease of access, challenges to detecting illicit activity, and our limited ability to anticipate how our adversaries might employ WMD all heighten the risk of unforeseen and un-attributable attacks against the U.S. or its allies.

Further, the sustained use of chemical weapons in the Middle East, and the increasing threat of weapons of mass destruction (WMD) on the Korean Peninsula not only illustrate the reality of threats we face, but also undermine the norms that protect civilians and security forces from these

6. Presentation at an event on "Combating Terrorism: National, Regional, and Global Lessons for the Next Decade and Beyond" held on April 30, 2018 at the National Press Club.

weapons. The reality is, many terrorist groups, including ISIS, al-Qa'ida, and the Nusrah Front, have the resources, intent, skills, and access to potentially acquire these capabilities, and they have publicly expressed their desire and intent to acquire WMD. Their targets are likely to be diverse, including attacks on small groups of individuals, tactical battlefield attacks on U.S. forces and those of our allies', and large-scale attacks with the potential to cause hundreds of injuries or death.

Further, rogue regimes, such as North Korea and Iran, continue to seek out or develop WMDs as well as long-range missile capabilities.

Pyongyang has been committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States. They have also had longstanding biological weapons capability and biotechnology infrastructure that could support a BW program. The intelligence community also assesses that North Korea has a chemical weapons program and the capability to employ these agents by modifying conventional munitions or with unconventional, targeted methods. Meanwhile, Iran's ballistic missile programs give it the potential ability to hold targets at risk across the region.

As we sit here today, the Syrian regime continues to kill its own citizens, aided by the Russian Government. The Assad regime's atrocities in Syria have caused tremendous human suffering, killing hundreds of thousands of people, and driving millions from their homes. Reports continue to emerge that the Assad regime is using chemical weapons to terrorize and kill the Syrian people.

Taking these factors into account, the threat of a terrorist using WMD against the U.S. and its allies beyond the battlefield is the highest it has ever been and will remain so for many years to come. We face powerful adverse trend lines that continue to erode the non-proliferation regimes and continue increasing the likelihood that somehow, some day, somewhere a terrorist group (VEO) will get a nuclear weapon and will explode it to destroy one of our cities – a world changing event to be sure. To make sure that does not happen, we work closely with our allies and partners to intercept and interdict trafficking in the materials to make such weapons to reduce the risk of that happening. But as one of our national lab directors noted: "If you believe it is easy to make an improvised nuclear weapon, you are wrong. But if you believe it is impossible for a terrorist group to make an improvised nuclear bomb, you are dead."

Importantly, the willingness of rivals to abandon aggression will largely depend on their perception of U.S. strength, the vitality of our alliances and partnerships, and our collective resolve to the norms and values we espouse.

In addition to advocating and supporting norms and treaties/conventions to combat the WMD terrorism threat, the readiness of our forces and the resilience of our societies are key. To address these challenges, the Secretary has prioritized rebuilding military readiness to build a more lethal

Joint Force; strengthening alliances to attract new partners; and reforming the Department's business practices for greater performance and affordability to rapidly respond to, among other things, a WMD use or proliferation event.

In support of the Secretary's and the President's goals, NCB's top objective is to dissuade, prevent, or deter state adversaries and VEOs from acquiring, proliferating, or using weapons of mass destruction.

As I look at how we are going to do that in the time ahead, there are a couple of areas of concern that I think require particular collective effort.

Emerging Issues of Concern

Since the 9/11 Commission, which predicted that it would be more likely than not that a nuclear weapon would be used by a terrorist by 2014, successive administrations have identified nuclear terrorism as one of the greatest threats. While certainly a nightmare scenario, I believe that recent advances in biological sciences has made the possibility of a biological event even more probable and nightmarish. In particular, synthetic biology is one of those key concerns.

Synthetic biology is generally defined as the advanced application of engineering principles for biological design and remains a foundational scientific field for chemical and biological defense.

Evolving biotechnologies, most recently the genome editing system known as CRISPR-Cas (clustered, regularly interspaced short palindromic repeats-CRISPR-associated protein), may provide significant advances in diverse technology areas, ranging from medicine to advanced materials. These new opportunities, however, may also pose potential risks that will need to be continually assessed. This is not a new issue. In fact, over the past decade, DoD has been preparing for the possibility of genetically-engineered threat agents by developing defensive countermeasure technologies.

Our Chemical and Biological Defense Program (CBDP) uses the tools of synthetic biology for the research and development of vaccines, therapeutics, diagnostic assays, and chemical and biological detection technologies. Underscoring the need to recognize and characterize emerging or novel threats, we are investing in bioinformatics to analyze DNA sequence data in deployed laboratories. We are also investing in infrastructure, such as our Advanced Development and Manufacturing Facility, which equips the Department with the ability to develop medical countermeasures at scale, on an as needed basis.

To be sure, the power of synthetic biology will be key to the development of innovative and beneficial defense programs of the future. But we must find ways to stop VEOs/terrorists from also taking advantage of these technologies for their nefarious purposes.

Protecting Norms: No Paper Tigeres

Russia's use of military-grade nerve agent in the United Kingdom not only violates the Chemical Weapons Convention (CWC), but brazenly flouts the international norms against the use of chemical weapons.

Indeed, any use of a chemical weapon by a State Party is a violation of the CWC and the international norms and standards that all members of the OPCW promise to uphold.

But Russia's attack validates a more fundamental concern – that the international norm against chemical weapons use is eroding. This is dangerous, and counter to our national vital interests and global stability.

I think Ambassador Ken Ward framed it well in his March statement before the OPCW: he said: "We are at the edge of a precipice where a new normal, a new era of chemical weapons use, is threatening to take hold. It is woefully naive to think that the evil genie of chemical weapons can be contained in the Syrian Arab Republic. Absent concerted international action, this scourge is spreading. It has already found its way to Iraq, Malaysia, and the United Kingdom."

We must deter this kind of war, and that requires us to acknowledge who is culpable for perpetrating such horrendous acts, and holding all individuals or entities involved responsible. We can only do that well together. And that, too, I look forward to hearing your thoughts on.

In closing, I think what brings us together today, is a mutual recognition that WMD threats continue to pose a clear and present danger to our way of life.

Terrorists groups pursue them because they believe doing so will give them significant leverage. Our job is to reduce and eliminate any advantage they may seek to gain, by either making their threats impotent or convincing them of our ability and will to impose costs that will outweigh any benefit they may conceive to gain by using WMD.

Given that our prosperity and global stability are at stake, the importance of modernizing our nuclear deterrent cannot be overstated, nor the value of our investments in developing protective equipment and medical countermeasures for our forces who represent the lethal backstop to our diplomacy.

We cannot afford to be the unready confronting the unthinkable. As we confront the challenges to the international norms we have fought so long and hard to create and nurture, we must also prepare our forces and our citizenry for the nightmare of WMD use. We are doing a lot but much more needs to be done.

Professor Rita Colwell

Distinguished University Professor at the University of Maryland, College Park and the Johns Hopkins University Bloomberg School of Public Health; Senior Fellow at the Potomac Institute[7]

I will confine my discussion to microbiological agents. Biology as a weapon of mass destruction has centuries of history, from the catapulting of a plague ridden carcass, the dead body of a bubonic plague victim, over the walls into castle grounds in Medieval times to the more recent case of a bioterrorist adding enteric bacterial pathogens to a salad bar in an Oregon public restaurant in the United States. We now face a much more sophisticated and frightening, insidious capability of biological weaponry whereby modification of microorganisms normally found in the healthy human body can be engineered to be virulent. Escherichia coli offers an illuminating example of a bacterium common to the healthy human gut that could be modified, perhaps by using CRISPR technology or other genetic engineering methods, for insertion of properties for pathogenicity and dissemination and would, thereby, become a dangerous bioweapon. By the time such modification would be detected, many victims would be in hospitals or, worse, dead.

The anthrax incident that occurred after 9/11 offers an appropriate contemporary example of modern day bioterrorism and has been described in a previous lecture at the Potomac Institute. A report was published with details, but a brief review may be useful. After destruction of the twin towers in 2001, a few months later a reporter in Florida received a letter that contained a powder. He subsequently became seriously ill. Because we did not have rapid methods at the time for detection and identification of microbial pathogens, several weeks passed before it was understood that the cause of his death was a Bacillus anthracis infection. By the time of final diagnosis, the victim had sickened and subsequently died. Other victims also died from anthrax within days of that initial death because powders in envelopes dropped in the mail were dispersed at the Post Office during routine mail processing procedures. Neither the perpetrator nor the community at large knew that the process of machine stamping envelopes in the post office would force powders through the pores of envelopes. Hence, there were deaths of several postal workers in the Washington D.C. Post Office building caused by the aerosol of anthrax powder.

It took approximately six years to amass the evidence needed to track the source of the anthrax. That was accomplished using molecular biology and genomic methods. It was possible to track the source of the anthrax because the Bacillus anthracis bacterium that infected the reporter in Florida has been isolated and grown in a laboratory. Its DNA had been extracted and sequenced so that its genetic composition could be ascertained and the genomic characteristics of anthrax elucidated. Identification was achieved using the science of genomics. Other bioevent strains of anthrax were also sequenced after the initial bioterrorism event, including anthrax bacteria in culture collections

7. Presentation at an event on "Combating Terrorism: National, Regional, and Global Lessons for the Next Decade and Beyond" held on April 30, 2018 at the National Press Club.

and obtained during the process of tracking the source of the anthrax. That is, anthrax bacteria were collected from every laboratory known to maintain the bacterium in their stock collection. A team of scientists from the agencies of the federal government worked together, meeting on a weekly basis for three years and monthly for an additional three years to advise the CIA and FBI in the task of determining the source of this anthrax. From my perspective as chair of the interagency committee that advised the CIA and the FBI during this time, the source of the anthrax was concluded to be a mixture of anthrax suspensions grown in different parts of the country in ultra-containment laboratories and composited for the purpose of providing a potent test culture for candidate vaccines being developed to protect against anthrax. Because mutations had occurred in the various batches of anthrax that had been grown in different laboratories, the composite vaccine test cultures allowed definitive determination of the origin of the material distributed as a bioweapon.

Subsequently, since 2001, many laboratories – including the University of Maryland, University of California at San Francisco, and others – have been working to develop rapid detection methods using DNA extracted from any sample, whether soil, water, or clinical material sequencing the DNA, and analyzing the sequences obtained employing bioinformatics. By analyzing DNA sequences, accurate identification and characterization of all pathogens present in a given sample can be determined, providing the ability to track the source with elegant accuracy and precision.

It took approximately six years to obtain sufficient evidence for the FBI to provide a sufficiently strong case to arrest the perpetrator. Unfortunately, we will never know all circumstances of this anthrax event because on the day of his arrest the suspected perpetrator committed suicide. But it should be noted that it did take six years to amass the needed evidence to make the arrest. The new techniques available today allow identification within a day or two and soon it will be possible to make accurate identification within minutes. Once the sequence is established, whatever the sample, within ten or twenty minutes, algorithms, and relatively soon artificial intelligence implemented algorithms, will allow accurate identification and characterization of an agent, its pathogenic properties, antibiotic resistance, and unique metabolic characteristics. We now have powerful tools that enable detection, identification, and forensic action.

What is important to understand is that a biological threat may have an origin of multiple possibilities, a rogue nation, an individual terrorist, or Mother Nature alone. The latter represents a wide source of pathogens from all areas of the world, including remote regions of Africa, Asia, and Latin America where humans have not previously inhabited. These represent emerging threats and terrorism derived from such natural sources must be understood because it represents a serious and continuing threat to society. We may be facing a future epidemic of massive proportions, as occurred with influenza in 1918, because, as humans, Mother Nature harbors microorganisms, whether bacteria, viruses, fungi, or parasites, to which we have not yet been exposed and these can be dangerous to human health. It is important to understand also that the potential, as mentioned

by our previous speaker, of genetically engineered microorganisms, whether bacteria or viruses, that are naturally benign but able to be rendered pathogenic or whose pathogenicity can be enhanced, perhaps by integrating genes for antibiotic resistance or enhancing invasive properties, are biological threats, both natural and manmade, against which we must be prepared.

There are organizations that define hotspots of potential emerging disease threats, an excellent example is the EcoHealth Alliance, located in New York City and funded by several federal agencies. The EcoHealth teams were instrumental in detecting the agent of SARS and were able to determine its source. Similarly their studies defined the agent of camel pox outbreaks. Identifying potential hotspots, namely those areas of the world where as yet unrecognized threats exist, allows characterization and prevention of massive epidemics.

Antibiotic resistance represents perhaps the most serious threat within the microbiological sphere. The number of deaths each year caused by antibiotic resistant microorganisms is greater than the number of deaths from food and water-borne diseases combined. Misuse of antibiotics is a factor in the rise of antibiotic resistance, by which we may be creating our own public health catastrophe, ironically.

It is important that we be proactive, not solely reactive, to the potential of biothreats. Determining hotspots of emerging infectious diseases and identification of potential new agents allows building vaccines and constructing preventive measures methodically that is constructive and definitive, as opposed to delaying and facing the prospect of victims for which protection would be lacking.

The most difficult aspect of a bio-threat is that a perpetrator, especially of a rogue nation, creates one set of complexities and a lone terrorist or lone actor another. The latter can be extremely difficult to identify because, as has been pointed out by our previous speaker, an expensive or elaborate laboratory may not be required to acquire or construct a biothreat agent. With a small amount of money, perhaps less than a few hundred dollars, an individual could obtain a culture of a pathogenic agent like anthrax and create a serious public threat, not only for those victims who become infected, but also for the public at large in ancillary economic and security costs.

The simple but important message is that a serious biological threat is a continuous concern that requires attention and should not be ignored until the threat occurs. We need to prepare for the potentiality by assuring that our public health laboratories are fully functioning and have the capacity to mobilize rapidly in the event of a biothreat incident. An informed citizenry is also protection against bioterrorism by being able to react appropriately, effectively, and rapidly.

In conclusion, while there may exist the threat of biological events, at the same time, we are gaining important new knowledge about the microbial world that exists in ourselves and around us. By

far, our normal microbial constituents are highly protective, those microorganisms in our gut, on our skin, in our respiratory passages, and in the world around us. They are our protection against disease and comprise a healthy compositional array of microorganisms serving as a bio-protective shield. Our gut carries our personally characteristic ecological composition and, depending on the region of the world in which we live, whether Asia, Europe, or the United States, we carry within and on ourselves a characteristic microbial flora. These comprise our identifier and at the same time represent a bioforensics tool. It is important not to emphasize only negative aspects of our microbial world, but to make clear we are just beginning to learn how about our microbiological world is highly protective of us, serving as a front line of defense against threat agents.

Carl Gershman

President of the National Endowment for Democracy; formerly, Senior Counselor to the United States Representative to the United Nations[8]

I have been asked to talk about the relationship between terrorism and democracy. I want to begin by noting that around the time of 9/11, the conventional wisdom that was expressed by U.S. Attorney General John Ashcroft in Senate testimony after 9/11 was that terrorists "…exploit our openness." He mentioned a captured al-Qa'ida training manual and warning that "terrorists are told how to use America's freedom as a weapon against us."

The National Endowment for Democracy, that I run, publishes the Journal of Democracy which in January 2018 ran an article by Amichai Magen challenging this assumption that democracy's openness makes it vulnerable to terrorism. Magen is an Israeli political scientist at the International Institute for Counter-Terrorism in Herzliya. His article entitled "Fighting Terrorism: The Democracy Advantage," used data from the Global Terrorism Database to show that over the past decade, higher-quality liberal democracies have experienced fewer terrorist attacks than all other regime types, and that there have also been fewer fatalities connected with these attacks. He calls this the "democracy advantage."

I think that Assistant Secretary Roberts touched on this when he talked about the resilience of our societies and the readiness of our forces. These are the reasons given by Magen to explain the so-called "Democracy Advantage."

Political openness, according to Magen, and the protection of civil liberties allow grievances to be peacefully and publicly expressed and redressed. Responsiveness to citizens' desire for physical safety also generates higher rates of life-saving investments in intelligence, infrastructure protection, first responders, social resilience, and specialized medical care. These measures reduce incidences of terrorist assaults and make them less deadly when they occur. Magen goes so far in his article to say that against the background of a surge in global terrorism, "…a consolidated, high-quality democracy is increasingly proving to be the best counter-terrorism organization known to humanity." That is quite a remarkable statement.

Magen cites the work of the economist Alberto Abadie who believes that the incidence of terrorism is explained more by the level of political freedom than poverty. In an essay in 2006 in the American Economic Review, Abadie wrote that the relationship of regime type to terrorism takes the form of an inverted U because "countries with intermediate levels of political freedom [are]

8. Presentation at an event on "Combating Terrorism: National, Regional, and Global Lessons for the Next Decade and Beyond" held on April 30, 2018 at the National Press Club.

more prone to terrorism than countries with high levels of political freedom or countries with highly authoritarian regimes." The reasoning is that intermediate regimes, such as electoral and minimalist democracies, are the most vulnerable because they lack what Magen calls "the grievance-assuaging and cooptation capacity" of liberal democracies as well as "the brutal, no-holds barred crackdown abilities of hardened autocracies."

But statistics that Magen cites from the GTD over the 2002-2016 period do not back up this thesis. They do show that higher quality democracies were less prone to terrorist attacks than all other regime types, and that intermediate regimes showed a far higher rate of increase in such attacks. Yet the greatest absolute rise in the number of terrorist attacks occurred in the more repressive regimes that the survey calls "multiparty autocracies" and "closed autocracies." The multiparty dictatorships were more vulnerable, according to Magen, because they "provide greater political space within which terrorists and their ideological and financial supporters can organize and mobilize, yet lack the avenues for meaningful political access and expression that even bare-bones democracies have. Whatever opportunities for political contestation do exist in multiparty autocracies amount to a sham, and are therefore ineffective in assuaging grievances and countering extremists' claims to legitimacy."

Significantly, the GTD data also show that the greatest percentage increase in terrorist attacks occurred in closed autocracies, the most illiberal and repressive category in the survey. This seems to be for two reasons, according to Magen. First, advanced communications technologies have made it easier for terrorists to generate and exploit strategic opportunities that exist in closed systems. And second, smartphones and social media have made it more difficult for autocratic regimes to hide terrorist incidents and have thus undermined the illusion inherited from an earlier time that dictatorships are less vulnerable to terrorism.

Egypt is an example of an authoritarian regime that is failing in its efforts to counter terrorism. An article last February in The Washington Post by two Egyptian-American human rights activists – one of them Aya Hijazi who became famous when President Trump intervened to secure her release from prison in Egypt – notes that:

> Sisi's counterterrorism policies, which serve as an important justification of his dictatorship, have created a fertile ground for radicalization. The authors of this article witnessed this firsthand during the collective 60 months we spent in prison between 2013 and 2017. We watched the process of radicalization unfold as recruiters for the Islamic State, while jailed themselves, appealed to innocent young prisoners who were facing unjust detainment, harsh sentences, and inhumane conditions. Sisi's heavy-handed crackdown has thus actually contributed to an increased Islamic State presence in Egypt.

A study by the Tahrir Institute for Middle East Policy has found that over Sisi's time in office, despite extensive military and police operations, terror groups are becoming more established and attacks still continuing regularly.

Not least, in an article recently published by the Atlantic Council, Yussef Auf, an Egyptian judge, criticizes the harmful effect of the emergency law now in effect in Egypt. "All doors," he writes, "are closed before any opposition and political activism. This is, indeed, a primary factor for the increasing rates of violence and extremism."

Because security forces in Egypt are focused on preserving the regime, they target nonviolent political opponents as much as, or perhaps even more than, militant groups. This means that civil society and dissenting political groups do not have the space to operate, expand their influence, and develop politically and organizationally. Thus, if and when another political opening comes, as it did in 2011, the democrats committed to nonviolence will not be organized and ready to compete politically. As a result, there will be the same kind of destructive polarization that existed after the Tahrir Square uprising between the Islamists and the autocrats.

Democracy does not just blossom automatically when dictators fall. If democrats and civil society activists are repressed, atomized, and helpless, they cannot fill the political vacuum that is created when a dictatorship falls. That is why it is in the interest of fighting terrorism to pressure the Sisi regime to allow space for nonviolent groups to function and grow.

Tunisia offers a different and more hopeful example. In an accompanying article to the Magen piece in the Journal of Democracy, Geoffrey Macdonald and Luke Waggoner warned that while Tunisia has been a political success story, the failure to address corruption, unemployment, and inadequate social services dashed hopes for progress that were engendered by the Jasmine Revolution. According to Macdonald and Waggoner, the resulting disillusionment inflamed grievance-driven radicalism and led thousands of young Tunisians to join ISIS in Syria and Iraq. The authors concluded that if a democratic political transition is not accompanied by an economic and social transformation, it could actually heighten the threat of terrorism.

But the flawed start in Tunisia was not the end of the story there because the democratic process is on-going and gives people the opportunity for self-correction. The next phase of strengthening Tunisian democracy will take place on May 6 with the holding of municipal elections, which is an important milestone in Tunisia's progress towards local governance and decentralization. These elections will give civil society and ordinary citizens unprecedented opportunities to participate and to make their voices heard. It is especially encouraging that 52% of the candidates for local office are under the age of 35. This strong participation shows that young Tunisians are embracing democracy's possibilities for reform and inclusion. Hopefully, this will counter the appeal of the extremists and make it possible for Tunisia to begin to reap the benefits of "the democracy advantage."

Professor Marvin Kalb

Edward R. Murrow Professor Emeritus at Harvard University's Kennedy School of Government, senior advisor to the Pulitzer Center on Crisis Reporting, and nonresident senior fellow at the Brookings Institution[9]

Thank you very much, Yonah, delighted to be with our fellow panelists, and thank you all for showing up. I am here essentially to talk about the media and terrorism. How you cover it is one aspect of it, but I want to talk about it in a more philosophical way and try to draw a distinction between the way two civilizations approach an understanding of news, of fact, of opinion.

I want to go back to the Russian Revolution. When Lenin took over, one of the first things he did was to say that the means of communication were to be in the direct control of the communist party. There is to be no democratizing of the idea of information. Information was to be a weapon. It was to be used by the party in order to advance a particular point of view. And that has been the case, certainly from 1917 to 1991, and since that time it has been back and forth. While it is not absolutely clear about the degree of the freedom of the press that exists in Russia today, I would argue that there is probably less of it than there is freedom of the press. Lenin idea was there was to be no romance when it comes to information. It was a weapon of political warfare. And that has been the way it has been seen not only by Lenin but by people who have lived in closed societies. People, generally terrorists, who have a particular point of view which they wish to impose on a society do that by terrorizing people. Lenin said at the very beginning the definition of terror is to terrorize – that is the point of the operation. And you use what to terrorize? You use information, if that is helpful in your cause.

And I remember clearly the first time I arrived in Russia in January of 1956, I rather quickly and oddly made friends with a reporter who worked for Pravda who had a wonderful sense of humor. He told me very quickly, which I knew, that the Russian word for truth was Pravda, and there was no truth in Pravda. Then he pointed out that the other major newspaper was Izvestia, which means news, but there is no news in Izvestia. And the whole point of it was up until this very day that terrorist use information to advance a political cause. And there are, as I said before, civilizational definitions here.

For me, as someone who has been in this line of work for a long time, I can say with total honesty and total belief that in the American way in which journalism is viewed, journalism is not an instrument of warfare. It is not supposed to be. It is supposed to be a way in communicating information as best as you can get it to the American people and the American people benefit from it, from that information. Something as simple as "what is the weather going to be?" you can get it from a weather forecast and that is part of the news.

9. Presentation at an event on "Combating Terrorism: National, Regional, and Global Lessons for the Next Decade and Beyond" held on April 30, 2018 at the National Press Club.

But if you begin to think of the news as a weapon then it has to be used in a certain way. And I can remember easily in the coverage of wars, for example, I never assumed that a bullet if it was shot at me would ever hit me. I assumed that the bullet was smart enough to understand that I am a reporter and I am only there to cover the news. So if it comes this way it then goes around and out the other way. And what is interesting to me is that I think up until recent decades, even the people who use journalism to advance their own political ends did understand the value and the importance of a free press, not for them but also for the opposition. And they would treat reporters, most of the time, with respect and would understand what it is that the reporter is there to do.

Today, reporters are seen by people who live by a terrorist understanding of the world as a warrior. Somebody who is involved either in helping your cause or in hurting your cause. And if the judgement be that the reporter is hurting your cause then it is in our interest to kill the reporter. In the war in Syria, for example, reporters have not only been kidnapped, they have been beheaded. What was the point of that? The point of that was to be able to show the beheading of a free press, of a reporter from the West, of the West itself with the reporter being a symbol of that and put it out as part of your propaganda. So, the reporter then could not expect the bullet to go around him. The reporter now expects to be part of a war. And if the reporter is part of the war then this has to do as well with the way in which the reporter is seen by, for the example, the U.S. government or governments in the Western world. If, as we heard this afternoon, the threat is there – and there is no doubt it is – and if we are to meet that threat, would it not make sense to try to advance your interest by using the press in a more intelligent way?

The press is not the enemy of freedom, it is the symbol of freedom, in my judgement. And if freedom is to be maintained, and I am sure we all argue that it should be, what is the best way of doing it?

If all the American people, people all over the world today, walk around with their iPhones and everything, and we are part of a revolution and in that revolution, the bad guy get it; I am not sure that we do. I have a feeling that the U.S. government still regards the press with just enough suspicion to put them on the other side of the line rather than on this side of the line. And I would love to be proven wrong. And to be shown time and time again that the press is one of the greats not only symbols of democracy but an asset in the function of a democratic system.

I think that, in closing, the press ought to be playing a more central role in educating the American people on the dangers of terrorism. And not only think about it in a ten-year framework but this is going to go on for a long time. It is very much part of our lives even now and will be even more so. We ought to be a little smarter about understanding it.

Ambassador (ret.) Ronald E. Neumann

Deputy Assistant Secretary of State (ret.) and U.S. Ambassador to Algeria, Bahrain, and Afghanistan; President, American Academy of Diplomacy[10]

Thank you. I am not sure that my book really connects with today's subject very well, except for a lifetime of experience, I suppose. It was an autobiography and it talks a lot about what diplomacy is. It is called *Three Embassies, Four Wars*, which were Vietnam, Algeria, where I was ambassador during very bloody years in the 90s, Iraq, where I spent sixteen months before becoming ambassador in Afghanistan, and that was the fourth war. There's a certain amount of experience with terrorism covered in that book, but that's all I am going to say about the book.

Terrorism is a tactic, it's not a goal of the perpetrators. Unless it is pure anarchism or someone goes on a shooting episode, and we don't usually define that as terrorism, although if you happen to be in the middle of one it is pretty terrifying. Terrorism as we talk about it in political terms usually has a goal of a political purpose. Frankly, outsiders, and we tend to be outsiders to almost every conflict which generates terrorism, actually have a very poor record of ever being able to resolve those conflicts. Usually they have to be resolved by other people. And through experience we know that terrorism tends to go on for a very long time. It has been around the world for quite a while in different guises, and I expect that will continue.

The other sad part about terrorism is it almost never achieves anything. It kills a lot of people and it almost never produces the final result that terrorists desire, a political result. It produces casualties in large numbers, but very rarely changes the course of events. Except for occasionally a lucky shot, like the fellow who shot Archduke Franz Ferdinand in 1914, and kicked off an entire world war. I guess you would have to say that that was a successful terrorist operation, in political terms.

The other thing about terrorism is that military tactics do not solve terrorism. They are highly necessary for protecting us and they are highly necessary in coping with terrorism. They do not solve anything. Only when you have an insurgency that is put down and loses militarily can you find examples of where military means alone resolve terrorism. Sri Lanka had a lot of terrorism and it finally had a very bloody and messy conclusion of its Tamil revolt. You could say that is a military solution. Other than that, there have been very few military solutions.

It is also worth noting that right now, the majority of terrorism we have to worry about is terrorism that comes out of Islamic jihadi movements. But it is good to remember that that has not always been the case. You had terrorism from anarchists, from communists in previous periods, terrorism from insurgent groups whose ends were all political, and these were not religious and they were not based on Islam. It is good to remember that not all terrorism comes from religious differences.

10. Presentation at an event on "The Role of Diplomacy in Combating Terrorism: Past Lessons and Future Outlook" held on July 25, 2018 at the International Law Institute.

When you look at recent experience, one of the things you see is that our experience in the recent big wars like Iraq and Afghanistan, where we have dealt with terrorism, is actually not very good. We have won lots of tactical victories but have not done too well, although I still think we have a chance in Afghanistan. But we have been at wars with terrorism being part of that war, even if it is not the driving force, for quite some time. When you look around and you ask, where do we have a better record of dealing with combinations of insurgencies and terrorism? It's Bosnia, Kosovo, Uganda against the Lord's Resistance Army. And the point there is simply how tied together counterterrorism and diplomacy are. They are not alternatives. They are separate tools that you use for the same problem, just as you might hold something with a wrench and turn it with a screwdriver. You need both pieces. And diplomacy is in fact not separable from the military instrument, it is an essential foundation.

On the simplest level, diplomacy is an enabler. Military operations require overflight authority, they require landing, they require refueling, they require fuel for the ships and the planes, and transit authorities. All of those things are negotiated by the way of diplomats, so without those authorities the military grinds to a halt. That is the simple level of enabling the military.

The more complex level is that diplomacy is an essential part of creating the strategies to deal with terrorism because the answers are often political. And that's a pretty simple truth but it is one of our weakest points in the United States, our recurring inability to combine our military and political tools. We treat them as alternatives, we give separate goals to the military. Civilians do not read mission statements that are written by the military, so if they happen to get the political piece of the mission statement wrong, we will not know about it. We do not have mission statements so they will not know if we understand what we are doing. But when you do not tie these things together, they do not work very well.

For example, we have done very well destroying at least the physical part of the Islamic State. We are not very close to security in Syria, we seem to be close to pulling out. We had a goal at one point of seeing Assad gone, that is now completely gone. The people we have armed have largely been defeated. And we now have the problem of Russians and Iranians. We are making a lot of noise about it but we are not sure of what we are going to do about it. But a lot of the tools that we could have used for that were during the military period but we did not integrate the military operation with political goals. The military operation was given a military goal, to destroy ISIS. There was nothing wrong with that goal. The problem was that it was not nested in any larger, political purpose. You ended up with a very messy situation.

In Iraq, the one piece of dealing with ISIS, we could have held back a little bit with some of our application of force. This would have been in order to the push the components of the Iraqi government, Arabs, Kurds, Sunnis, Shias, to work out in advance some of their issues, like how to govern

Mosul. We spent a lot of time, the whole military operation, driving for the taking of Mosul. Mosul is a divided city, it is half Kurdish and half Sunni. You could guarantee that you were going to have problems governing it after you took it back with. You had the same problem governing it before the battle, before our military was a critical piece. We could have, at that point, maybe said wait a minute, we are not quite going to go forward with this. You guys have to work out a solution on how you are going to govern afterwards. It is not ours to work out.

We have a lot of leverage to push people to get reasonable when they need our backing for a battle. Once the battle is over, they do not need us. They may soon be asking us to go home. Political leverage is not a constant and it is not just because you have troops on the ground, it is the political situation that surrounds the troops that creates leverage. We need to bring these things together and we do this terribly.

For instance, at what point does the chain of command between the civilians and the military come together in a single decision maker? The President of the United States. There is no point in our entire structure below the President of the United States where one person is in charge of what we are doing in the field. There are certainly places where it works very well. I had very good relations with General Eikenberry when I was with Afghanistan. General Sanchez had horrible relations with Ambassador Bremer in one case. I have seen it go both ways. But the important point of the discussion is that we leave it entirely to personalities. We have no integrated structure to put our diplomats and military together in some regular, normal way. We have a lot of good examples and we have some horribly bad examples.

I do not know of a situation where cabinet department disciplines its own person when the two in the field do not get along. Cabinet departments almost universally support their own. The only person who can tell the commanding general and the ambassador to play nice is the President of the United States. He is usually busy! This illustrates the need for an integrated structure or some delegation of authority. I wrote an article once with former Director of National Intelligence Admiral Dennis Blair and former Head of Special Forces Admiral Eric Olson. We recommended, among other things, a much stronger role for ambassadors in the field and carrying out operations in certain fragile states. I think nobody need worry that this is going to happen but it was amusing to produce the article with one retired diplomat and two retired flag officers.

There are a lot of people who recognize the need but we have not done anything about it. We have situations with terrorism which are historic and we are likely to deal with it for a very long time. The particular piece of the phenomenon we are in of Islamic jihad is not a function of the Muslim world at large. Until it burns itself out somehow within Muslim societies, it is not going away. It is probably not going away in your lifetime. Therefore, we do need tactics and strategies and policies to deal with as many pieces of the phenomenon as we can. That is going to require that we look at

the things that Ambassador Ray was talking about. We must understand cultures, something which tends to be more the diplomat's function than the military's. It also means that as we develop the strategies based on that understanding that the pieces work together and the military and the civilian piece come together in much more integrated structures, in more formal chains of command, and with some form of accountability to a single rather than a separate source within our bureaucracies. Those are very large needs and they have been there for the last twenty years or even longer, but they are still there today. Once some of you have gotten your degrees and are giving these lectures, they still may be there then, but I hope not.

Ambassador (ret.) Charles Ray

US Ambassador to Cambodia and Zimbabwe; Deputy Assistant Secretary of Defense for POW/Missing Personnel Affairs[11]

With all of the other international crises of late, it's easy to forget that international terrorism and violent extremism is still a significant security threat – indeed, for many people in many places, an existential threat.

While we're preoccupied with rogue nuclear programs, the threat of a global trade war, and decidedly unsettled global climate conditions—all of which are, in fact, existential threats—extremist groups continue to pursue their radical agendas on multiple fronts.

Even if our defense and security forces weren't occupied with other priorities, even if those other crises should suddenly disappear, these forces are ill-equipped to deal with such a complex threat alone.

Before those who are part of the defense establishment rise up in righteous indignation, allow me to make one thing crystal clear. This is not a negative assessment of our defense capability. I believe that we have the most capable military in the world, and as a veteran of 20 years of military service, and a student of history, I think I know what I'm talking about.

There is no military force on the planet that is a match for us when it comes to doing the things we were organized and trained to do.

But, let's be real. The threats posed by extremist groups don't fall into neat categories that lend themselves to kinetic solutions. You don't use a sledge hammer to hang wallpaper.

So, having stipulated that the threat is complex and multi-faceted, what is the appropriate solution?

The answer is deceptively simple; the solution, less so.

First, borrowing from the military, we need to analyze the problem. The approach I recommend is one that I use when plotting and writing my mystery novels, which I call 'chunking.' Chunking, as I apply it, is breaking a complex situation (or plot) into its component parts, determining what tools (or methods) are most appropriate for each part, and then using those tools or methods in coordination with each other to solve the problem – chunk by chunk.

11. Presentation at an event on "The Role of Diplomacy in Combating Terrorism: Past Lessons and Future Outlook" held on July 25, 2018 at the International Law Institute.

The tool I wish to address here is the soft power of diplomacy.

Many people, when you say diplomacy, have in mind an image of people spending a lot of time talking, thinking, and analyzing. How, you might ask, does that contribute to solving the problem of terrorism?

I recall a phrase from my days as a young lieutenant; 'Know Your Enemy.' Back then, it was mostly confined to tactical order of battle; the number of guns, tanks, and men, and the capability of that combination to inflict damage on our forces. But, when dealing with shadowy extremist groups, our forces need to know much more.'

Of course, they still need to know the numbers, because on occasion, a kinetic solution is called for. But killing one terrorist or destroying or neutralizing a cell or even a large terrorist formation, is a short-term fix that fails to address the larger problem.

Terrorism is much more than the terrorists who commit heinous acts. We need to develop methods and courses of action to address the issues underlying the motivations for extremism and getting the information we need to do that effectively is outside the competence of our military forces.

Here are just a few of the issues that need to be addressed:

1. What factors motivate individual terrorists and extremist organizations?

2. How are these organizations funded and supported?

3. How, where, and who do they recruit?

4. What is the ultimate objective of the organization?

Diplomats are often immersed in the very societies from which terrorist groups originate and are best positioned to get the answers to these and other questions. They should also be part of the discussions about the courses of action to address the problems.

No nation, no matter how powerful, can deal with the complex challenge of terrorism alone. We need allies willing to cooperate with us on all fronts to address not just the acts of terrorism, but the underlying causes, if we are to effectively neutralize or destroy these organizations. Diplomats, skilled in conducting international negotiations, are the best tool to develop these alliances.

Even in cases where it's been determined that a kinetic response to a terrorist group is the best course of action, there is a role for diplomacy. When we deploy military forces against a terrorist organization, in addition to the usual order of battle, we need to equip them with more if they are to prevail. Those forces need to understand the cultural and political environment in which the terrorist operates, the extent of local support for or opposition to the terrorists, and what non-military problems they are likely to encounter as they carry out their military mission.

I witnessed an example of this during my time as a consultant to the US Army, helping prepare units for deployment to areas where they faced situations short of open warfare. In one exercise, the training objective was to secure an American diplomatic facility prior to evacuation of American citizens from the area. A group of soldiers at the entrance of the facility were keeping back a crowd of locals who were clamoring to be included in the evacuation, when a local militia group, ostensibly our allies, approached the crowd and grabbed an individual who they proceeded to threaten. The man was made to kneel, in full view of the American soldiers, and a gun was put to his head. The objective of this part of the exercise was to force the soldiers to consider a situation that was not part of their original rules of engagement—a decidedly non-military wrinkle in the operation. Without going into further detail, this is just an example of what our forces are likely to encounter in operations against unconventional extremist groups, and if we don't prepare them adequately in advance, the end result is likely to be catastrophic, and dangerous for them.

I could go on, but I hope that you get the point.

The problems we face when dealing with terrorist organizations are complex and multi-dimensional, requiring complex, interagency solutions. Each situation our forces face is unique, but most still have a common thread, and it's often not remotely military.

A master carpenter's tool kit never has only one tool, but a variety of tools which can be applied to whatever situation that arises. We need to make sure that our tool kit for dealing with terrorism has all of the tools needed, and be prepared to use them as appropriate.

Academic Centers

Inter-University Center for Terrorism Studies (IUCTS)

Established in 1994, the activities of IUCTS are guided by an International Research Council that offers recommendations for study on different aspects of terrorism, both conventional and unconventional. IUCTS is cooperating academically with universities and think tanks in over 40 countries, as well as with governmental, intergovernmental, and nongovernmental bodies.

International Center for Terrorism Studies (ICTS)

Established in 1998 by the Potomac Institute for Policy Studies, in Arlington, VA, ICTS administers IUCTS activities and sponsors an internship program in terrorism studies.

Inter-University Center for Legal Studies (IUCLS)

Established in 1999 and located at the International Law Institute in Washington, D.C., IUCLS conducts seminars and research on legal aspects of terrorism and administers training for law students.

Summer and Fall 2018 Internship Program

Talia Andreottola	American University	David Matvey	Carnegie Mellon University	Linda Rauch	University at Albany, SUNY
Jesse Berman	University of Virginia	Dante Moreno	George Washington University	Lauren Sasseville	College of William and Mary
John Keblish	University of Pennsylvania	Emily Nestler	College at Brockport, SUNY	David Silverman	George Washington Universit
Catie Ladas	University of Maryland	Robin O'Luanaigh	University of North Carolina	Johnathan Trent	Loyola University Chicago
		Lavanya Rajpal	Georgetown University		

Please contact the Inter-University Center for Terrorism Studies at the Potomac Insitute for Policy Studies, 901 North Stuart Street, Suite 200, Arlington, VA 22203.
Tel.:703-525-0770 Email: yalexander@potomacinstitute.org, ICTS@potomacinstitute.org