International Terrorism

Ivan Langley

INTERNATIONAL TERRORISM

INTERNATIONAL TERRORISM

Ivan Langley

BIBLIOTEX
Digital Library

International Terrorism
by Ivan Langley

Copyright© 2022 BIBLIOTEX

www.bibliotex.com

All rights reserved. No part of this book may be reproduced or used in any manner without the prior written permission of the copyright owner, except for the use brief quotations in a book review.

To request permissions, contact the publisher at info@bibliotex.com

Ebook ISBN: 9781984662491

Published by:
Bibliotex
Canada
Website: www.bibliotex.com

Contents

Chapter 1

Introduction

Terrorism

Terrorism is, in the broadest sense, the unlawful use of intentional violence to achieve political aims, especially against civilians. It is used in this regard primarily to refer to violence during peacetime or in the context of war against non-combatants (mostly civilians and neutral military personnel). The terms "terrorist" and "terrorism" originated during the French Revolution of the late 18th century but became widely used internationally and gained worldwide attention in the 1970s during the conflicts of Northern Ireland, the Basque Country, and the Israeli–Palestinian conflict. The increased use of suicide attacks from the 1980s onwards was typified by the September 11 attacks in New York City, Arlington and Pennsylvania in 2001.

There are various different definitions of terrorism, with no universal agreement about it. Terrorism is a charged term. It is often used with the connotation of something that is "morally wrong". Governments and non-state groups use the term to abuse or denounce opposing groups. Varied political organizations have been accused of using terrorism to achieve their objectives. These include right-wing and left-wing political organizations, nationalist groups, religious groups, revolutionaries and ruling governments. Legislation declaring terrorism a crime has been

adopted in many states. When terrorism is perpetrated by nation states, it is not considered terrorism by the state conducting it, making legality a largely grey-area issue. There is no consensus as to whether terrorism should be regarded as a war crime.

The Global Terrorism Database, maintained by the University of Maryland, College Park, has recorded more than 61,000 incidents of non-state terrorism, resulting in at least 140,000 deaths, between 2000 and 2014.

Etymologically, the word terror is derived from the Latin verb *Tersere*, which later becomes *Terrere*. The latter form appears in European languages as early as the 12th century; its first known use in French is the word *terrible* in 1160. By 1356 the word *terreur* is in use. *Terreur* is the origin of the Middle English term *terrour*, which later becomes the modern word "terror". The term *terroriste*, meaning "terrorist", is first used in 1794 by the French philosopher François-Noël Babeuf, who denounces Maximilien Robespierre's Jacobin regime as a dictatorship. In the years leading up to what became known as the Reign of Terror, the Brunswick Manifesto threatened Paris with an "exemplary, never to be forgotten vengeance: the city would be subjected to military punishment and total destruction" if the royal family was harmed, but this only increased the Revolution's will to abolish the monarchy. Some writers attitudes about French Revolution grew less favorable after the French monarchy was abolished in 1792. During the Reign of Terror, which began in July 1793 and lasted thirteen months, Paris was governed by the Committee of

Public safety who oversaw a regime of mass executions and public purges.

Prior to the French Revolution, ancient philosophers wrote about tyrannicide, as tyranny was seen as the greatest political threat to Greco-Roman civilization. Medieval philosophers were similarly occupied with the concept of tyranny, though the analysis of some theologians like Thomas Aquinas drew a distinction between usurpers, who could be killed by anyone, and legitimate rulers who abused their power—the latter, in Aquinas' view, could only be punished by a public authority. John of Salisbury was the first medieval Christian scholar to defend tyrannicide.

Most scholars today trace the origins of the modern tactic of terrorism to the Jewish Sicarii Zealots who attacked Romans and Jews in 1st-century Palestine. They follow its development from the Persian Order of Assassins through to 19th-century anarchists. The "Reign of Terror" is usually regarded as an issue of etymology. The term terrorism has generally been used to describe violence by non-state actors rather than government violence since the 19th-century Anarchist Movement.

In December 1795, Edmund Burke used the word "Terrorists" in a description of the new French government called 'Directory':

At length, after a terrible struggle, the [Directory] Troops prevailed over the Citizens... To secure them further, they have a strong corps of irregulars, ready armed. Thousands of those Hell-hounds called **Terrorists**, whom they had shut up in Prison on

their last Revolution, as the Satellites of Tyranny, are let loose on the people.(emphasis added)

The terms "terrorism" and "terrorist" gained renewed currency in the 1970s as a result of the Israeli–Palestinian conflict, the Northern Ireland conflict, the Basque conflict, and the operations of groups such as the Red Army Faction. Leila Khaled was described as a terrorist in a 1970 issue of *Life* magazine. A number of books on terrorism were published in the 1970s. The topic came further to the fore after the 1983 Beirut barracks bombings and again after the 2001 September 11 attacks and the 2002 Bali bombings.

In 2006 it was estimated that there were over 109 different definitions of terrorism. American political philosopher Michael Walzer in 2002 wrote: "Terrorism is the deliberate killing of innocent people, at random, to spread fear through a whole population and force the hand of its political leaders". Bruce Hoffman, an American scholar, has noted that it is not only individual agencies within the same governmental apparatus that cannot agree on a single definition of terrorism. Experts and other long-established scholars in the field are equally incapable of reaching a consensus.

C. A. J. Coady has written that the question of how to define terrorism is "irresolvable" because "its natural home is in polemical, ideological and propagandist contexts".

Experts disagree about "whether terrorism is wrong by definition or just wrong as a matter of fact; they disagree about whether

terrorism should be defined in terms of its aims, or its methods, or both, or neither; they disagree about whether states can perpetrate terrorism; they even disagree about the importance or otherwise of *terror* for a definition of *terrorism*."

State terrorism refers to acts of terrorism conducted by a state against its own citizens or against another state. In November 2004, a Secretary-General of the United Nations report described terrorism as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act". The international community has been slow to formulate a universally agreed, legally binding definition of this crime. These difficulties arise from the fact that the term "terrorism" is politically and emotionally charged. In this regard, Angus Martyn, briefing the Australian parliament, stated,

The international community has never succeeded in developing an accepted comprehensive definition of terrorism. During the 1970s and 1980s, the United Nations attempts to define the term floundered mainly due to differences of opinion between various members about the use of violence in the context of conflicts over national liberation and self-determination.

These divergences have made it impossible for the United Nations to conclude a Comprehensive Convention on International Terrorism that incorporates a single, all-encompassing, legally binding, criminal law definition of terrorism. The international

community has adopted a series of sectoral conventions that define and criminalize various types of terrorist activities.

Since 1994, the United Nations General Assembly has repeatedly condemned terrorist acts using the following political description of terrorism:

Criminal acts intended or calculated to provoke a state of terror in the public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.

Various legal systems and government agencies use different definitions of terrorism in their national legislation.

U.S. Code Title 22 Section 2656f(d) defines terrorism as: "Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents".

18 U.S.C. § 2331 defines "international terrorism" and "domestic terrorism" for purposes of Chapter 113B of the Code, entitled "Terrorism":

"International terrorism" means activities with the following three characteristics:

Involve violent acts or acts dangerous to human life that violate federal or state law;

Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.

A definition proposed by Carsten Bockstette at the George C. Marshall European Center for Security Studies, underlines the psychological and tactical aspects of terrorism:

Terrorism is defined as political violence in an asymmetrical conflict that is designed to induce terror and psychic fear (sometimes indiscriminate) through the violent victimization and destruction of noncombatant targets (sometimes iconic symbols). Such acts are meant to send a message from an illicit clandestine organization. The purpose of terrorism is to exploit the media in order to achieve maximum attainable publicity as an amplifying force multiplier in order to influence the targeted audience(s) in order to reach short- and midterm political goals and/or desired long-term end states.

Terrorists attack national symbols, which may negatively affect a government, while increasing the prestige of the given terrorist group or its ideology.

Political violence

Terrorist acts frequently have a political purpose. Some official, governmental definitions of terrorism use the criterion of the illegitimacy or unlawfulness of the act. to distinguish between actions authorized by a government (and thus "lawful") and those of other actors, including individuals and small groups. For example, carrying out a strategic bombing on an enemy city, which is designed to affect civilian support for a cause, would not be considered terrorism if it were authorized by a government. This criterion is inherently problematic and is not universally accepted, because: it denies the existence of state terrorism. An associated term is violent non-state actor.

According to Ali Khan, the distinction lies ultimately in a political judgment. Having the moral charge in our vocabulary of 'something morally wrong', the term 'terrorism' is often used to abuse or denounce opposite parties, either governments or non-state groups.

Those labeled "terrorists" by their opponents rarely identify themselves as such, and typically use other terms or terms specific to their situation, such as separatist, freedom fighter, liberator, revolutionary, vigilante, militant, paramilitary, guerrilla, rebel, patriot, or any similar-meaning word in other

languages and cultures. Jihadi, mujahideen, and fedayeen are similar Arabic words that have entered the English lexicon. It is common for both parties in a conflict to describe each other as terrorists.

On whether particular terrorist acts, such as killing non-combatants, can be justified as the lesser evil in a particular circumstance, philosophers have expressed different views: while, according to David Rodin, utilitarian philosophers can (in theory) conceive of cases in which the evil of terrorism is outweighed by the good that could not be achieved in a less morally costly way, in practice the "harmful effects of undermining the convention of non-combatant immunity is thought to outweigh the goods that may be achieved by particular acts of terrorism". Among the non-utilitarian philosophers, Michael Walzer argued that terrorism can be morally justified in only one specific case: when "a nation or community faces the extreme threat of complete destruction and the only way it can preserve itself is by intentionally targeting non-combatants, then it is morally entitled to do so".

In his book *Inside Terrorism* Bruce Hoffman offered an explanation of why the term *terrorism* becomes distorted:

On one point, at least, everyone agrees: *terrorism* is a pejorative term. It is a word with intrinsically negative connotations that is generally applied to one's enemies and opponents, or to those with whom one disagrees and would otherwise prefer to ignore. 'What is called terrorism,' Brian Jenkins has written, 'thus seems to depend on one's point of view. Use of the term implies a moral

judgment; and if one party can successfully attach the label *terrorist* to its opponent, then it has indirectly persuaded others to adopt its moral viewpoint.' Hence the decision to call someone or label some organization *terrorist* becomes almost unavoidably subjective, depending largely on whether one sympathizes with or opposes the person/group/cause concerned. If one identifies with the victim of the violence, for example, then the act is terrorism. If, however, one identifies with the perpetrator, the violent act is regarded in a more sympathetic, if not positive (or, at the worst, an ambivalent) light; and it is not terrorism.

The pejorative connotations of the word can be summed up in the aphorism, "One man's terrorist is another man's freedom fighter". This is exemplified when a group using irregular military methods is an ally of a state against a mutual enemy, but later falls out with the state and starts to use those methods against its former ally. During the Second World War, the Malayan People's Anti-Japanese Army were allied with the British, but during the Malayan Emergency, members of its successor organisation (the Malayan Races Liberation Army) started campaigns against them, and were branded "terrorists" as a result. More recently, Ronald Reagan and others in the American administration frequently called the mujaheddin "freedom fighters" during the Soviet–Afghan War yet twenty years later, when a new generation of Afghan men were fighting against what they perceive to be a regime installed by foreign powers, their attacks were labelled "terrorism" by George W. Bush. Groups accused of terrorism understandably prefer terms reflecting legitimate military or ideological action. Leading terrorism

researcher Professor Martin Rudner, director of the Canadian Centre of Intelligence and Security Studies at Ottawa's Carleton University, defines "terrorist acts" as unlawful attacks for political or other ideological goals, and said:

There is the famous statement: 'One man's terrorist is another man's freedom fighter.' But that is grossly misleading. It assesses the validity of the cause when terrorism is an act. One can have a perfectly beautiful cause and yet if one commits terrorist acts, it is terrorism regardless.

Some groups, when involved in a "liberation" struggle, have been called "terrorists" by the Western governments or media. Later, these same persons, as leaders of the liberated nations, are called "statesmen" by similar organizations. Two examples of this phenomenon are the Nobel Peace Prize laureates Menachem Begin and Nelson Mandela. WikiLeaks editor Julian Assange has been called a "terrorist" by Sarah Palin and Joe Biden.

Sometimes, states that are close allies, for reasons of history, culture and politics, can disagree over whether members of a certain organization are terrorists. For instance, for many years, some branches of the United States government refused to label members of the Provisional Irish Republican Army (IRA) as terrorists while the IRA was using methods against one of the United States' closest allies (the United Kingdom) that the UK branded as terrorism. This was highlighted by the *Quinn v. Robinson* case. Media outlets who wish to convey impartiality may limit their usage of "terrorist" and "terrorism" because they are

loosely defined, potentially controversial in nature, and subjective terms. Depending on how broadly the term is defined, the roots and practice of terrorism can be traced at least to the 1st century AD. Sicarii Zealots, though some dispute whether the group, a radical offshoot of the Zealots which was active in Judaea Province at the beginning of the 1st century AD, was in fact terrorist. According to the contemporary Jewish-Roman historian Josephus, after the Zealotry rebellion against Roman rule in Judea, when some prominent Jewish collaborators with Roman rule were killed, Judas of Galilee formed a small and more extreme offshoot of the Zealots, the Sicarii, in 6 AD. Their terror was directed against Jewish "collaborators", including temple priests, Sadducees, Herodians, and other wealthy elites.

The term "terrorism" itself was originally used to describe the actions of the Jacobin Club during the "Reign of Terror" in the French Revolution. "Terror is nothing other than justice, prompt, severe, inflexible", said Jacobin leader Maximilien Robespierre. In 1795, Edmund Burke denounced the Jacobins for letting "thousands of those hell-hounds called Terrorists... loose on the people" of France.

In January 1858, Italian patriot Felice Orsini threw three bombs in an attempt to assassinate French Emperor Napoleon III. Eight bystanders were killed and 142 injured. The incident played a crucial role as an inspiration for the development of the early terrorist groups. Arguably the first organization to utilize modern terrorist techniques was the Irish Republican Brotherhood, founded in 1858 as a revolutionary Irish nationalist group that

carried out attacks in England. The group initiated the Fenian dynamite campaign in 1881, one of the first modern terror campaigns. Instead of earlier forms of terrorism based on political assassination, this campaign used timed explosives with the express aim of sowing fear in the very heart of metropolitan Britain, in order to achieve political gains.

Another early terrorist group was Narodnaya Volya, founded in Russia in 1878 as a revolutionary anarchist group inspired by Sergei Nechayev and "propaganda by the deed" theorist Carlo Pisacane. The group developed ideas—such as targeted killing of the 'leaders of oppression'—that were to become the hallmark of subsequent violence by small non-state groups, and they were convinced that the developing technologies of the age—such as the invention of dynamite, which they were the first anarchist group to make widespread use of—enabled them to strike directly and with discrimination.

David Rapoport refers to four major waves of global terrorism: "the Anarchist, the Anti-Colonial, the New Left, and the Religious. The first three have been completed and lasted around 40 years; the fourth is now in its third decade."

In early 1975, the Law Enforcement Assistant Administration in the United States formed the National Advisory Committee on Criminal Justice Standards and Goals. One of the five volumes that the committee wrote was titled *Disorders and Terrorism*, produced by the Task Force on Disorders and Terrorism under the direction of H. H. A. Cooper, Director of the Task Force staff.

The Task Force defines terrorism as "a tactic or technique by means of which a violent act or the threat thereof is used for the prime purpose of creating overwhelming fear for coercive purposes". It classified disorders and terrorism into six categories:

Civil disorder – A form of collective violence interfering with the peace, security, and normal functioning of the community.

Political terrorism – Violent criminal behaviour designed primarily to generate fear in the community, or substantial segment of it, for political purposes.

Non-Political terrorism – Terrorism that is not aimed at political purposes but which exhibits "conscious design to create and maintain a high degree of fear for coercive purposes, but the end is individual or collective gain rather than the achievement of a political objective".

Anonymous terrorism – In the two decades prior to 2016-19, "fewer than half" of all terrorist attacks were either "claimed by their perpetrators or convincingly attributed by governments to specific terrorist groups". A number of theory have been advanced as to why this has happened.

Quasi-terrorism – The activities incidental to the commission of crimes of violence that are similar in form and method to genuine terrorism but which nevertheless lack its essential ingredient. It is not the main purpose of the quasi-terrorists to induce terror in the immediate victim as in the case of genuine terrorism, but the

quasi-terrorist uses the modalities and techniques of the genuine terrorist and produces similar consequences and reaction. For example, the fleeing felon who takes hostages is a quasi-terrorist, whose methods are similar to those of the genuine terrorist but whose purposes are quite different.

Limited political terrorism – Genuine political terrorism is characterized by a revolutionary approach; limited political terrorism refers to "acts of terrorism which are committed for ideological or political motives but which are not part of a concerted campaign to capture control of the state".

Official or state terrorism – "referring to nations whose rule is based upon fear and oppression that reach similar to terrorism or such proportions". It may be referred to as **Structural Terrorism** defined broadly as terrorist acts carried out by governments in pursuit of political objectives, often as part of their foreign policy.

Other sources have defined the typology of terrorism in different ways, for example, broadly classifying it into **domestic terrorism** and **international terrorism**, or using categories such as vigilante terrorism or insurgent terrorism. One way the typology of terrorism may be defined:

Political terrorism

Sub-state terrorism

- Social revolutionary terrorism
- Nationalist-separatist terrorism
- Religious extremist terrorism
- Religious fundamentalist Terrorism
- New religions terrorism
- Right-wing terrorism
- Left-wing terrorism
- Communist terrorism
- State-sponsored terrorism
- Regime or state terrorism
- Criminal terrorism
- Pathological terrorism

Causes and motivations

Individuals and groups choose terrorism as a tactic because it can:

Act as a form of asymmetric warfare in order to directly force a government to agree to demands

Intimidate a group of people into capitulating to the demands in order to avoid future injury

Get attention and thus political support for a cause

Directly inspire more people to the cause (such as revolutionary acts) – propaganda of the deed

Indirectly inspire more people to the cause by provoking a hostile response or over-reaction from enemies to the cause

Attacks on "collaborators" are used to intimidate people from cooperating with the state in order to undermine state control. This strategy was used in Ireland, in Kenya, in Algeria and in Cyprus during their independence struggles.

Stated motives for the September 11 attacks included inspiring more fighters to join the cause of repelling the United States from Muslim countries with a successful high-profile attack. The attacks prompted some criticism from domestic and international observers regarding perceived injustices in U.S. foreign policy that provoked the attacks, but the larger practical effect was that the United States government declared a War on Terror that resulted in substantial military engagements in several Muslim-majority countries. Various commentators have inferred that al-Qaeda expected a military response, and welcomed it as a provocation that would result in more Muslims fight the United States. Some commentators believe that the resulting anger and suspicion directed toward innocent Muslims living in Western countries and the indignities inflicted upon them by security forces and the general public also contributes to radicalization of new recruits. Despite criticism that the Iraqi government had no involvement with the September 11 attacks, Bush declared the

2003 invasion of Iraq to be part of the War on Terror. The resulting backlash and instability enabled the rise of Islamic State of Iraq and the Levant and the temporary creation of an Islamic caliphate holding territory in Iraq and Syria, until ISIL lost its territory through military defeats.

Attacks used to draw international attention to struggles that are otherwise unreported have included the Palestinian airplane hijackings in 1970 and the 1975 Dutch train hostage crisis.

Causes motivating terrorism

Specific political or social causes have included:

- Independence or separatist movements
- Irredentist movements

Adoption of a particular political philosophy, such as socialism (left-wing terrorism), anarchism, or fascism (possibly through a coup or as an ideology of an independence or separatist movement)

- Environmental protection (ecoterrorism)
- Supremacism of a particular group

Preventing a rival group from sharing or occupying a particular territory (such as by discouraging immigration or encouraging flight)

Subjugation of a particular population (such as lynching of African Americans)

Spread or dominance of a particular religion – religious terrorism

Ending perceived government oppression

Responding to a violent act (for example, tit-for-tat attacks in the Israeli–Palestinian conflict, in The Troubles in Northern Ireland, or Timothy McVeigh's revenge for the Waco siege and Ruby Ridge incident)

Causes for right-wing terrorism have included white nationalism, ethnonationalism, fascism, anti-socialism, the anti-abortion movement, and tax resistance.

Sometimes terrorists on the same side fight for different reasons. For example, in the Chechen–Russian conflict secular Chechens using terrorist tactics fighting for national independence are allied with radical Islamist terrorists who have arrived from other countries.

Personal and social factors

Various personal and social factors may influence the personal choice of whether to join a terrorist group or attempt an act of terror, including:

Identity, including affiliation with a particular culture, ethnicity, or religion

Previous exposure to violence

Financial reward (for example, the Palestinian Authority Martyrs Fund)

Mental health disorder

Social isolation

Perception that the cause responds to a profound injustice or indignity

A report conducted by Paul Gill, John Horgan and Paige Deckert found that for "lone wolf" terrorists:

43% were motivated by religious beliefs

32% had pre-existing mental health disorders, while many more are found to have mental health problems upon arrest

At least 37% lived alone at the time of their event planning and/or execution, a further 26% lived with others, and no data were available for the remaining cases

40% were unemployed at the time of their arrest or terrorist event

19% subjectively experienced being disrespected by others

14% percent experienced being the victim of verbal or physical assault

Ariel Merari, a psychologist who has studied the psychological profiles of suicide terrorists since 1983 through media reports that contained biographical details, interviews with the suicides' families, and interviews with jailed would-be suicide attackers, concluded that they were unlikely to be psychologically abnormal. In comparison to economic theories of criminal behaviour, Scott Atran found that suicide terrorists exhibit none of the socially dysfunctional attributes—such as fatherless, friendless, jobless situations—or suicidal symptoms. By which he means, they do not kill themselves simply out of hopelessness or a sense of 'having nothing to lose'. Abrahm suggests that terrorist organizations do not select terrorism for its political effectiveness. Individual terrorists tend to be motivated more by a desire for social solidarity with other members of their organization than by political platforms or strategic objectives, which are often murky and undefined.

Michael Mousseau shows possible relationships between the type of economy within a country and ideology associated with terrorism. Many terrorists have a history of domestic violence.

Democracy and domestic terrorism

Terrorism is most common in nations with intermediate political freedom, and it is least common in the most democratic nations. Some examples of "terrorism" in non-democratic nations include ETA in Spain under Francisco Franco (although the group's terrorist activities increased sharply after Franco's death), the Organization of Ukrainian Nationalists in pre-war Poland, the

Shining Path in Peru under Alberto Fujimori, the Kurdistan Workers Party when Turkey was ruled by military leaders and the ANC in South Africa. Democracies, such as Japan, the United Kingdom, the United States, Israel, Indonesia, India, Spain, Germany, Italy and the Philippines, have experienced domestic terrorism.

While a democratic nation espousing civil liberties may claim a sense of higher moral ground than other regimes, an act of terrorism within such a state may cause a dilemma: whether to maintain its civil liberties and thus risk being perceived as ineffective in dealing with the problem; or alternatively to restrict its civil liberties and thus risk delegitimizing its claim of supporting civil liberties. For this reason, homegrown terrorism has started to be seen as a greater threat, as stated by former CIA Director Michael Hayden. This dilemma, some social theorists would conclude, may very well play into the initial plans of the acting terrorist(s); namely, to delegitimize the state and cause a systematic shift towards anarchy via the accumulation of negative sentiments towards the state system.

Religious terrorism

According to the Global Terrorism Index by the University of Maryland, College Park, religious extremism has overtaken national separatism and become the main driver of terrorist attacks around the world. Since 9/11 there has been a five-fold increase in deaths from terrorist attacks. The majority of incidents over the past several years can be tied to groups with a

religious agenda. Before 2000, it was nationalist separatist terrorist organizations such as the IRA and Chechen rebels who were behind the most attacks. The number of incidents from nationalist separatist groups has remained relatively stable in the years since while religious extremism has grown. The prevalence of Islamist groups in Iraq, Afghanistan, Pakistan, Nigeria and Syria is the main driver behind these trends.

Four of the terrorist groups that have been most active since 2001 are Boko Haram, Al Qaeda, the Taliban and ISIL. These groups have been most active in Iraq, Afghanistan, Pakistan, Nigeria and Syria. Eighty percent of all deaths from terrorism occurred in one of these five countries. In 2015 four Islamic extremist groups were responsible for 74% of all deaths from Islamic terrorism: ISIS, Boko Haram, the Taliban, and al-Qaeda, according to the Global Terrorism Index 2016. Since approximately 2000, these incidents have occurred on a global scale, affecting not only Muslim-majority states in Africa and Asia, but also states with non-Muslim majority such as United States, United Kingdom, France, Germany, Spain, Belgium, Sweden, Russia, Australia, Canada, Sri Lanka, Israel, China, India and Philippines. Such attacks have targeted both Muslims and non-Muslims, however the majority affect Muslims themselves.

Terrorism in Pakistan has become a great problem. From the summer of 2007 until late 2009, more than 1,500 people were killed in suicide and other attacks on civilians for reasons attributed to a number of causes—sectarian violence between

Sunni and Shia Muslims; easy availability of guns and explosives; the existence of a "Kalashnikov culture"; an influx of ideologically driven Muslims based in or near Pakistan, who originated from various nations around the world and the subsequent war against the pro-Soviet Afghans in the 1980s which blew back into Pakistan; the presence of Islamist insurgent groups and forces such as the Taliban and Lashkar-e-Taiba. On July 2, 2013 in Lahore, 50 Muslim scholars of the Sunni Ittehad Council (SIC) issued a collective fatwa against suicide bombings, the killing of innocent people, bomb attacks, and targeted killings declaring them as Haraam or forbidden.

In 2015, the Southern Poverty Law Center released a report on terrorism in the United States. The report (titled *The Age of the Wolf*) found that during that period, "more people have been killed in America by non-Islamic domestic terrorists than jihadists." The "virulent racist and anti-semitic" ideology of the ultra-right wing Christian Identity movement is usually accompanied by anti-government sentiments. Adherents of Christian Identity are not connected with specific Christian denominations, and they believe that whites of European descent can be traced back to the "Lost Tribes of Israel" and many consider Jews to be the Satanic offspring of Eve and the Serpent. This group has committed hate crimes, bombings and other acts of terrorism. Its influence ranges from the Ku Klux Klan and neo-Nazi groups to the anti-government militia and sovereign citizen movements. Christian Identity's origins can be traced back to Anglo-Israelism, which held the view that the British people were descendants of ancient Israelites. However, in the United States,

the ideology started to become rife with anti-Semitism, and eventually Christian Identity theology diverged from the philo-semitic Anglo-Israelism, and developed what is known as the "two seed" theory. According to the two-seed theory, the Jewish people are descended from Cain and the serpent (not from Shem). The white European seedline is descended from the "lost tribes" of Israel. They hold themselves to "God's laws", not to "man's laws", and they do not feel bound to a government that they consider run by Jews and the New World Order. The Ku Klux Klan is widely denounced by Christian denominations.

Israel has had problems with Jewish religious terrorism even before independence in 1948. During British mandate over Palestine, the Irgun were among the Zionist groups labelled as terrorist organisations by the British authorities and United Nations, for violent terror attacks against Britons and Arabs. Another extremist group, the Lehi, openly declared its members as "terrorists". Historian William Cleveland stated many Jews justified any action, even terrorism, taken in the cause of the creation of a Jewish state. In 1995, Yigal Amir assassinated Israeli Prime Minister Yitzhak Rabin. For Amir, killing Rabin was an exemplary act that symbolized the fight against an illegitimate government that was prepared to cede Jewish Holy Land to the Palestinians.

The perpetrators of acts of terrorism can be individuals, groups, or states. According to some definitions, clandestine or semi-clandestine state actors may carry out terrorist acts outside the framework of a state of war. The most common image of terrorism

is that it is carried out by small and secretive cells, highly motivated to serve a particular cause and many of the most deadly operations in recent times, such as the September 11 attacks, the London underground bombing, 2008 Mumbai attacks and the 2002 Bali bombing were planned and carried out by a close clique, composed of close friends, family members and other strong social networks. These groups benefited from the free flow of information and efficient telecommunications to succeed where others had failed.

Over the years, much research has been conducted to distill a terrorist profile to explain these individuals' actions through their psychology and socio-economic circumstances. Others, like Roderick Hindery, have sought to discern profiles in the propaganda tactics used by terrorists. Some security organizations designate these groups as *violent non-state actors*. A 2007 study by economist Alan B. Krueger found that terrorists were less likely to come from an impoverished background (28 percent versus 33 percent) and more likely to have at least a high-school education (47 percent versus 38 percent). Another analysis found only 16 percent of terrorists came from impoverished families, versus 30 percent of male Palestinians, and over 60 percent had gone beyond high school, versus 15 percent of the populace.A study into the poverty-stricken conditions and whether terrorists are more likely to come from here,show that people who grew up in these situations tend to show aggression and frustration towards others. This theory is largely debated for the simple fact that just because one is frustrated,does not make them a potential terrorist.

To avoid detection, a terrorist will look, dress, and behave normally until executing the assigned mission. Some claim that attempts to profile terrorists based on personality, physical, or sociological traits are not useful. The physical and behavioral description of the terrorist could describe almost any normal person. the majority of terrorist attacks are carried out by military age men, aged 16 to 40.

Groups not part of the state apparatus of in opposition to the state are most commonly referred to as a "terrorist" in the media.

According to the Global Terrorism Database, the most active terrorist group in the period 1970 to 2010 was Shining Path (with 4,517 attacks), followed by Farabundo Marti National Liberation Front (FMLN), Irish Republican Army (IRA), Basque Fatherland and Freedom (ETA), Revolutionary Armed Forces of Colombia (FARC), Taliban, Liberation Tigers of Tamil Eelam, New People's Army, National Liberation Army of Colombia (ELN), and Kurdistan Workers Party (PKK).

A state can sponsor terrorism by funding or harboring a terrorist group. Opinions as to which acts of violence by states consist of state-sponsored terrorism vary widely. When states provide funding for groups considered by some to be terrorist, they rarely acknowledge them as such. As with "terrorism" the concept of "state terrorism" is controversial. The Chairman of the United Nations Counter-Terrorism Committee has stated that the committee was conscious of 12 international conventions on the subject, and none of them referred to state terrorism, which was

not an international legal concept. If states abused their power, they should be judged against international conventions dealing with war crimes, international human rights law, and international humanitarian law. Former United Nations Secretary-General Kofi Annan has said that it is "time to set aside debates on so-called 'state terrorism'. The use of force by states is already thoroughly regulated under international law". he made clear that, "regardless of the differences between governments on the question of the definition of terrorism, what is clear and what we can all agree on is that any deliberate attack on innocent civilians [or non-combatants], regardless of one's cause, is unacceptable and fits into the definition of terrorism."

USS Arizona (BB-39) burning during the Japanese surprise attack on Pearl Harbor, December 7, 1941.

State terrorism has been used to refer to terrorist acts committed by governmental agents or forces. This involves the use of state resources employed by a state's foreign policies, such as using its military to directly perform acts of terrorism. Professor of Political Science Michael Stohl cites the examples that include the German bombing of London, the Japanese bombing of Pearl Harbor, the Allied firebombing of Dresden, and the U.S. atomic bombings of Hiroshima and Nagasaki during World War II. He argues that "the use of terror tactics is common in international relations and the state has been and remains a more likely employer of terrorism within the international system than insurgents." He cites the first strike option as an example of the

"terror of coercive diplomacy" as a form of this, which holds the world hostage with the implied threat of using nuclear weapons in "crisis management" and he argues that the institutionalized form of terrorism has occurred as a result of changes that took place following World War II. In this analysis, state terrorism exhibited as a form of foreign policy was shaped by the presence and use of weapons of mass destruction, and the legitimizing of such violent behavior led to an increasingly accepted form of this behavior by the state.

Charles Stewart Parnell described William Ewart Gladstone's Irish Coercion Act as terrorism in his "no-Rent manifesto" in 1881, during the Irish Land War. The concept is used to describe political repressions by governments against their own civilian populations with the purpose of inciting fear. For example, taking and executing civilian hostages or extrajudicial elimination campaigns are commonly considered "terror" or terrorism, for example during the Red Terror or the Great Terror. Such actions are often described as democide or genocide, which have been argued to be equivalent to state terrorism. Empirical studies on this have found that democracies have little democide. Western democracies, including the United States, have supported state terrorism and mass killings, with some examples being the Indonesian mass killings of 1965–66 and Operation Condor.

The connection between terrorism and tourism has been widely studied since the Luxor massacre in Egypt. In the 1970s, the targets of terrorists were politicians and chiefs of police while now, international tourists and visitors are selected as the main

targets of attacks. The attacks on the World Trade Center and the Pentagon on September 11, 2001, were the symbolic center, which marked a new epoch in the use of civil transport against the main power of the planet. From this event onwards, the spaces of leisure that characterized the pride of West, were conceived as dangerous and frightful. Terrorist attacks are often targeted to maximize fear and publicity, most frequently using explosives. Terrorist groups usually methodically plan attacks in advance, and may train participants, plant undercover agents, and raise money from supporters or through organized crime. Communications occur through modern telecommunications, or through old-fashioned methods such as couriers. There is concern about terrorist attacks employing weapons of mass destruction. Some academics have argued that while it is often assumed terrorism is intended to spread fear, this is not necessarily true, with fear instead being a by-product of the terrorist's actions, while their intentions may be to avenge fallen comrades or destroy their perceived enemies.

Terrorism is a form of asymmetric warfare, and is more common when direct conventional warfare will not be effective because opposing forces vary greatly in power. Yuval Harari argues that the peacefulness of modern states makes them paradoxically more vulnerable to terrorism than pre-modern states. Harari argues that because modern states have committed themselves to reducing political violence to almost zero, terrorists can, by creating political violence, threaten the very foundations of the legitimacy of the modern state. This is in contrast to pre-modern states, where violence was a routine and recognised aspect of

politics at all levels, making political violence unremarkable. Terrorism thus shocks the population of a modern state far more than a pre-modern one and consequently the state is forced to overreact in an excessive, costly and spectacular manner, which is often what the terrorists desire.

The type of people terrorists will target is dependent upon the ideology of the terrorists. A terrorist's ideology will create a class of "legitimate targets" who are deemed as its enemies and who are permitted to be targeted. This ideology will also allow the terrorists to place the blame on the victim, who is viewed as being responsible for the violence in the first place.

The context in which terrorist tactics are used is often a large-scale, unresolved political conflict. The type of conflict varies widely; historical examples include:

- Secession of a territory to form a new sovereign state or become part of a different state
- Dominance of territory or resources by various ethnic groups
- Imposition of a particular form of government
- Economic deprivation of a population
- Opposition to a domestic government or occupying army
- Religious fanaticism
- Responses to terrorism are broad in scope. They can include re-alignments of the political spectrum and reassessments of fundamental values.

Specific types of responses include:

- Targeted laws, criminal procedures, deportations, and enhanced police powers
- Target hardening, such as locking doors or adding traffic barriers
- Preemptive or reactive military action
- Increased intelligence and surveillance activities
- Preemptive humanitarian activities
- More permissive interrogation and detention policies
- The term "counter-terrorism" has a narrower connotation, implying that it is directed at terrorist actors.

Terrorism research, also called terrorism studies, or terrorism and counter-terrorism research, is an interdisciplinary academic field which seeks to understand the causes of terrorism, how to prevent it as well as its impact in the broadest sense. Terrorism research can be carried out in both military and civilian contexts, for example by research centres such as the British Centre for the Study of Terrorism and Political Violence, the Norwegian Centre for Violence and Traumatic Stress Studies, and the International Centre for Counter-Terrorism (ICCT). There are several academic journals devoted to the field, including *Perspectives on Terrorism*.

International agreements

One of the agreements that promote the international legal anti-terror framework is the Code of Conduct Towards Achieving a World Free of Terrorism that was adopted at the 73rd session of the United Nations General Assembly in 2018. The Code of Conduct was initiated by Kazakhstan President Nursultan Nazarbayev. Its main goal is to implement a wide range of international commitments to counter terrorism and establish a broad global coalition towards achieving a world free of terrorism by 2045. The Code was signed by more than 70 countries. According to a report by Dana Priest and William M. Arkin in The Washington Post, "Some 1,271 government organizations and 1,931 private companies work on programs related to counterterrorism, homeland security and intelligence in about 10,000 locations across the United States."

America's thinking on how to defeat radical Islamists is split along two very different schools of thought. Republicans, typically follow what is known as the Bush Doctrine, advocate the military model of taking the fight to the enemy and seeking to democratize the Middle East. Democrats, by contrast, generally propose the law enforcement model of better cooperation with nations and more security at home. In the introduction of the *U.S. Army / Marine Corps Counterinsurgency Field Manual*, Sarah Sewall states the need for "U.S. forces to make securing the civilian, rather than destroying the enemy, their top priority. The civilian population is the center of gravity—the deciding factor in the struggle.... Civilian deaths create an extended family of

enemies—new insurgent recruits or informants—and erode support of the host nation." Sewall sums up the book's key points on how to win this battle: "Sometimes, the more you protect your force, the less secure you may be.... Sometimes, the more force is used, the less effective it is.... The more successful the counterinsurgency is, the less force can be used and the more risk must be accepted.... Sometimes, doing nothing is the best reaction." This strategy, often termed "courageous restraint", has certainly led to some success on the Middle East battlefield. However, it does not address the fact that terrorists are mostly homegrown.

Mass media exposure may be a primary goal of those carrying out terrorism, to expose issues that would otherwise be ignored by the media. Some consider this to be manipulation and exploitation of the media.

The Internet has created a new channel for groups to spread their messages. This has created a cycle of measures and counter measures by groups in support of and in opposition to terrorist movements. The United Nations has created its own online counter-terrorism resource.

The mass media will, on occasion, censor organizations involved in terrorism (through self-restraint or regulation) to discourage further terrorism. This may encourage organizations to perform more extreme acts of terrorism to be shown in the mass media. Conversely James F. Pastor explains the significant relationship

between terrorism and the media, and the underlying benefit each receives from the other.

There is always a point at which the terrorist ceases to manipulate the media gestalt. A point at which the violence may well escalate, but beyond which the terrorist has become symptomatic of the media gestalt itself. Terrorism as we ordinarily understand it is innately media-related.

—Novelist William Gibson

Former British Prime Minister Margaret Thatcher famously spoke of the close connection between terrorism and the media, calling publicity 'the oxygen of terrorism'.

Outcome of terrorist groups

Jones and Libicki (2008) created a list of all the terrorist groups they could find that were active between 1968 and 2006. They found 648. Of those, 136 splintered and 244 were still active in 2006. Of the ones that ended, 43 percent converted to nonviolent political actions, like the Irish Republican Army in Northern Ireland. Law enforcement took out 40 percent. Ten percent won. Only 20 groups, 7 percent, were destroyed by military force.

Forty-two groups became large enough to be labeled an insurgency; 38 of those had ended by 2006. Of those, 47 percent converted to nonviolent political actors. Only 5 percent were taken out by law enforcement. Twenty-six percent won. Twenty-one percent succumbed to military force. Jones and Libicki

concluded that military force may be necessary to deal with large insurgencies but are only occasionally decisive, because the military is too often seen as a bigger threat to civilians than the terrorists. To avoid that, the rules of engagement must be conscious of collateral damage and work to minimize it.

Another researcher, Audrey Cronin, lists six primary ways that terrorist groups end:

- Capture or killing of a group's leader. (Decapitation).
- Entry of the group into a legitimate political process. (Negotiation).
- Achievement of group aims. (Success).
- Group implosion or loss of public support. (Failure).
- Defeat and elimination through brute force. (Repression).
- Transition from terrorism into other forms of violence. (Reorientation).

The following terrorism databases are or were made publicly available for research purposes, and track specific acts of terrorism:

Global Terrorism Database, an open-source database by the University of Maryland, College Park on terrorist events around the world from 1970 through 2017 with more than 150,000 cases.

MIPT Terrorism Knowledge Base

Worldwide Incidents Tracking System

Tocsearch (dynamic database)

The following public report and index provides a summary of key global trends and patterns in terrorism around the world

Global Terrorism Index, produced annually by the Institute for Economics and Peace

The following publicly available resources index electronic and bibliographic resources on the subject of terrorism

Human Security Gateway

The following terrorism databases are maintained in secrecy by the United States Government for intelligence and counter-terrorism purposes:

- Terrorist Identities Datamart Environment
- Terrorist Screening Database

Jones and Libicki (2008) includes a table of 268 terrorist groups active between 1968 and 2006 with their status as of 2006: still active, splintered, converted to nonviolence, removed by law enforcement or military, or won. (These data are not in a convenient machine-readable format but are available.)

Analysis of Terrorist Attack Scenarios and Measures for Countering Terrorist Threats

Complex engineering systems (CESs), such as nuclear and thermal power stations; hydro engineering facilities; chemical, metallurgical, and oil refinery plants; etc., are critical in terms of population life support and ensuring sustainable economic development. The functioning of complex engineering systems is connected with storing, processing, and transportation of huge amounts of energy and hazardous materials. The unauthorized release of energy and hazardous material at a CES may cause disastrous consequences and trigger cascading failures in interrelated infrastructures. This makes complex engineering systems attractive targets for terrorists and requires special attention in countering terrorist threats.

Complex engineering systems are characterized by a complex structure, complicated behavior, and interaction between their components, which determine the ability of systems to redistribute loads and to resist cascading failures occurring after local failure of their individual components. Owing to the high level of uncertainty concerning the governing parameters of CESs, environmental conditions, and external impacts, the estimation of the complex engineering system performance should be probabilistic. Their evolution should be described by

multivariate scenario trees. Through the efforts of specialists from many countries, an extensive bank of knowledge has been developed for analyzing accidents and catastrophes at complex engineering systems, studying scenarios by which they might be initiated, and reducing the vulnerability of CESs with regard to natural and man-made disasters. This bank of knowledge should be used as widely as possible to ensure security against the impacts of terrorism. This approach to analyzing terrorism-related threats presupposes that emergency situations triggered by terrorist attacks develop according to laws analogous to the development of emergency situations caused by natural or industrial disasters. Therefore, they may be analyzed by methods and models used to address classical problems in risk and safety theory.

The threat of terrorist attacks must be included in the system of studies of possible scenarios of how emergency situations might develop. In particular, event trees used in risk analysis at critically important infrastructure sites must be augmented with scenarios taking into account the possibilities of terrorist attacks that substantially change the scenarios themselves as the structure of primary initiating factors in emergency situations. They also lead to the initiation of cascading processes in the development of accidents and catastrophes with the most serious losses to the population, economic objects, and other vital resources. A classification and probabilistic models of basic scenarios of terrorist attacks were developed (Figure).

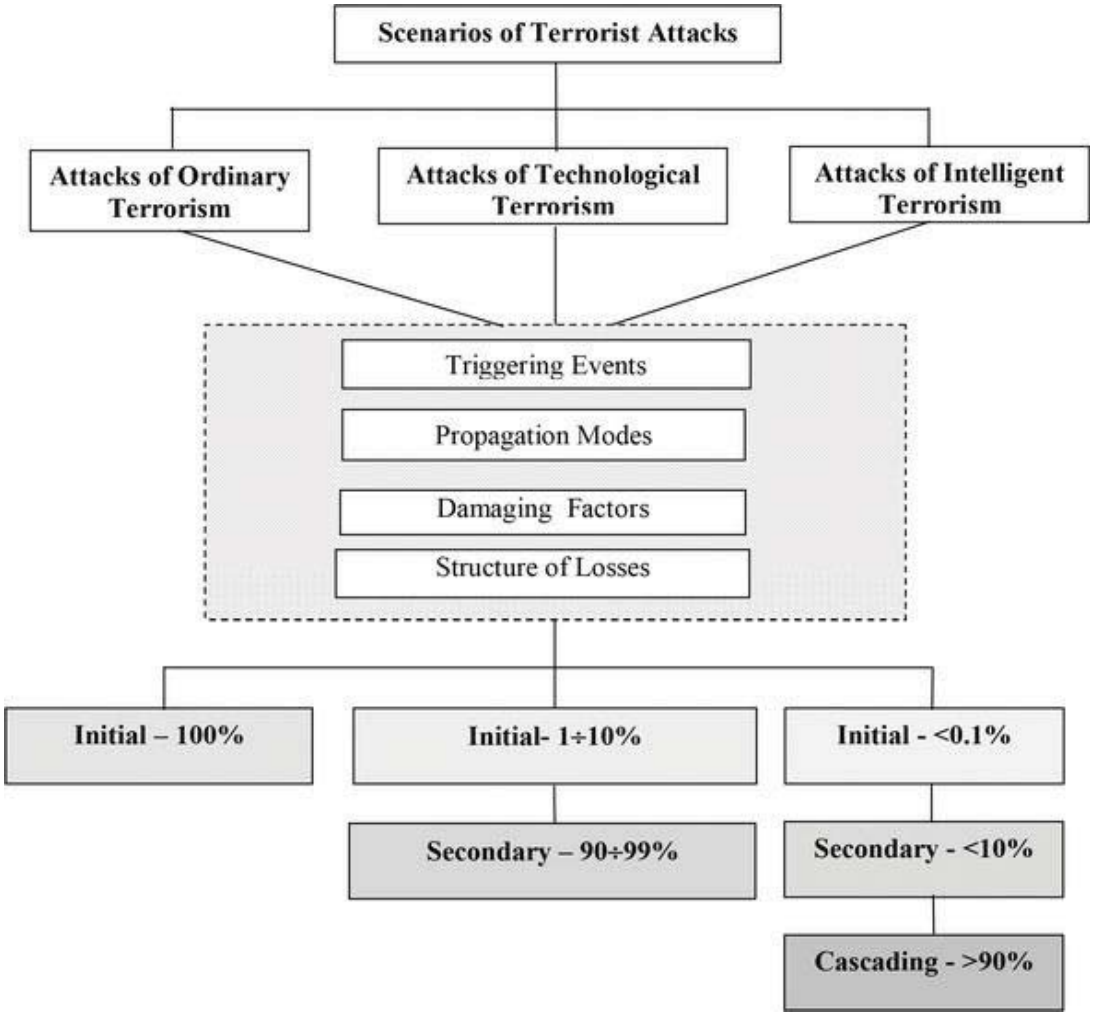

Fig. Basic scenarios of terrorist attacks.

The need to include in the range of problems being considered the analysis of terrorism risks and terrorist mechanisms for initiating extreme situations requires developing and adapting existing models and methods for studying catastrophes with the aim of taking into account the special characteristics of their initiation with the help of unauthorized and terrorist actions that could be taken to attack at the most vulnerable and significant targets critically important for the national security

infrastructure. As it is imperative that terrorist risks and terrorist mechanisms of triggering emergencies be included into the framework of traditional risk assessment, the existing models and methods for analysis of accidents at CES should be modified, and new ones have to be developed in order to take into account specific properties of emergency initiation by terrorist impacts which can be targeted at the most vulnerable facilities of critical infrastructures. Most of the components of complex engineering systems were however constructed in conformity with national and international regulations and norms for design, construction, and maintenance without direct consideration of terrorist threats. In this context, two major security-related problems arise:

Ensuring protection of the existent CES against terrorist attacks

Designing and constructing of a new CES with special protection barriers against terrorist attacks

To cope with these fundamental problems, it is necessary that a special analysis of methods and scenarios of terrorist acts be carried out and a study into how the existing and new protection barriers respond to terrorist attacks be conducted.

Conventional safety analysis for CES is to be focused on the question: What is the way for an accident scenario to be realized in the given system?

When addressing security problems for complex engineering systems, one should also consider the situation from the

terrorist's standpoint. Hence, the modified question for security analysis should be: What is to be done for the given scenario to be realized at a CES?

According to the traditional risk assessment model, risk is considered to be a function of threat T, vulnerability V, and consequences C: $R=f(T,V,C)$. The model was developed to assess risks of technological catastrophes and natural disasters and now is widely used in terrorist risk assessments. Here threat is defined as probability of terrorist attack on a certain complex engineering system, $T=P(A)$; vulnerability is estimated as conditional probability of a system's failure given the attack occurs, $V=P(F|A)$ and consequences are defined as losses that occur as a result of the attack and the system failure, $C=E(U|A,F)$. Then terrorist risk index is determined by Eq. (1):

$$R = P(A) \cdot P(F|A) \cdot E(U|A,F). \qquad \text{E1}$$

For complex engineering systems that are subjected to multiple threats and multiple failure scenarios, risk assessment implies assessment of a scenario tree (Figure). This is being done using graph models called scenario trees. The system is designed to fulfill the so-called success scenario $S0$ (i.e., a transition from its initial state IS to the designed end state $ES0$). Since any failure scenario $S*$ presents a deviation from the success scenario $S0$ that corresponds to the successful functioning of the CES, the scenario $S*$ must have a disturbance point at which an extreme event, or, in case of terrorism, a terrorist attack (Ak), occurs (Figure). Each attack gives rise to a branch of a scenario tree

that has a corresponding set of scenarios *Si* that ends with an end state (*ESi*). In this case, one can get a similar risk index using matrix expression:

$$R = \underbrace{\{P(A_1); P(A_2); \ldots; P(A_n)\}}_{\text{Threat } T} \times \underbrace{\begin{bmatrix} P[ES_1 \mid A_1]\, P[ES_2 \mid A_1] \cdots P[ES_m \mid A_1] \\ P[ES_1 \mid A_2]\, P[ES_2 \mid A_2] \cdots P[ES_m \mid A_2] \\ \ldots \\ P[ES_1 \mid A_n]\, P[ES_2 \mid A_n] \cdots P[ES_m \mid A_n] \end{bmatrix}}_{\text{Vulnerability } \mathbf{V}} \times \underbrace{\begin{Bmatrix} U_{ES_1} \\ U_{ES_2} \\ \ldots \\ U_{ES_m} \end{Bmatrix}}_{\text{Consequences } \mathbf{C}}$$

E2

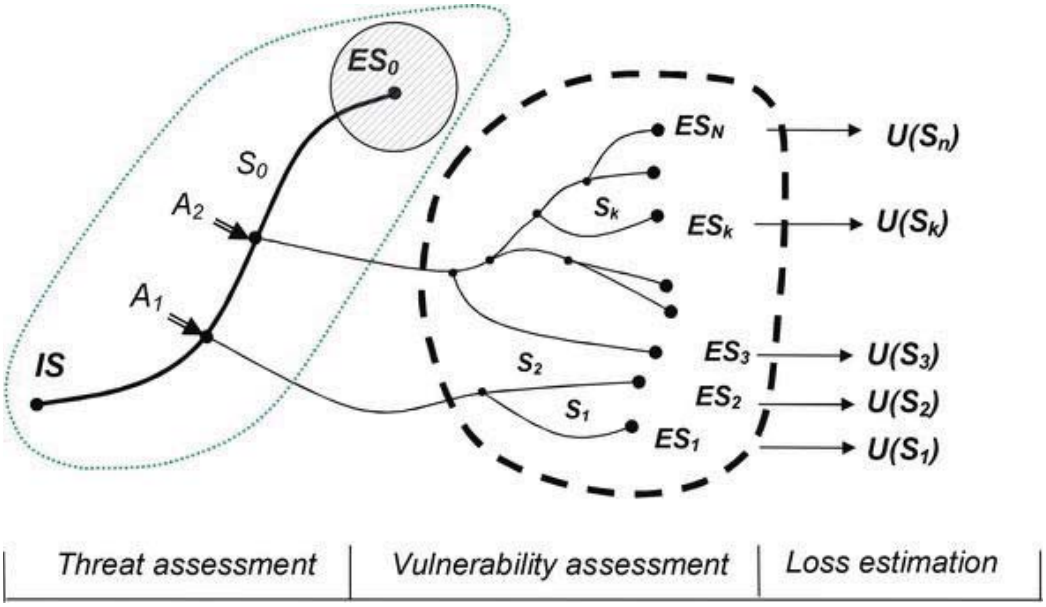

Fig. General risk assessment framework.

Eqs. (1) give first-order indicators of terrorist risk. They also determine three main ways of risk reduction: Reduction of terrorist threat is in the sphere of responsibility of law enforcement and intelligence communities, while reduction of vulnerability and consequences are the domains of engineering community and emergency management agencies, respectively.

In terrorist risk assessment framework, the main challenge is to estimate the probability of a terrorist attack. Some specialists believe that probabilistic measure is not adequate for the terrorist risk assessment since terrorist attack is not a stochastic event but a deliberate action based on the assessment made by terrorists regarding their skills and capabilities and the system's vulnerabilities.

Assignment of probabilities to the terrorist attack is a task which has a substantial human and behavioral dimension. The main problem is to describe the intentions of terrorists, their preferences, system of values (i.e., utility function), and decision rule. This allows one to assess the probability of different attack scenarios. The probability of each attack scenario is a function of the scenario's successful realization and their preferences regarding the expected consequences of that scenario.

Unfortunately, Eqs. (1) could only be considered first-order indicators of the terrorist risk. The problem is that these equations do not allow one to account for a number of specific features of terrorism.

Specific features of terrorist threats

When assessing security-related problems for complex engineering systems, one should take into account the following characteristics of the terrorist threat.

High level of uncertainty: In modeling terrorist scenarios, we encounter a higher level of uncertainty. In addition to the

uncertain factors inherent in threats of a natural or man-made nature, terrorist threats entail new factors of uncertainty resulting from the complexity of evaluating terrorists' system of values and behavioral logic as well as their organizational-technical potential and the resources at their disposal.

High level of dynamism: Terrorist attack scenarios and impact factors are more dynamic by nature than scenarios and impact factors for natural and man-made disasters to which the system is subject. A change in the spectrum and intensity of terrorism-related extreme effects on the system is significantly more rapid than in the case of natural or man-made threat. This is due to the terrorists' capacity for constantly expanding their arsenal of mechanisms for initiating emergency situations using modern means of attack, reacting to changes in protection barriers, and learning lessons from mistakes made during previous attacks on the system similar to it.

The capability of terrorists to choose attack scenarios deliberately: This refers to terrorists' deliberate selection of attack scenarios (places, times, and types of actions), taking into account the system vulnerability parameters and the losses expected if an attack is successfully carried out. That is, terrorists are capable of analyzing the vulnerability matrix and structure of losses for various types of actions against the CES and selecting the attack scenario that maximizes the harm to society (taking into account secondary and cascading losses). Here, in addition to probability analysis, it is also necessary to apply the tools of game theory, which makes it possible to take into account the intentional

actions of terrorists. *Complex nature of the terrorist threat*: The presence of a terrorist organization in a region may give rise to the possibility of a broad spectrum of attack scenarios. Thus, to counter terrorist threats and terrorist mechanisms for initiating emergency situations to an even greater degree than for natural and man-made risks, a systemic approach is needed for ensuring security and developing an optimal strategy for counterterrorism force and resource deployment. Inasmuch as concentrating resources on protecting one system element (or protecting a target from one scenario of terrorist action) could prove useless because, after evaluating the situation, the terrorists could redirect the attack against another element of the system or switch to a different attack scenario. In this case, counterterrorism efforts will fail to reduce risk and increase the system's level of protection.

Presence of two-way linkages between the terrorist threat and system vulnerability: The structure of linkages among the risk factors for the given *CES* in case of natural or manmade catastrophes is presented in Figure. One differentiating feature of a terrorist risk assessment is the presence of two-way linkages (feedbacks) between the terrorist threat and (a) vulnerability of the system to the threat and (b) the magnitude of expected losses if the threat is successfully realized. This characteristic of terrorism must be examined in detail. In particular, reducing the vulnerability of a given system makes it possible to reduce substantially the level of the terrorist threat it faces.

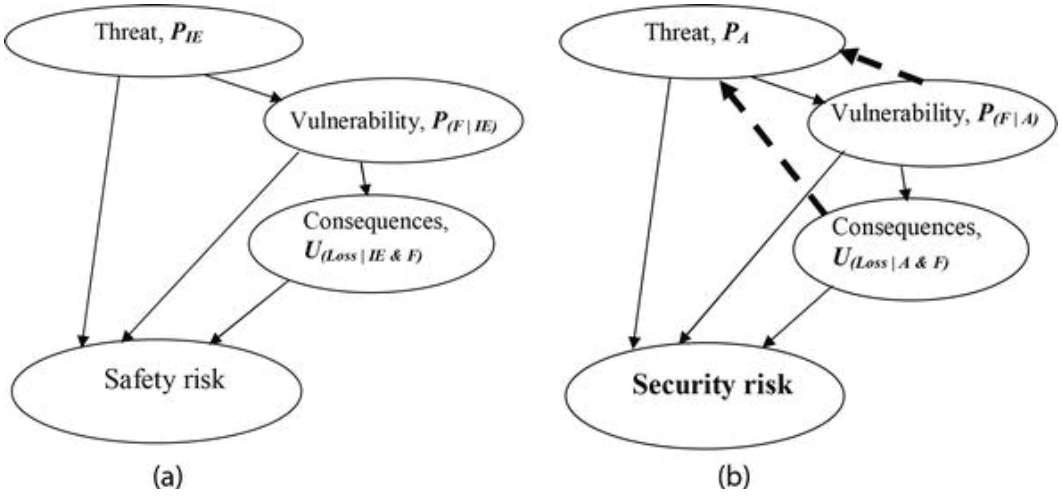

Fig. (a) System of linkages among risk factors for natural or man-made hazards (safety context). (b) System of linkages among risk factors for terrorist threat (security context).

In terrorist risk assessment framework, the main challenge is to estimate the probability of a terrorist attack. Some specialists believe that probabilistic measure is not adequate for the terrorist risk assessment since terrorist attack is not a stochastic event but a deliberate action based on the assessment made by terrorists regarding their skills and capabilities and the system's vulnerabilities.

Assignment of probabilities to the terrorist attack is a task which has a substantial human and behavioral dimension. The main problem is to describe the intentions of terrorists, their preferences, system of values (i.e., utility function), and decision rule. This allows assessing probability of different attack scenarios. *Terrorists' capacity for self-learning*: Because terrorists are capable of analyzing the results of previous attacks and

drawing conclusions from them, their experience in "successful" and "unsuccessful" attacks can have a noticeable effect on the selection of a scenario for the next attack. Attack scenarios that proved their effective in the past are most likely to be repeated by terrorists in the future, while scenarios that ended unsuccessfully will most likely to be less attractive to terrorists and consequently are less likely to be repeated. Therefore, in assessing the chances that various attack scenarios will be realized, statistical self-learning models are more effective than traditional frequency methods.

In solving the above problem of security analysis, it is necessary to assess the resources the terrorists possess. In security analysis, by resources we mean a broad set of factors that determine the potential of a terrorist organization. These include:

Material resources: technical means, equipment, and "human material" that can be used for terrorist attack

Nonmaterial resources: experience and skills of terrorists, their knowledge, and access to the CES internal procedures

To answer the question of security analysis, experts should consider the quality of equipment the terrorists have, their skills and knowledge of *CES*, and their ability to take advantage of the existing vulnerabilities (and even create new ones) in order to organize the attack.

The ability of terrorists to select the most vulnerable and critical elements of *CES*, choose the time and place of an attack, adapt to

changes of safety barriers and defense strategies, and learn lessons from previous attacks requires that the game theory approaches be included into probabilistic risk assessment models. That means that (a) traditional scenario trees used in safety risk assessment, which include only chance nodes, have to be supplemented by decision nodes that describe rational deliberate actions and counteractions of terrorists and counterterrorists; (b) models for terrorist risk assessment should be multi-sided and describe the situation from the perspective of terrorists and counterterrorist forces; (c) these models should be dynamic and allow one to update actions and counteractions of various sides involved at different time steps.

Three types of terrorist attack scenarios

Scenarios of terrorist attacks can be divided into three types, scenarios of ordinary, technological, and intelligent terrorism, that differ in resources used by terrorists to carry out the attacks and structure of losses inflicted by the attacks (Figure).

Scenarios of ordinary terrorism imply organization of explosions, fires, and assassinations of officials, public figures, and people at large in order to intimidate people and destabilize political situation in the country or region. Scenarios of ordinary terrorism are not considered in this paper since these scenarios are not focused on complex engineering systems. We are going to deal with two other types of terrorist attack scenarios that are directly related to *CES.*

Scenarios of technological terrorism

Scenarios of technological terrorism (*STT*) imply powerful unauthorized impacts at complex engineering system capable of:

Breaking through the *CES* protection system

Initiating secondary catastrophic processes due to hazardous substances (*W*), energy (*E*), and information (*I*) stored or processed at the *CES*

Escalation of the accident outside the *CES* boundaries with substantially increased secondary and cascade losses

Technological terrorism is based on taking advantage of the existing vulnerability of the system. To perform an attack of technological terrorism, it is necessary to preliminarily:

Analyze the *CES* structure and vulnerability, i.e., to reveal potential sources of secondary catastrophic processes (stocks of *W,E,I*), the weak points in the *CES* protection systems, and to devise the most efficient attack scenarios.

Identify the *CES* key elements and links whose failure would disrupt the system.

Calculate the strength of the initial impacts that might break through the *CES* protection barriers.

Assess the *CES* scenario tree and determine the end states $ES*$

capable of initiating major secondary catastrophic processes outside the *CES.*

Scenarios of technological terrorism do not require that the attacking party have any insider information and can inflict point impacts imperceptible by the *CES* monitoring systems; therefore, they have to prepare a powerful action capable of breaking through the *CES* protection barriers. It is necessary for the terrorist to select the method for the attack resulting in the CES end state that would initiate the accident propagation outside the *CES* boundaries.

The selection of the attack scenario is made through a hybrid scenario tree that in case of *TT* could be quite simple. It incorporates several attack trees describing the abilities and resources of terrorists and the event tree describing the *CES* vulnerability (Figure).

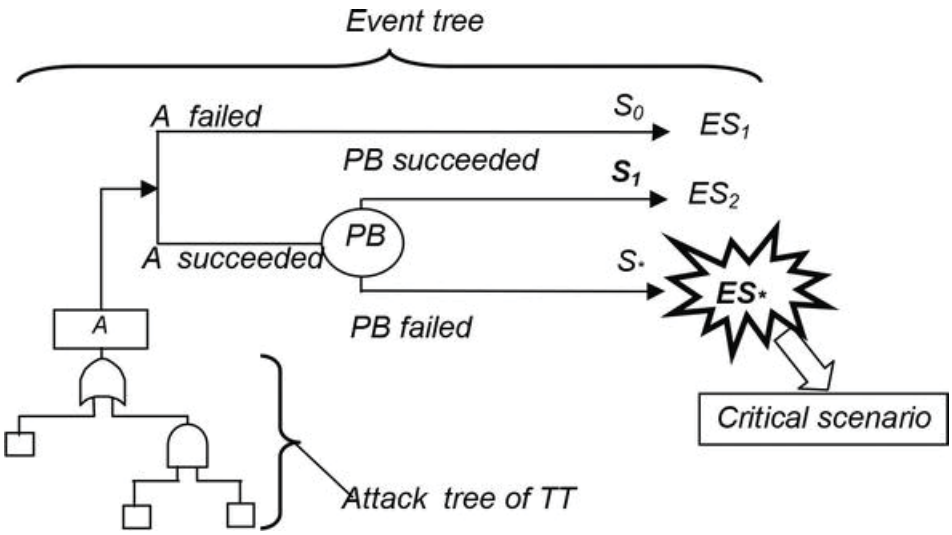

Fig. The scenario tree for technological terrorism.

Scenarios of intelligent (or highly sophisticated, insiders') terrorism

*Intelligent*terrorism (*IT*) is a deliberate unauthorized interference into the process of designing, building, and/or operating the CES aimed at increasing its existing vulnerabilities and creating new ones in the system so that these input vulnerabilities, insider's knowledge of the system, and access to its elements are used for future realization of most disastrous scenarios of a terrorist attack.

IT implies:

A comprehensive vulnerability assessment of a system under design, construction, or operation with respect to various scenarios of terrorist impacts and identification of the most effective way of realization of the initiating impact upon the system

Insertion of latent changes into the system at the stage of its being designed, built, or operated, in order to give rise to new vulnerabilities in the CES

Disconnection or disruption of the *CES* monitoring and protection systems

Triggering cascading failures in the system and the environment

As a rule, scenarios *of IT* require that a member of a terrorist group penetrate into the staff of the organization that is

designing, building, or operating the *CES*. The terrorist must possess insider's information on the *CES* and be able to perform well-camouflaged actions in order to weaken protection systems and create latent defects undetectable by the existing monitoring systems.

Consequently intelligent terrorism implicates detailed knowledge of the *CES* structure and working principles. It also implies awareness of its existing and potential vulnerabilities, possible end states, possible scenarios of accident propagation, and initial impacts that can trigger them. Additionally, *IT* can anticipate distortion of the success scenario, formulate false targets, and generate new disastrous scenarios.

Attacks of intelligent terrorism can be carried out at any stage of the *CES*'s life cycle:

At the stage of design, some latent defects can be intentionally introduced into the system.

At the stage of construction, additional vulnerabilities can be input into the *CES* through intentional violations of the technological processes.

At the stage of operation, some maintenance procedures that are critical for the *CES*'s safety can be intentionally violated.

Intelligent terrorism implies maximal level of the terrorist competence (comprehensive knowledge of the *CES* and its control, operation, and protection barriers), which enables it to select the

most disastrous accident scenarios and find the most effective way of their initiation, disconnection, or disruption of the *CES* monitoring systems in order to prevent prompt response to failures. The assessment of the attack scenarios is made through a hybrid scenario tree that in case of *IT* could be more complicated (Figure). It incorporates several attack trees describing the abilities and resources of terrorists and the decision tree describing the system's vulnerability.

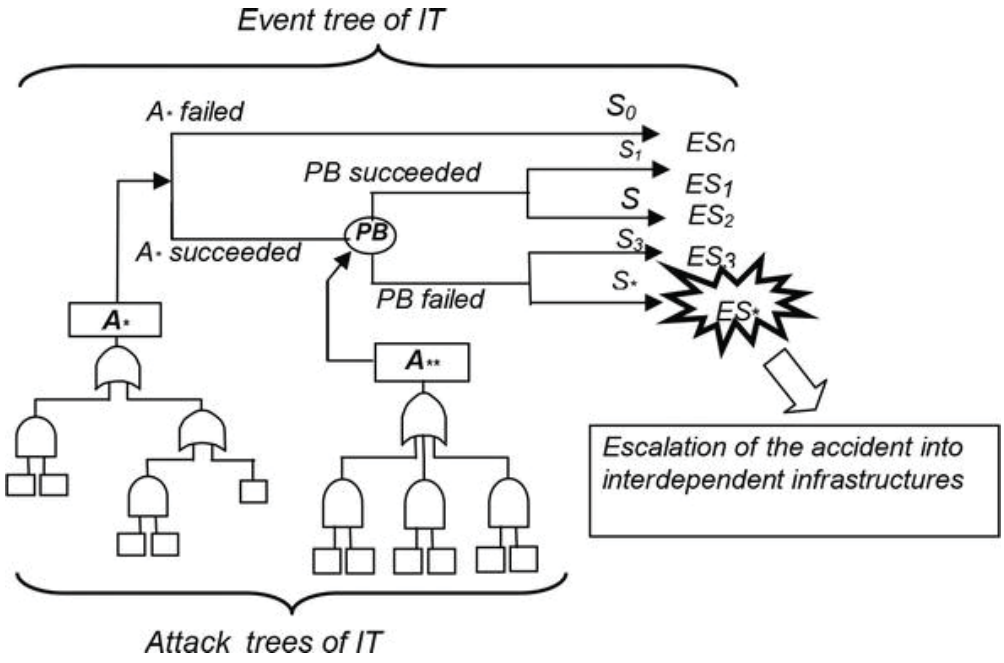

Fig. The scenario tree for intelligent terrorism.

Development of dynamic multi-sided models for analyzing scenarios of terrorist attacks and developing counterterrorist measures

In view of the specific features of terrorist threats addressed in p.3 and the analysis of the scenarios of terrorist attacks on CESs presented in p.4 of this chapter, an integrated (three-sided) terrorist risk model based on the approaches developed in Bayesian networks and game theory has been developed. The schematic representation of the model is given in Figure. Each of the three graphs represents an influence diagram from the perspective of the following players: terrorist group, administration of industrial facility subjected to terrorist threat, and municipal authorities. These three diagrams are separated to keep the decisions made by different parties separate. Oval nodes represent random variables or events with their possible realizations and probabilities assigned. Rectangular nodes represent decisions and are characterized by possible options. The arrows represent probabilistic dependences between the events, state of variables or decision variables.

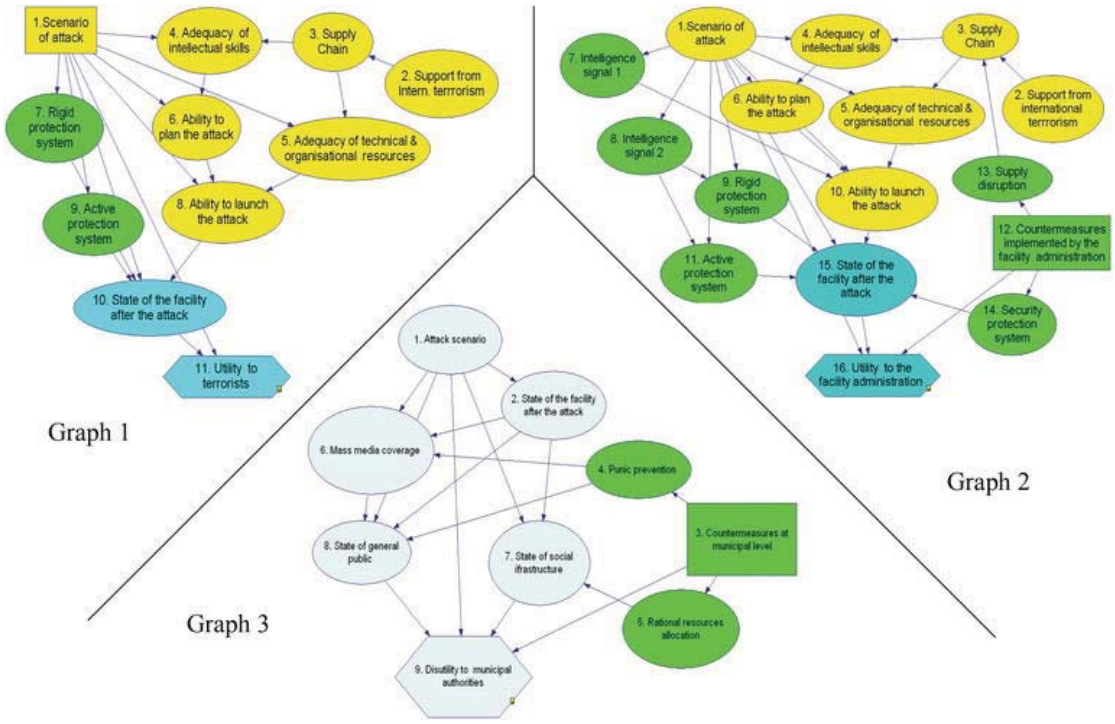

Fig. Multi-sided terrorist risk assessment model.

The model is based on the assumption that all the players act in such a way as to minimize their maximum losses. This strategy is governed by so-called minimax criterion: Counterterrorist players don't know which attack scenario the terrorist group will select, that is why they should choose the defense strategy that results in the lowest possible worst-case expected losses.

Graph 1 (Figure) represents an influence diagram from the perspective of terrorists. It allows one to assess (a) the probabilities that the specified attack scenario will result in damage and (b) the expected utility of terrorist of different attack scenarios.

$$EU(s_i) = \sum_{j=0}^{m} [Ut(s_i; v_j) \times P(V = v_j | S = s_i)] \ (i = 1, \ 2, \ \ldots \ , \ n), \qquad \text{E3}$$

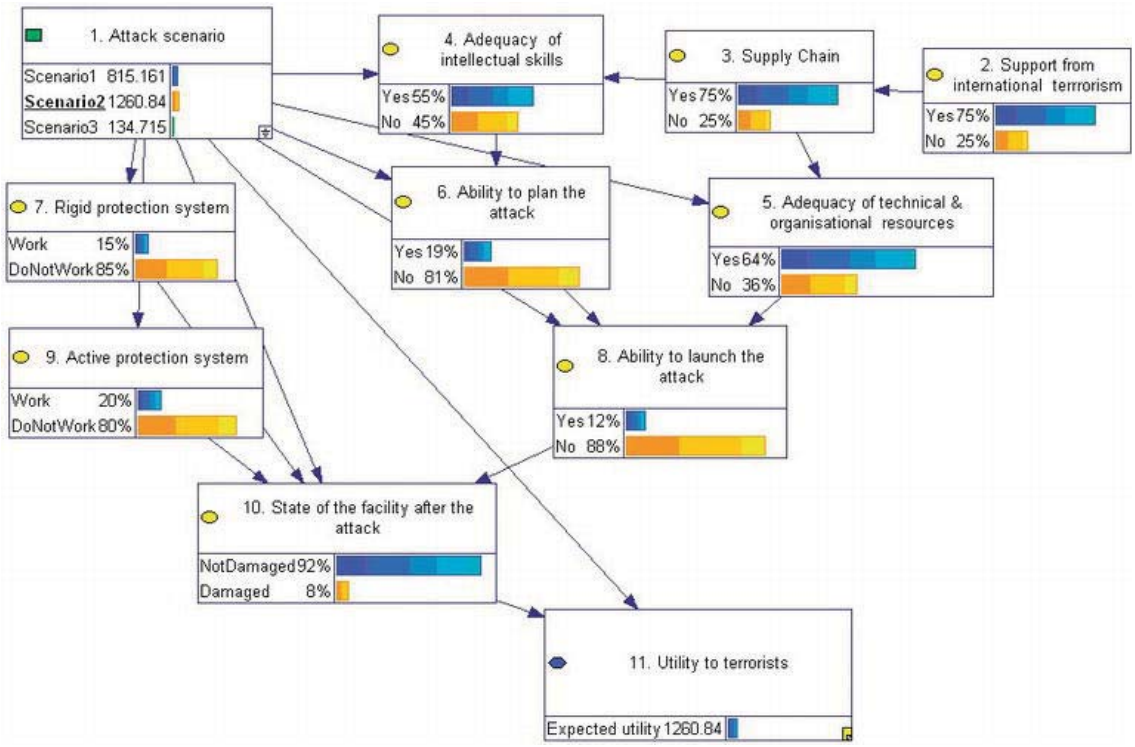

Fig. An illustrative example of the influence diagram from the perspective of terrorist group.

where $Ut(s_i; v_j)$ is an element of utility matrix.

$$\begin{bmatrix} W(s_1; v_0) - Z(s_1) & W(s_1; v_1) - Z(s_1) & \cdots & W(s_1; v_m) - Z(s_1) \\ W(s_2; v_0) - Z(s_2) & W(s_2; v_1) - Z(s_2) & \cdots & W(s_2; v_m) - Z(s_2) \\ & \cdots & & \\ W(s_n; v_0) - Z(s_n) & W(s_n; v_1) - Z(s_n) & \cdots & W(s_n; v_m) - Z(s_n) \end{bmatrix}$$

si is attack scenario; vj is damage factor of the facility inflicted by the attack (j=0,1,...n: j=0 corresponds to a not damaged system, while j=n corresponds to completely destroyed system); $P(V=vj \mid S=si)$ is conditional probability of inflicting damage factor j to the facility provided that attack scenario i was carried out; $W(si; vj)$ is the outcome in case of attack scenario i and damage state j; $Z(si)$ are the costs of implementing attack scenario i.

Calculation of expected utility values for different attack scenarios allows one to estimate probabilities of these scenarios (Eq. (5)):

$$P_t(S = s_i) = \frac{EU_t(s_i)}{\sum_{k=1}^{n} EU_t(s_k)} \quad (i = 1, 2, \ldots n). \qquad \text{E5}$$

Eq. (5) assumes that (a) different attack scenarios are mutually exclusive and (b) the decision taken by terrorists is rational (i.e., they chose attack scenarios that maximize the expected utility). The results obtained in Graph 1 are then used as inputs to Graphs 2 and 3. The results of Graph 2 are then used in Graph 3.

Graph 2 (Figure) represents an influence diagram from the perspective of administration of industrial facility subjected to terrorist threat. It allows one to assess expected disutilities related to various countermeasures made by the administration of the facility involved. The probabilities $Pt(S=si)$

(Eq. (5)) are used in Graph 2 as state probabilities of the chance node 1. The graph permits estimation of expected disutilities to facility administration in case of various countermeasures adopted by the facility administration, to rank countermeasures.

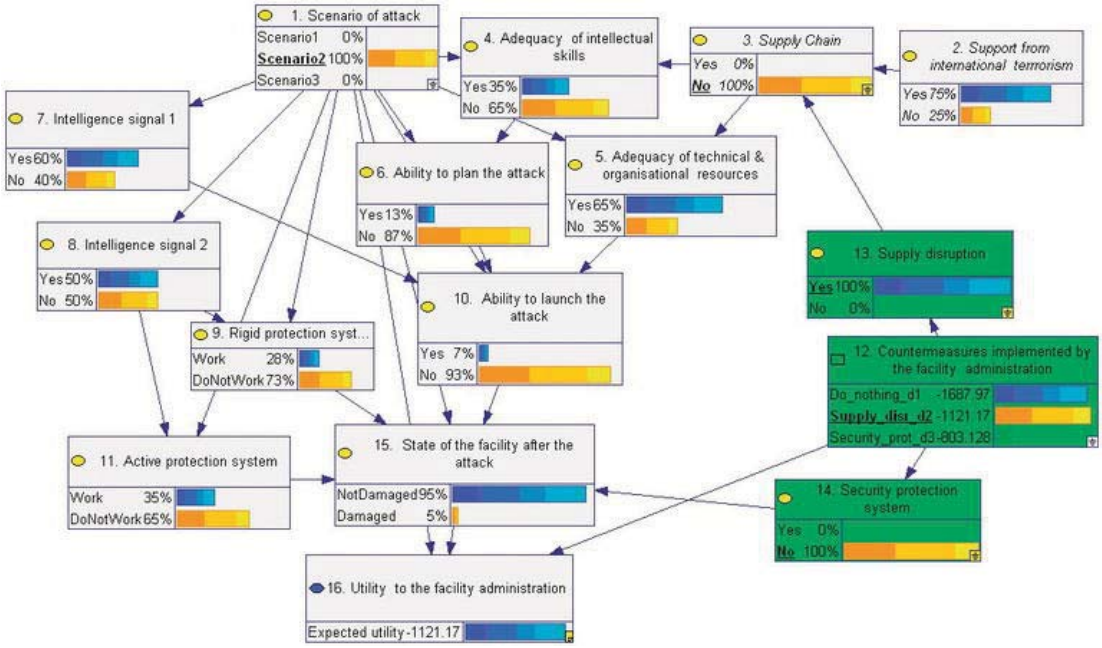

Fig. An illustrative example of the influence diagram from the perspective of CES's administration

Graph 3 (Figure) represents an influence diagram from the perspective of local community authorities. Graph 2 and Graph 3 permit assessment of risk reduction benefits of different countermeasures and their costs.

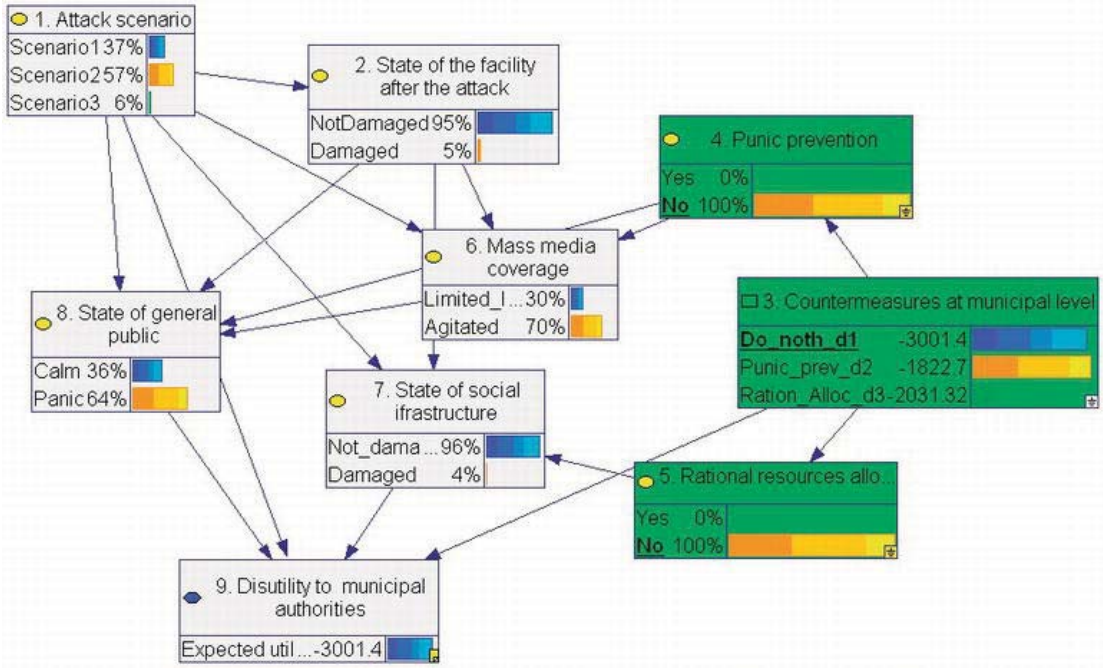

Fig. An illustrative example of the influence diagram from the perspective of community authorities.

The structure of the influence diagrams and probabilistic dependences between the variables should be developed by the joint efforts of specialists representing a broad spectrum of disciplines (these include specialists in terrorist threat assessment, reliability theory, social sciences, loss estimation), each providing insights in their relevant area of expertise. The model permits identification of effects of different factors and parameter values on the likelihood of success of different attack scenarios and on the expected utilities to different sides involved.

The model described above can be used in dynamic fashion via discrete time steps. At each step, each player updates his beliefs, objectives, and decisions based on his previous step. Each of the

players is uncertain about the other's actions and state of knowledge. To address the dynamics of security problem, one needs to model moves and countermoves of all three sides involved, changes in the structure of terrorist organizations and systems of protection, and lessons learned by all parties from previous attacks.

At each consecutive time period, all three parties make decisions regarding their actions in the upcoming time period based on the information accumulated so far (Blocks *Itk*

and *Itk*+1, Figure). Estimations of probabilities of various attack scenarios and countermeasures adopted by facility administration and community authorities obtained at time step *tk* could be treated as prior estimates for the time period *tk*+1. Terrorist may take into account countermeasures of counterterrorist forces by including the respective chance nodes into Graph 1 at time step *tk*+1 and estimate probabilities of countermeasures adopted by facility administration *dj* and municipal authorities *ml* using Eq.(6) similar to Eq.(5):

$$P_a\left(D=d_j\right)=\frac{EU_a(d_j)}{\sum_{g=1}^{3} EU_a(d_g)}, k=1,\ 2,\ 3; P_m\left(M=m_l\right)=\frac{EU_m(m_l)}{\sum_{f=1}^{3} EU_m(m_f)}, l=1,\ 2,\ 3$$

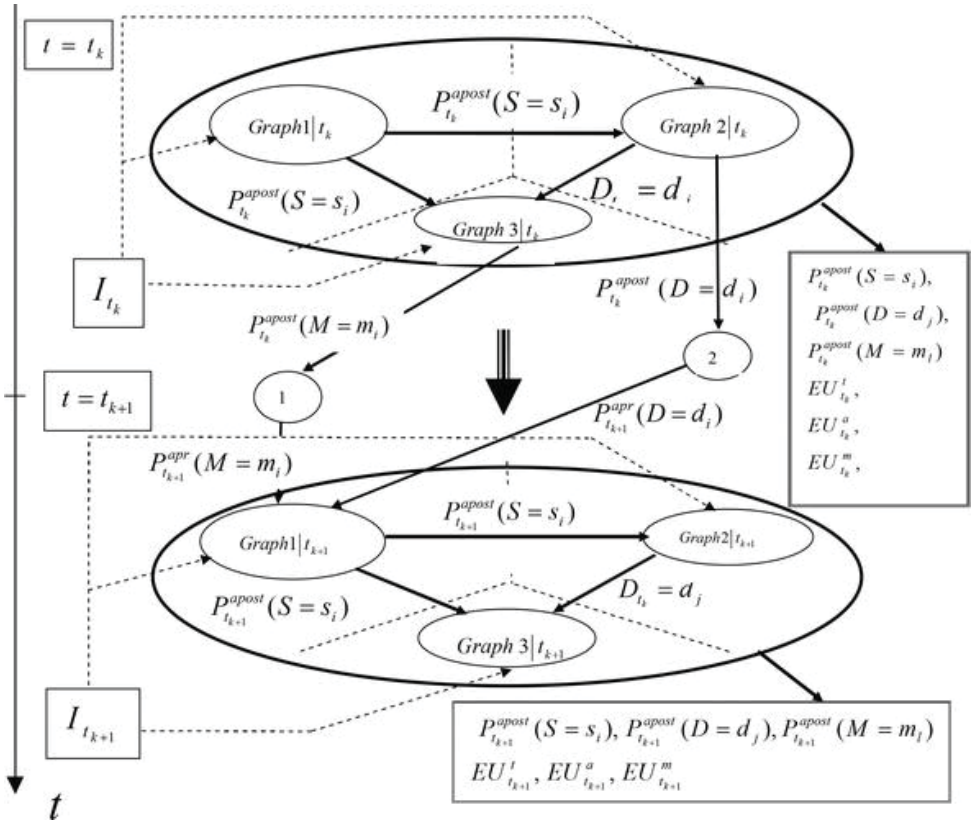

Fig. Dynamic multi-sided terrorist assessment model.

Measures aimed at increasing protection of a CES from terrorist

The complexity of modern engineering systems and their interdependence with other systems make them vulnerable to attacks of technological and intelligent terrorism. This complexity stems largely from the vast functional and spatial dependencies and nonlinear interactions between the components of CES as well as from interdependencies that exist among the CESs which enable failures to cascade within one system and pass from one system to another. Different historical, economic, political,

social, as well as cultural traditions have formed different approaches to ensuring safety of complex engineering systems. Contemporary CESs, i.e., power, transport, and telecommunication networks, are becoming transboundary. Their significant spatial extension makes their functioning dependent on many factors and events in different parts of the world. The ensuring of CES's security is a complex interdisciplinary problem. It is impossible to solve this problem without joining efforts of experts in different fields and taking into account technical, social, psychological, and cultural-historical aspects.

Analysis of major disasters at CES in different countries shows that high-risk engineering systems in many cases are being designed and constructed according to traditional design codes and norms that are based on common and quite simple linear "sequential" risk assessment models and employ traditional design, diagnostics, and protection methods and procedures. This is being done in the assumption that a bounded set of credible design-basis impacts and subsequent failure scenarios could be determined for the CES, thus allowing one to create a system of protection barriers and safeguards that could secure the CES from the identified impacts with required substantially and high probability. This bounded set of impacts referred to as design-basis impacts includes normal operation events as well as abnormal events (component failures, human errors, extreme environmental loads, attacks of technological terrorism on CES) that are expected to occur or might occur at least once during the lifetime of the CES. The currently available approach to ensuring security of complex engineering systems is based on the so-called

protection approach that provides for the development of a set of protection barriers against the list of terrorist attack scenarios that were identified in advance. Within this approach, attacks of technological terrorism should be included into the list of design-basis events. To protect CESs from these scenarios of terrorist attacks, the following types of protection barriers should be developed:

Rigid protection barrier (protection barrier that requires a powerful impact to be broken)

Functional protection barrier (protection barrier that in case of an accident could take on certain system's functions for a limited time or could prevent an accident from progressing further) Natural protection barrier (involves the use of passive natural phenomena and processes aimed at limiting the scales of the accident)

Security guards

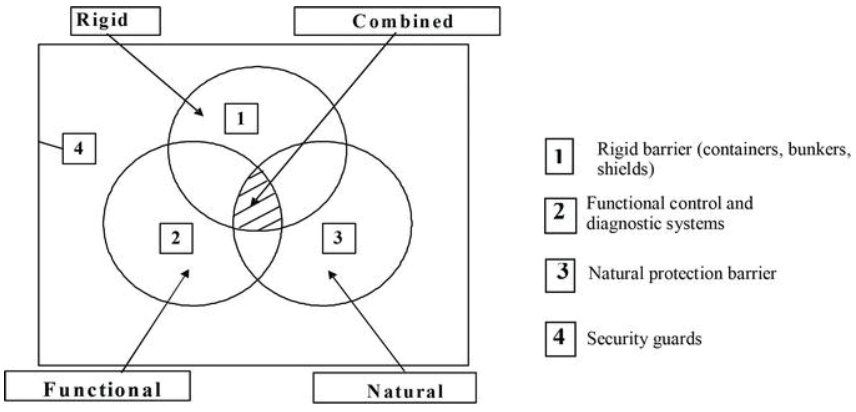

Fig. Types of protection barriers.

Circles "1," "2," and "3" stand for separate types of protection barriers. Areas of intersection ('1-2," "2-3," "1-3," and "1-2-3″) – correspond to combination of correspondent types of protection barriers. Security guard barrier "4″ is organized to ensure protection of all of the above mentioned barriers ("1," "2," "3," "1-2," "2-3," "1-3," and "1-2-3″).

Application of this protection approach allows one to reduce risks of design-basis scenarios of technological terrorism (compare FN curves 1 and 2; Figure). However, it should be noted that this protection-based approach does not allow one to reduce risk of unforeseen "low-probability-high-consequence" scenarios of intelligent terrorism that could not be included into the list of design-basis events.

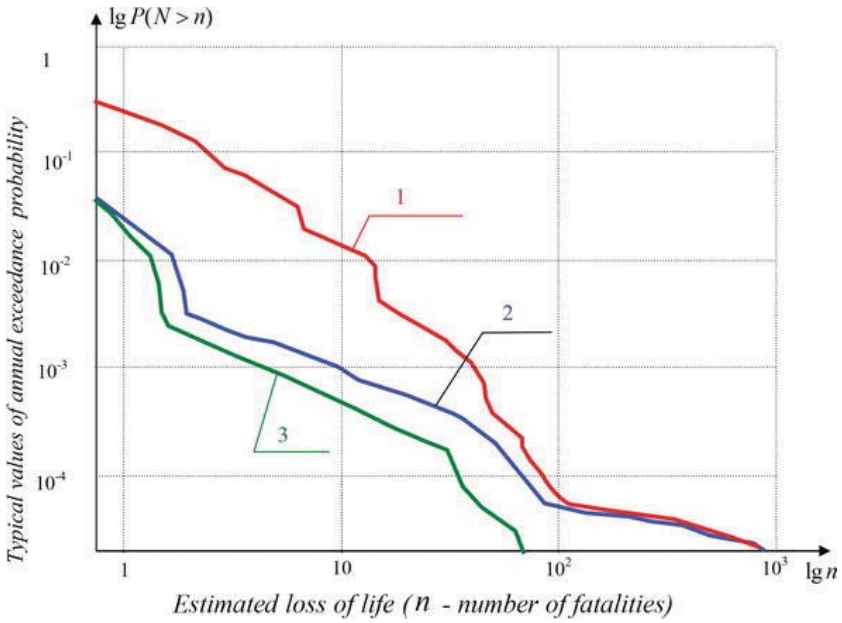

Fig. FN curves before and after realization of protection and resilience measures. (1) FN, curve before realization of any

measure; (2) FN, curve after realization of protection measures; (3) FN, curve after realization of protection and resilience measures.

In currently applied protection-based approach, a number of low-probability impacts of extreme intensity are neglected as being practically incredible. Other impacts (such as attacks of intelligent terrorism) are not identified and, consequently, not analyzed. Such impacts are classified as beyond design-basis impacts. Thus, the issue of protection of CES from beyond design-basis impacts has not been addressed in a proper manner. These impacts however can cause large-scale disasters of extreme severity and induce tremendous property losses and a great number of victims.

Measures focused on ensuring CES's resilience to beyond design-basis events

Complex engineering systems are becoming global networks. The currently available methodologies of risk assessment and reliability engineering were developed for technological systems with fixed boundaries and well-specified hazards for which exists statistical and/or actuarial data on accident initiation events, component failure rates, and accidents' consequences which allow one to quantify and verify models taking into account uncertainties deriving from both natural variations of the system parameters (and performance conditions) and from lack of knowledge of the system itself. The protection-based approach is focused on developing safety barriers for countering the identified

scenarios of terrorist attacks that were included in the list of design-basis events. This approach however has the weakness of neglecting the possibility of beyond design-basis events. To overcome this weakness, a new comprehensive strategy is needed. This strategy should not only include measures aimed at development protection barriers against design-basis attacks of technological terrorism but also development of special measures aimed at increasing the system's resilience to future yet-to-be-determined scenarios of attacks of intelligent terrorism.

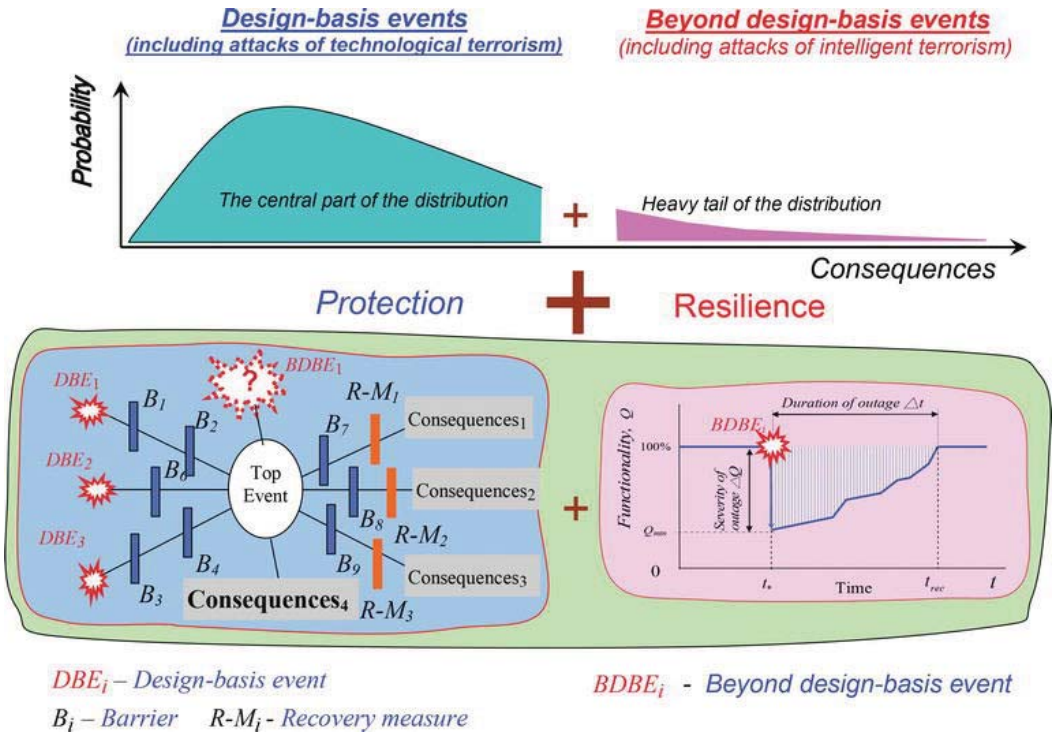

Fig. A new comprehensive approach to ensuring CES's security based on implementation of protection measures and measures for improving resilience of CES.

The current accident models and risk assessment techniques such as fault and event tree analysis are not adequate to account for the complexity of modern engineering systems. Due to rapid technological and societal developments of the recent decades, modern engineering systems are becoming steadily more complex. It means that (a) in safety assessments for CES, there are too many details to be considered, and (b) some modes of CES's operation may be incompletely known due to complex nonlinear interactions between components of CES, due to tight couplings among different systems, and because CES and its environment may change faster than they can be described. As a result, it is impossible to describe the performance of CESs in every detail. In other words for complex engineering systems, it is practically impossible to define a bounded set of design-basis impacts that are expected to occur or might occur at least once during the lifetime of the CES.

This problem can be solved by including the concept of resilience in the processes of designing and ensuring the safety and security of CESs. The proposed approach should not be considered as a substitute but rather a supplement to the traditional one. Adopting this view creates a need to move beyond traditional "threat-vulnerability-consequence" models that are limited to analyzing design-basis events and deal with beyond design-basis impacts and impact combinations. This comprehensive approach will be based on such concepts as resilience to provide more adequate explanations of accidents as well as identify ways to reduce risks caused by beyond design-basis impacts.

In other words, the new security paradigm for complex engineering systems should focus the efforts not only on development of protection barriers and safeguards against design-basis accidents but also on increasing the CES's resilience toward beyond design-basis impacts (Figure).

The CES's resilience is the capacity of the system potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning. This is determined by the degree to which the CES is capable of organizing itself to increase its capacity, of learning from past disasters for better future protection, and to improve risk reduction measures.

Figure presents the so-called resilience profile of the system: a powerful beyond design-basis event (BDBE) occurs at the time moment $t*$

resulting in a slump of the system's performance characteristics Q which recovers at the time moment *trec*. A ratio of the square *Fe* of the figure BDEF that is located under the chart of the CES's performance characteristics in the period between the time moment $t*$, when the beyond design-basis event occurs, and the moment *trec* when the system returns to its normal operation level and the square *Fn* of the rectangular ADEF can be considered as a quantitative measure of the system's resilience:

$$Res = \frac{F_e}{F_n} = \frac{\int_{t_*}^{t_c} Q(t)\,dt}{(t_{rec} - t_*) \cdot Q_n} \times 100\% \qquad \text{E7}$$

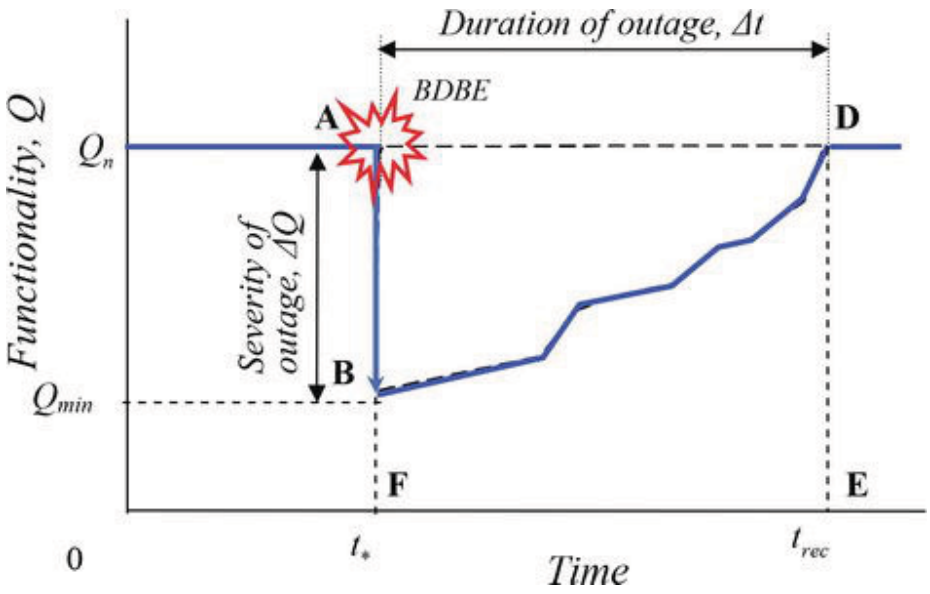

Fig. Resilience profile of CES.

Two groups of measures aimed at increasing the CES resilience can be identified:

Measures focused on reducing the severity of outage ΔQ (Figure)

Measures focused on the reducing the duration of the outage Δt (Figure)

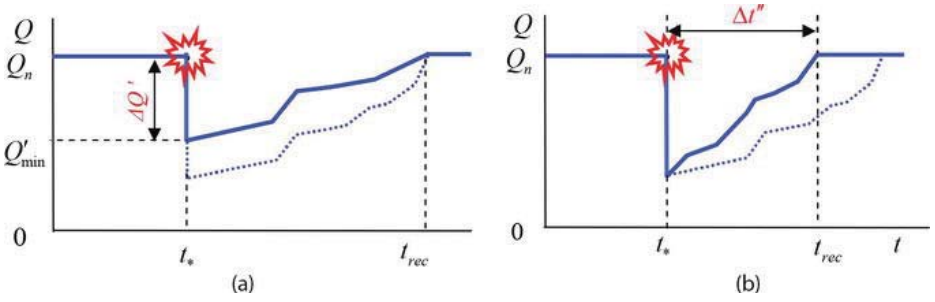

Fig. Measures to increase CES resilience. (a) Reduction of the outage severity. (b) Reduction of the outage duration.

As previously stated, due to the complexity of modern engineering systems and their potentially large-scale catastrophes, in order to ensure security of such systems, one needs to move beyond traditional design-basis risk management framework. The new paradigm needs to be focused on increasing CES's resilience (Figure). That means that if the beyond design-basis accidents are to be considered, the scope of the analysis should be widened. Security-related efforts should be focused not only on the development of protection barriers and safeguards from predetermined (postulated) set of design-basis attacks of technological terrorism but also on additional set of measures aimed at increasing complex engineering system resilience that would prevent catastrophic failure and long-term dysfunctioning of CESs in case of beyond design-basis attacks. Application of such comprehensive (protection and resilience focused) approach allows one to reduce risks of beyond design-basis scenarios of intelligent terrorism (compare FN curves 2 and 3; Figure).

Chapter 2

Nuclear Terrorism

The International Task Force

Nuclear terrorism denotes the use, or threat of the use, of nuclear weapons or radiological weapons in acts of terrorism, including attacks against facilities where radioactive materials are present. In legal terms, nuclear terrorism is an offense committed if a person unlawfully and intentionally "uses in any way radioactive material ... with the intent to cause death or serious bodily injury", according to International conventions. The attacks of September 11, 2001 have provided a wake-up call for facing the threat of nuclear terrorism.

The Nuclear Control Institute, since its inception in 1981, has been analyzing the risks of nuclear terrorism and seeking to alert policymakers and the public to the danger. There was a solid basis for concern long before the attacks of September 11. Iran threatened attacks against U.S. reactors as early as 1987. Trial testimony has revealed that Osama bin Ladens al Qaeda training camps offered instruction in urban warfare against enemies' installations including power plants. It is prudent to assume, especially after the highly coordinated, surprise attacks on the World Trade Center and the Pentagon, that bin Ladens soldiers have done their homework and are fully capable of attacking nuclear plants for maximum effect.

It is also clear that bin Laden was seeking nuclear explosive materials (plutonium or highly enriched uranium) and know-how for building atomic bombs, and other dangerous nuclear materials for use in "dirty bombs" to spread radioactive contamination with conventional high explosives. In 1986, the Nuclear Control Institute, in cooperation with the Institute for Studies in International Terrorism of the State University of New York, convened the International Task Force on Prevention of Nuclear Terrorism, comprised of 26 nuclear scientists and industrialists, current and former government officials, and experts on terrorism from nine countries.

The report issued by the Task Force, along with more than 20 commissioned studies, remains the most definitive examination of nuclear terrorism in the unclassified literature. The Task Force warned that the "probability of nuclear terrorism is increasing" because of a number of factors including "the growing incidence, sophistication and lethality of conventional forms of terrorism," as well as the vulnerability of nuclear power and research reactors to sabotage and of weapons-usable nuclear materials to theft.

The Task Force's warnings and its recommendations for reducing vulnerabilities, many of which went unheeded, are all the more relevant in today's threat environment of sophisticated and suicidal terrorists dedicated to mass killing and destruction. Recent Developments There is now intense national and international attention to the risks of nuclear terrorism. The possibilities that al Qaeda might acquire the materials and the

knowledge for building nuclear weapons or "dirty bombs" or might attack commercial nuclear-power facilities to trigger a nuclear melt down, are of particular concern. The Nuclear Control Institute has been alerting the public and policymakers to these risks, seeking emergency measures to reduce the vulnerabilities, and monitoring and assessing the responses of industry, governments and international agencies.

Are reactors adequately protected against attack? For nearly 20 years, the Nuclear Control Institute has pressed the U.S. Nuclear Regulatory Commission to upgrade security at nuclear power plants. In 1994, we and the California-based Committee to Bridge the Gap finally succeeded in getting NRC to require nuclear-power plant operators to install defenses against truck bombs, although we remain concerned that these protective measures are inadequate to defend against the larger bombs used by terrorists since the 1993 truck-bomb attack against the World Trade Center.

Current NRC security regulations do not address the magnitude of threat demonstrated by the September 11 attacks. NRC standards require that nuclear plant operators protect against a much smaller number of attackers than involved in these attacks. Yet, even under the current weak standards, the armed guards at nearly half of the nuclear plants tested in NRC-supervised security exercises have failed to repel mock terrorist attacks or prevent simulated destruction of redundant safety systems that in real attacks could cause severe core damage, meltdown, and catastrophic radioactive releases. This outcome is all the more

worrisome because the NRCs mock terrorist exercises severely limit the tactics, weapons and explosives used by the adversary, do not test plant defenses against attacks from the air or from the water, and do not test whether guards could repel an attack on the spent-fuel pools at plant sites that contain many times more deadly radioactivity than the reactor cores.

In addition, in response to industry complaints that the exercises are unfairly severe, the NRC is now preparing to shift responsibility for supervising the exercises to the plant operators themselves. Current events clearly demonstrate that nuclear power plant security is too important to be left to industry self-assessment or to the level of protection that industry is willing to pay for. The heightened security at nuclear plants since 9/11 still falls far short of the military-type protection we have recommended. The NRC is undertaking a "top to bottom" review of plant security with no indication of how long it will take to complete and implement or what additional measures will be required. Despite nuclear industry claims to the contrary, it is highly unlikely that nuclear-power reactor containment domes are robust enough to withstand a direct hit from a jumbo jetliner.

Dr. Edwin Lyman, NCIs scientific director, has calculated that a direct, high-speed hit by a large commercial passenger jet "would in fact have a high likelihood a penetrating a containment building" that houses a power reactor. "Following such an assault," Dr. Lyman said, "the possibility of an unmitigated loss-of-coolant accident and significant release of radiation into the environment is a very real one." Such a release, whether caused

by an air strike, or by a ground or water assault, or by insider sabotage could result in tens of thousands of cancer deaths. Could terrorists build nuclear weapons? A study prepared for Nuclear Control Institute by five former U.S. nuclear weapons designers concluded that a sophisticated terrorist group would be capable of designing and building a workable nuclear bomb from stolen plutonium or highly enriched uranium, with potential yields in the kiloton range.

This risk must be taken seriously, particularly in light of documented attempts by al Qaeda to acquire nuclear material and nuclear-weapon design information. Despite claims to the contrary from plutonium-fuel advocates in the nuclear power industry, effective and devastating weapons could be made using "reactor-grade" plutonium, hundreds of tons of which are processed, stored and circulated around the world in civilian nuclear commerce. Would we know if fissile materials were stolen? Less than 18 pounds of plutonium or 55 pounds of highly enriched uranium are sufficient to make a nuclear bomb, but these materials circulate in civilian nuclear commerce by the ton. A crucial defense against nuclear terrorism and nuclear proliferation is to end civilian commerce in plutonium and highly enriched uranium and to convert military stocks of these nuclear explosives into non-weapon-usable forms as soon as possible.

Even the International Atomic Energy Agency, a staunch promoter of nuclear power, has acknowledged an urgent need to improve protection of civilian and military nuclear materials at plant sites as well as in transit. Nuclear Control Institute has

long been a critic of the inability of IAEA inspections and other "safeguards" measures to detect large process losses of plutonium and highly enriched uranium or to ensure adequate protection against thefts of these materials in transit and in storage. IAEA physical-security standards now only apply to international shipments of nuclear materials, not to the facilities where these materials are processed, stored and used.

Because of these shortcomings, we may not even know if materials that could be used in nuclear weapons is missing. The vulnerabilities of Russian nuclear installations have been well documented, but protection of many Western facilities is also inadequate. Shortcomings in security of materials and warheads have even been documented in the U.S. nuclear-weapons complex. The situation in such emerging nuclear-weapon states as India and Pakistan is even more troubling. Contingency responses to theft and smuggling of materials or warheads must be further developed, and technical capabilities for finding and disarming terrorist bombs must be improved.

Vulnerable to Theft

Although generally better secured than nuclear materials, there is still a possibility that nuclear weapons could be stolen by terrorists. In 1986, the NCI\SUNY International Task Force on the Prevention of Nuclear Terrorism raised concerns about the vulnerability of tactical nuclear weapons to theft. Since the 1991 collapse of the Soviet Union, the United States and Russia have removed nearly all their tactical nuclear weapons from overseas

deployment. However, there has been continued speculation that some number of Soviet "suitcase bombs" (small portable nuclear weapons) remain unaccounted for, with unconfirmed reports that they have been obtained by al Qaeda.

Also, security weaknesses have been identified at nuclear weapons laboratories and other installations in both Russia and the United States. Further, the security of India and Pakistans embryonic nuclear arsenals is uncertain, as is the question of whether weapons in these states are secured by Permissive Action Link (PAL) systems (coded, electronic locks). In the United States, the Nuclear Emergency Search Team (NEST) is a highly secretive federal inter-agency group that has had the responsibility for more than 20 years for locating and deactivating terrorist nuclear weapons, but its technical ability to fulfill this daunting mission if the need arose remains uncertain.

How Vulnerable are Russian Weapons, Fissile Materials, and Reactors? Since the collapse of the Soviet Union in 1991, the uncertain status of nuclear weapons, fissile materials and nuclear scientists in Russia and other former Soviet republics are widely regarded as posing perhaps the most immediate threat of nuclear proliferation and nuclear terrorism. Despite significant assistance from the United States over the last ten years, many of Russias nuclear facilities seem poorly secured, and there is still no comprehensive, verifiable system of nuclear materials accountancy. No one even knows for certain how much nuclear weapons material the Soviet Union produced.

With confirmed incidents of Russian-origin fissile materials turning up for sale on the black market, this danger is more than hypothetical. Controversy also rages over how to dispose of plutonium recovered from dismantled Russian warheads. The Russian government and the Bush Administration plan to fabricate excess Russian and U.S. plutonium into mixed-oxide fuel (MOX) for irradiation in nuclear-power reactors (including Russias BN-600 prototype fast breeder reactor). However, a safer, less costly and more secure alternative would be to combine the plutonium with highly radioactive waste in molten glass. This immobilized plutonium, embedded in massive, highly radioactive glass blocks, could be directly disposed of in a geologic repository, and would prevent the circulation of tens of tons of plutonium in civilian commerce throughout Russia (as well as the United States) that the MOX-fuel approach would necessitate.

NCI has supported U.S. assistance to secure Russias nuclear weapons, materials and facilities under the Defense Departments Cooperative Threat Reduction Program (Nunn-Lugar) since its inception in 1991. NCI has played a leading role in advocating the shutdown of Russias military plutonium production reactors, and has strongly and successfully opposed Russian proposals to convert these reactors to bomb-usable HEU fuel rather than closing them or converting to low-enriched uranium fuel. Are "Dirty Bombs" a Major Terrorism Risk? "Dirty bombs," known also as radiation dispersal devices (RDDs), are weapons that use conventional explosives to disperse radioactive materials, thereby augmenting the injury and property damage caused by the explosion.

The capability of an RDD to cause significant harm is strongly dependent on the type of radioactive material used and the means used to disperse it. Other important variables include location of the device and prevailing weather conditions. Radioactive materials that could be employed in RDDs range from radiation sources used in medicine or industry to spent nuclear fuel from nuclear power plants. In general, the physical protection requirements for radioactive sources widely used in commerce are quite lax; however, the largest radiotherapy sources typically contain no more than a few hundred curies of gamma-emitters like cesium-137 or cobalt-60. Sources of this size, if removed from their shielded containers, could present an acute hazard to individuals within the vicinity (tens of meters) of the source.

However, an effective dispersal of the material would tend to dilute the concentration downwind of the site of detonation to relatively low levels quickly. Acute radiation hazard would probably be confined to an area of a few hundred meters radius around the site for a ground-level release. However, the occurrence of localized areas of contamination further downwind would be a possibility, depending on the meteorology. Standard modeling of these events in the midst of densely populated urban areas indicates no acute fatalities from radiation exposure and few cancer deaths. However, these models do not take into account the additional consequences that might occur from radioactive contamination of wounds suffered by people injured during the blast, which could cause additional internal

contamination, or direct radiation exposure, which could impair the immune systems of burn victims and thwart their recovery.

The most concentrated sources of large quantities of radioactive isotopes are contained in spent nuclear fuel from power plants, but these sources are relatively inaccessible due to their size (several meters in height), weight (half a metric ton) and radiation barrier (thousands to tens of thousands of rem per hour surface dose). A single spent fuel assembly typically can be transported only in a shielded shipping cask weighing many tons. However, if such a package, usually containing radioactive inventories hundreds or thousands of times greater than those of the medical sources, could be acquired by terrorists or sabotaged during transport in an urban area, severe consequences could result, including thousands of latent cancer fatalities.

Nuclear terrorism denotes the use, or threat of the use, of nuclear weapons or radiological weapons in acts of terrorism, including attacks against facilities where radioactive materials are present. In legal terms, nuclear terrorism is an offense committed if a person unlawfully and intentionally "uses in any way radioactive material ... with the intent to cause death or serious bodily injury", according to International conventions. The notion of terrorist organizations using nuclear weapons (especially very small ones, such as suitcase nukes) has been a threat in American rhetoric and culture.

Two of the main dangers associated with nuclear reactors are nuclear proliferation and nuclear terrorism. Terrorism involving

nuclear weapons or radioactive materials could take a variety of forms. Terrorists could:

Attack a nuclear reactor.

Disrupt critical inputs (eg., water supply) for the safe running of a nuclear reactor.

Steal nuclear fuel or waste.

Acquire fissile material and fabricate a crude nuclear bomb.

Acquire a ready-made nuclear weapon or take over a nuclear-armed submarine, plane or base.

Radiological Weapons

It may be possible for a terrorist group to acquire or build the capability to detonate a radiological or 'dirty bomb'. A 'dirty bomb' is composed of depleted uranium or plutonium produced as a byproduct of the nuclear fuel cycle in a civilian reactor. Detonation of such a weapon is not as powerful as a nuclear blast, but would produce considerable radioactive fallout.

This type of weapon may be very appealing to terrorist groups as it is highly successful in instilling fear and panic amongst a population (particularly because of the widespread fear of radiation poisoning), and would make the immediate area surrounding the blast untenable for some period of time,

disrupting attempts to repair the damage and reassure the population.

Planned and attempted attacks

In June 2002, U.S. citizen Jose Padilla was arrested for allegedly planning a radiological attack on the city of Chicago; however, he was never charged with such conduct. He was instead convicted of charges that he conspired to "murder, kidnap and maim" people overseas. In November 2006, MI5 warned that Islamic terrorists, specifically the al-Qaida were planning on using nuclear weapons against cities in the United Kingdom by obtaining the bombs via clandestine means. In June 2007 Fox News claimed that the FBI released to the press the name of the operations leader for developing tactical plans for detonating nuclear bombs in several American cities simultaneously as Adnan Gulshair el Shukrijumah.

Radiological assassinations

It is also possible that a terrorist group could utilise radiological agents (such as thallium or polonium) in order to poison officials or members of government. These agents could be injected into or ingested by the target, resulting in radiological poisoning and death, either immediately or over an extended period of time. Although no such act has yet been committed by terrorists, some covert intelligence agencies have been accused of using this tactic in the past. Examples include:

- Poisoning of Nikolai Khokhlov by radioactive thallium poisoning in Frankfurt in 1957 by KGB
- Assassination of Alexander Litvinenko with radionuclide polonium-210 on November 1, 2006
- Death of Yuri Shchekochikhin on July 3, 2003 in Moscow (suspected)

Recovering lost weapons & material

In August 2002, the United States launched a program to track and secure enriched uranium from 24 Soviet-style reactors in 16 countries, in order to reduce the risk of the materials falling into the hands of terrorists or "rogue states". The first such operation was *Project Vinca*, an operation in Serbia "to remove a quantity of highly enriched uranium, sufficient to produce 2-1/2 nuclear weapons from a research reactor near downtown Belgrade"

In order to reduce the danger of attacks using nuclear waste material, European Union Commissioner Loyola de Palacio suggested in November 2002 the creation of common standards in the European Union, especially in the new member states operating Soviet-era reactors, for subterranean nuclear waste disposal.

Countries involved in nuclear threat

Some nations have been identified as a "nuclear threat" by countries like USA, China et al. based on the perception of threat the countries' nukes and their misuse might pose. Pakistan tops

the list of nations whose possession of nuclear weapons poses a serious and grave risk to international security by proliferation to various countries including North Korea. According to a recent poll of 100 US foreign policy experts by the Centre for American Progress and the Carnegie Endowment, both in Washington, Pakistan poses today's greatest nuclear threat to the world Pakistan's nuclear chief A.Q. Khan had also sold nuclear secrets in the black market and is likely to pose a threat in the form of a dirty bomb attack.

Preparations to nuclear sabotage

The highest-ranking GRU defector Stanislav Lunev described alleged Soviet plans for using tactical nuclear weapons for sabotage against the United states in the event of war. He described Soviet-made suitcase nukes identified as RA-115s (or RA-115-01s for submersible weapons) which weigh from fifty to sixty pounds. These portable bombs can last for many years if wired to an electric source. "In case there is a loss of power, there is a battery backup. If the battery runs low, the weapon has a transmitter that sends a coded message – either by satellite or directly to a GRU post at a Russian embassy or consulate."

Lunev was personally looking for hiding places for weapons caches in the Shenandoah Valley area. He said that "it is surprisingly easy to smuggle nuclear weapons into the US" either across the Mexican border or using a small transport missile that can slip though undetected when launched from a Russian airplane US Congressman Curt Weldon supported claims by

Lunev, but "Weldon said later the FBI discredited Lunev, saying that he exaggerated things." Searches of the areas identified by Lunev - who admits he never planted any weapons in the US - have been conducted, "but law-enforcement officials have never found such weapons caches, with or without portable nuclear weapons."

Privately owned nuclear weapons

According to high-ranking Russian SVR defector Tretyakov, he had a meeting with two Russian businessmen representing a state-created *Chetek* corporation in 1991. They came up with a fantastic project of destroying large quantities of chemical wastes collected from Western countries at the island of Novaya Zemlya (a test place for Soviet nuclear weapons) using an underground nuclear blast. The project was rejected by Canadian representatives, but one of the businessmen told Tretyakov that he keeps his own nuclear bomb at his dacha outside Moscow.

Tretyakov thought that man was insane, but the "businessmen" (Vladimir K. Dmitriev) replied: "Do not be so naive. With economic conditions the way they are in Russia today, anyone with enough money can buy a nuclear bomb. It's no big deal really" period of time. Although no such act has yet been committed by terrorists, some covert intelligence quantity of highly enriched uranium, sufficient to produce 2-1/2 nuclear weapons from a research reactor near downtown Belgrade". In order to reduce the danger of attacks using nuclear waste material, European Union Commissioner Loyola de Palacio

suggested in November 2002 the creation of common standards in the European Union, especially in the new member states operating Soviet-era reactors, for subterranean nuclear waste disposal. A weapon of mass destruction (WMD) is a weapon that can kill large numbers of humans and/or cause great damage to man-made structures (e.g. buildings), natural structures (e.g. mountains), or the biosphere in general. The term covers several weapon types, including nuclear, biological, chemical (NBC), and radiological weapons.

Additional terms used in a military context include atomic, biological, and chemical (ABC) warfare and chemical, biological, radiological, and nuclear (CBRN) warfare. The phrase was predominantly used in reference to nuclear weapons during the Cold War; following the collapse of the Soviet Union and increasing tensions between the Middle East and the Western powers, the term broadened to its modern, more inclusive definition. It entered widespread usage in relation to the U.S.-led 2003 invasion of Iraq.

Early uses of the term

The first use of the term "weapons of mass destruction" on record is from *The Times* (London) in 1937 in reference to the aerial bombardment of Guernica, Spain:

- At that time, there were no nuclear weapons; biological weapons were already being researched by Japan (see

Unit 731), and chemical weapons had seen wide use, most notably in World War I.

Following the atomic bombings of Hiroshima and Nagasaki, and progressing through the Cold War, the term came to refer more to non-conventional weapons. The application of the term to specifically nuclear and radiological weapons is traced by William Safire to the Russian phrase *oruziye massovovo porazheniya*. He credits James Goodby (of the Brookings Institution) with tracing what he considers the earliest known English-language use soon after the nuclear bombing of Hiroshima and Nagasaki (although it is not quite verbatim): a communique from a November 15, 1945 meeting of Harry Truman, Clement Attlee and Mackenzie King (probably drafted by Vannevar Bush – or so Bush claimed in 1970) referred to "weapons adaptable to mass destruction".

That exact phrase, says Safire, was also used by Bernard Baruch in 1946 (in a speech at the United Nations probably written by Herbert Bayard Swope). The same phrase found its way into the UN resolution to create the Atomic Energy Commission (predecessor of the International Atomic Energy Agency (IAEA)), which used the wording "...atomic weapons and of all other weapons adaptable to mass destruction". An exact use of this term was given in a lecture "Atomic Energy as an Atomic Problem" by J. Robert Oppenheimer. The lecture was delivered to the Foreign Service and the State Department, on September 17th, 1947. The lecture is reprinted in *The Open Mind* (New York: Simon and Schuster, 1955). "It is a very far reaching control which would eliminate the rivalry between nations in this field,

which would prevent the surreptitious arming of one nation against another, which would provide some cushion of time before atomic attack, and presumably therefore before any attack with weapons of mass destruction, and which would go a long way toward removing atomic energy at least as a source of conflict between the powers." An early use of the exact phrase in an international treaty was in the Outer Space Treaty of 1967, however no definition was provided.

Evolution of its use

During the Cold War, the term "weapons of mass destruction" was primarily a reference to nuclear weapons. At the time, the US arsenal of thermonuclear weapons were regarded as a necessary deterrent against an all-out strike from the Soviet Union (see Mutual Assured Destruction), and the euphemism "strategic weapons" was used to refer to the American nuclear arsenal. The term "weapons of mass destruction" continued to see periodic use throughout this time, usually in the context of nuclear arms control; Ronald Reagan used it during the 1986 Reykjavík Summit, when referring to the 1967 Outer Space Treaty.

Reagan's successor, George H.W. Bush, used the term in an 1989 speech to the United Nations, using it primarily in reference to chemical arms. The end of the Cold War reduced U.S. reliance on nuclear weapons as a deterrent, causing it to shift its focus to disarmament. This period coincided with an increasing threat to U.S. interests from Islamic nations and independent Islamic groups. With the 1990 invasion of Kuwait and 1991 Gulf War,

Iraq's nuclear, biological, and chemical weapons programs became a particular concern of the first Bush Administration.

Following the war, the Clinton Administration and other western politicians and media continued to use the term, usually in reference to ongoing attempts to dismantle Iraq's weapons programs. After the September 11, 2001 attacks and the 2001 anthrax attacks, an increased fear of non-conventional weapons and asymmetrical warfare took hold of the United States and other Western powers. This fear reached a crescendo with the 2002 Iraq disarmament crisis and the alleged existence of weapons of mass destruction in Iraq that became the primary justification for the 2003 invasion of Iraq. Because of its prolific use during this period, the American Dialect Society voted "weapons of mass destruction" (and its abbreviation, "WMD") the word of the year in 2002, and in 2003 Lake Superior State University added WMD to its list of terms banished for "*Mis-use, Over-use and General Uselessness*".

Definitions of the term

The most widely used definition of "weapons of mass destruction" is that of nuclear, biological or chemical weapons (NBC), although there is no treaty or customary international law that contains an authoritative definition. Instead, international law has been used with respect to the specific categories of weapons within WMD, and not to WMD as a whole. The acronym NBC (for nuclear, biological and chemical) is used with regards to battlefield protection systems for armored vehicles, because all

three involve insidious toxins that can be carried through the air and can be protected against with vehicle air filtration systems.

However, there is an argument that nuclear weapons do not belong in the same category as chemical, biological, or "dirty bomb" radiological weapons, which have limited destructive potential (and close to none, as far as property is concerned), whereas nuclear weapons are immensely destructive and could be said to belong in a class by themselves. The NBC definition has also been used in official U.S. documents, by the U.S. President, the U.S. Central Intelligence Agency, the U.S. Department of Defense, and the U.S. Government Accountability Office.

Other documents expand the definition of WMD to also include radiological or conventional weapons. The U.S. military refers to WMD as:

Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

The significance of the words *separable and divisible part of the weapon* is that missiles such as the Pershing II and the SCUD are considered weapons of mass destruction, while aircraft capable of carrying bombloads are not. Within U.S. civil defense organizations, the category is now Chemical, Biological,

Radiological, Nuclear, and Explosive (CBRNE), which defines WMD as:

(1) Any explosive, incendiary, poison gas, bomb, grenade, or rocket having a propellant charge of more than four ounces [113 g], missile having an explosive or incendiary charge of more than one-quarter ounce [7 g], or mine or device similar to the above. (2) Poison gas. (3) Any weapon involving a disease organism. (4) Any weapon that is designed to release radiation at a level dangerous to human life. This definition derives from US law, 18 U.S.C. Section 2332a and the referenced 18 USC 921. Indictments and convictions for possession and use of WMD such as truck bombs, pipe bombs, shoe bombs, cactus needles coated with botulin toxin, etc. have been obtained under 18 USC 2332a.

The U.S. FBI also considers conventional weapons (i.e. bombs) as WMD: "*A weapon crosses the WMD threshold when the consequences of its release overwhelm local responders*". Gustavo Bell Lemus, the Vice President of Colombia, at the 2001 United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, quoted the Millennium Report of the UN Secretary-General to the General Assembly, in which Kofi Annan said that small arms could be described as WMD because the fatalities they cause "*dwarf that of all other weapons systems - and in most years greatly exceed the toll of the atomic bombs that devastated Hiroshima and Nagasaki*"

Chemical weapons expert Gert G. Harigel considers only nuclear weapons true weapons of mass destruction, because "only nuclear weapons are completely indiscriminate by their explosive

power, heat radiation and radioactivity, and only they should therefore be called a weapon of mass destruction". He prefers to call chemical and biological weapons "weapons of terror" when aimed against civilians and "weapons of intimidation" for soldiers. Testimony of one such soldier expresses the same viewpoint. For a period of several months in the winter of 2002-2003, U.S. Deputy Secretary of Defense Paul Wolfowitz frequently used the term "weapons of mass terror," apparently also recognizing the distinction between the psychological and the physical effects of many things currently falling into the WMD category.

An additional condition often implicitly applied to WMD is that the use of the weapons must be strategic. In other words, they would be designed to "*have consequences far outweighing the size and effectiveness of the weapons themselves*". The strategic nature of WMD also defines their function in the military doctrine of total war as targeting the means a country would use to support and supply its war effort, specifically its population, industry, and natural resources. *The Washington Post* reported on 3/30/2006: "Jurors asked the judge in the death penalty trial of Zacarias Moussaoui today to define the term "weapons of mass destruction" and were told it includes airplanes used as missiles". Moussaoui was indicted and tried for the use of airplanes as WMD.

WMD use and control

The development and use of WMD is governed by international conventions and treaties, although not all countries have signed and ratified them:

- Partial Test Ban Treaty
- Outer Space Treaty
- Nuclear Non-Proliferation Treaty (NPT)
- Seabed Arms Control Treaty
- Comprehensive Test Ban Treaty (CTBT)
- Biological and Toxin Weapons Convention (BWC)
- Chemical Weapons Convention (CWC)

In 1996 the International Court of Justice provided an advisory opinion regarding the use and threat of use of nuclear weapons. The statement is an authoritative legal pronouncement but not legally binding. It stated that any threat of the use of force, or the use of force, by means of nuclear weapons that is contrary to Article 2, paragraph 4 of the United Nations Charter or that fails to meet all the requirements of Article 51 would be unlawful. Adopted by the UN Security Council on April 28, 2004, UN Resolution 1540 recognizes the threat posed to international peace and security by nuclear, chemical and biological weapons, as well as their means of delivery. It calls upon greater effort by nations to limit proliferation of such weapons.

Weapons of mass destruction, especially nuclear weapons, are rarely used because their use is essentially an "invitation" for a

WMD retaliation, which in turn could escalate into a war so destructive it could easily destroy huge segments of the world's population. During the Cold War, this understanding became known as mutually assured destruction and was largely the reason war never broke out between the WMD-armed United States and Soviet Union. The only country to have used a nuclear weapon in war is the United States. There are eight countries that have declared they possess nuclear weapons and are known to have tested a nuclear weapon, only five of which are members of the NPT. The eight include: People's Republic of China; France; India; Pakistan; Russia; The United Kingdom; the United States of America; and North Korea. Israel is considered by most analysts to have nuclear weapons numbering in the low hundreds as well, but maintains an official policy of nuclear ambiguity, neither denying nor confirming its nuclear status.

Iran is suspected by western countries of seeking nuclear weapons, a claim that it denies. South Africa developed a small nuclear arsenal in the 1980s but disassembled them in the early 1990s, making it the only country to have fully given up an independently developed nuclear weapons arsenal. Belarus, Kazakhstan, and Ukraine inherited stockpiles of nuclear arms following the break-up of the Soviet Union, but relinquished them to the Russian Federation. Countries with access to nuclear weapons through nuclear sharing agreements include: Belgium, Germany, Italy, the Netherlands, and Turkey. North Korea has claimed to have developed and tested nuclear devices; although outside sources have been unable to unequivocally support the

state's claims, North Korea has officially been identified to have nuclear weapons.

United States politics

Due to the indiscriminate impact of WMDs, the fear of a WMD attack has shaped political policies and campaigns, fostered social movements, and has been the central theme of many films. Support for different levels of WMD development and control varies nationally and internationally. Yet understanding of the nature of the threats is not high, in part because of imprecise usage of the term by politicians and the media. Fear of WMD, or of threats diminished by the possession of WMD, has long been used to catalyze public support for various WMD policies. They include mobilization of pro- and anti-WMD campaigners alike, and generation of popular political support. The term WMD may be used as a powerful buzzword, or to generate a culture of fear.. It is also used ambiguously, particularly by not distinguishing among the different types of WMD.

A television commercial called *Daisy*, promoting Democrat Lyndon Johnson's 1964 presidential candidacy, invoked the fear of a nuclear war and was an element in Johnson's subsequent election. More recently, the threat of potential WMD in Iraq was used by President George W. Bush to generate public support for the 2003 invasion of Iraq. Broad reference to Iraqi WMD in general was seen as an element of President Bush's arguments. As Paul Wolfowitz explained: "For bureaucratic reasons, we settled on one issue, weapons of mass destruction, because it

was the one reason everyone could agree on." To date, however, Coalition forces have found mainly degraded artillery shells. On June 21, 2006, United States Senator Rick Santorum claimed that "We have found weapons of mass destruction in Iraq, chemical weapons."

According to the Washington Post, he was referring to 500 such shells "that had been buried near the Iranian border, and then long forgotten, by Iraqi troops during their eight-year war with Iran, which ended in 1988." That night, "intelligence officials reaffirmed that the shells were old and were not the suspected weapons of mass destruction sought in Iraq after the 2003 invasion or Iraq." The shells had been uncovered and reported on in 2004. In 2004 Polish troops found 17 1980s-era rocket warheads, thwarting an attempt by militants to buy them at $5000 each. Some of the rockets contained extremely deteriorated nerve agent.

Media coverage of WMD

In 2004 the Center for International and Security Studies at Maryland (CISSM) released a report examining the media's coverage of WMD issues during three separate periods: India's nuclear weapons tests in May 1998; the US announcement of evidence of a North Korean nuclear weapons program in October 2002; and revelations about Iran's nuclear program in May 2003. The CISSM report notes that poor coverage resulted less from political bias among the media than from tired journalistic conventions. The report's major findings were that:

Most media outlets represented WMD as a monolithic menace, failing to adequately distinguish between weapons programs and actual weapons or to address the real differences among chemical, biological, nuclear, and radiological weapons.

Most journalists accepted the Bush administration's formulation of the "War on Terror" as a campaign against WMD, in contrast to coverage during the Clinton era, when many journalists made careful distinctions between acts of terrorism and the acquisition and use of WMD.

Many stories stenographically reported the incumbent administration's perspective on WMD, giving too little critical examination of the way officials framed the events, issues, threats, and policy options.

Too few stories proffered alternative perspectives to official line, a problem exacerbated by the journalistic prioritizing of breaking-news stories and the "inverted pyramid" style of storytelling.

In a separate study published in 2005, a group of researchers assessed the effects reports and retractions in the media had on people's memory regarding the search for WMD in Iraq during the 2003 Iraq War. The study focused on populations in two coalition countries (Australia and USA) and one opposed to the war (Germany). Results showed that US citizens generally did not correct initial misconceptions regarding WMD, even following disconfirmation; Australian and German citizens were more responsive to retractions. Dependence on the initial source of information led to a substantial minority of Americans exhibiting

false memory that WMD were indeed discovered, while they were not. This led to three conclusions:

The repetition of tentative news stories, even if they are subsequently disconfirmed, can assist in the creation of false memories in a substantial proportion of people.

Once information is published, its subsequent correction does not alter people's beliefs unless they are suspicious about the motives underlying the events the news stories are about.

When people ignore corrections, they do so irrespective of how certain they are that the corrections occurred.

A poll conducted between June and September 2003 asked people whether they thought WMD had been discovered in Iraq since the war ended. They were also asked which media sources they relied upon. Those who obtained their news primarily from Fox News were three times as likely to believe that evidence confirming WMD had been discovered in Iraq than those who relied on PBS and NPR for their news, and one third more likely than those who primarily watched CBS.

Public perceptions of WMD

Awareness and opinions of WMD have varied during the course of their history. Their threat is a source of unease, security and pride to different people. The anti-WMD movement is embodied most in nuclear disarmament, and led to the formation of the Campaign for Nuclear Disarmament. In 1998 University of New

Mexico's Institute for Public Policy released their third report on US perceptions - including the general public, politicians and scientists - of nuclear weapons since the break up of the Soviet Union. Risks of nuclear conflict, proliferation, and terrorism were seen as substantial.

While maintenance of a nuclear US arsenal was considered above average in importance, there was widespread support for a reduction in the stockpile, and very little support for developing and testing new nuclear weapons. Also in 1998, but after the UNM survey was conducted, nuclear weapons became an issue in India's election of March in relation to political tensions with neighboring Pakistan. Prior to the election the Bharatiya Janata Party (BJP) announced it would “declare India a nuclear weapon state” after coming to power. BJP won the elections, and on May 14, three days after India tested nuclear weapons for the second time, a public opinion poll reported that a majority of Indians favored the country’s nuclear build-up.

On April 15, 2004, the Program on International Policy Attitudes (PIPA) reported that US citizens showed high levels of concern regarding WMD, and that preventing the spread of nuclear weapons should be "a very important US foreign policy goal", accomplished through multilateral arms control rather than the use of military threats. A majority also believed the US should be more forthcoming with its biological research and its Nuclear Non-Proliferation Treaty commitment of nuclear arms reduction, and incorrectly thought the US was a party to various non-proliferation treaties.

A Russian opinion poll conducted on August 5, 2005 indicated half the population believes new nuclear powers have the right to possess nuclear weapons. 39% believes the Russian stockpile should be reduced, though not fully eliminated.

Chapter 3

Radioactive Weaponry/hazard Symbol

Nuclear 9/11

The international radioactivity symbol (also known as trefoil) first appeared in 1946, at the University of California, Berkeley Radiation Laboratory. At the time, it was rendered as magenta, and was set on a blue background. It is drawn with a central circle of radius R, the blades having an internal radius of $1.5R$ and an external radius of $5R$, and separated from each other by 60°. It is meant to represent a radiating atom.

The International Atomic Energy Agency found, however, that the symbol is unintuitive and can be variously interpreted by those uneducated in its meaning, and that its role as a hazard warning was compromised as it did not clearly indicate "danger" to many non-Westerners and children who encountered it. As a result of research, a new radiation hazard symbol was developed to be placed near the most dangerous parts of radiation sources featuring a skull, someone running away, and using the color red rather than yellow as the background.

Nuclear weapons materials on the black market is a growing global concern, and a nuclear 9/11 could involve the detonation

of a small, crude nuclear weapon by a terrorist group, in a major U.S. city, with significant loss of life and property. On September 11, 2001, nineteen al Qaeda hijackers killed some 3,000 people and caused billions of dollars damage to New York City and the Pentagon.

This toll would be small compared with a *nuclear 9/11* — a nuclear attack launched by a terrorist group. Detonation of a crude strategic nuclear weapon in a major U.S. city could kill more than 500,000 people and cause more than a trillion dollars in damage:

Half a million people would be killed immediately. Hundreds of thousands would die from fallout, the resulting fires and collapsing buildings. Uncontrolled fires would rage for days and emergency services and hospitals would be completely overwhelmed.

Current risk

Large quantities of nuclear materials are inadequately secured in several countries, including Russia and Pakistan. Since 1993, there have been more than 1,300 reported incidents of illicit trafficking of nuclear materials, including plutonium and highly enriched uranium, both of which can be used as the basis for an atomic bomb. When enough stolen material had been collected, only a few specialists would be needed to construct a nuclear weapon, which could then be delivered by truck to the detonation point. Paul Williams, in his book *The Al Qaeda Connection*,

reports that Osama Bin Laden has already obtained nuclear weapons and smuggled them into the US through Mexico with the help of the MS-13 criminal group.

In 2004, Graham Allison, U.S. Assistant Secretary of Defense during the Clinton administration, wrote that “on the current path, a nuclear terrorist attack on America in the decade ahead is more likely than not". Also in 2004, Bruce Blair, president of the Center for Defense Information stated: "I wouldn't be at all surprised if nuclear weapons are used over the next 15 or 20 years, first and foremost by a terrorist group that gets its hands on a Russian nuclear weapon or a Pakistani nuclear weapon". In 2006, Robert Gallucci, Dean of the Georgetown University School of Foreign Service, estimated that “it is more likely than not that al Qaeda or one of its affiliates will detonate a nuclear weapon in a U.S. city within the next five to ten years".

As the United States proceeds with its war on terrorism, one of the darkest clouds hanging over the campaign is the question of whether the perpetrators of the Sept. 11 horrors could strike again, this time with nuclear weapons. It seems doubtful that U.S. intelligence can definitively answer this question. Absent perfect foresight, one can nonetheless outline some of the plausible threats and identify the range of U.S. responses that could reduce the exposure of citizens and troops to nuclear attack.

Threat Scenarios

The most accessible nuclear device for any terrorist would be a radiological dispersion bomb. This so-called 'dirty bomb' would consist of waste by-products from nuclear reactors wrapped in conventional explosives, which upon detonation would spew deadly radioactive particles into the environment. This is an expedient weapon, in that radioactive waste material is relatively easy to obtain. Radioactive waste is widely found throughout the world, and in general is not as well guarded as actual nuclear weapons.

In the United States, radioactive waste is located at more than 70 commercial nuclear power sites, in 31 states. Enormous quantities also exist overseas — in Europe and Japan in particular. Tons of wastes are transported long distances, including between continents. In Russia, security for nuclear waste is especially poor, and the potential for diversion and actual use by Islamic radicals has been shown to be very real indeed. In 1996, Islamic rebels from the break-away province of Chechnya planted, but did not detonate, such a device in Moscow's Izmailovo park to demonstrate Russia's vulnerability.

This dirty bomb consisted of a deadly brew of dynamite and one of the highly radioactive by-products of nuclear fission — Cesium 137. Extreme versions of such gamma-ray emitting bombs, such as a dynamite-laden casket of spent fuel from a nuclear power plant, would not kill quite as many people as died on Sept. 11. A worst-case calculation for an explosion in downtown Manhattan

during noontime: more than 2,000 deaths and many thousands more suffering from radiation poisoning. Treatment of those exposed would be greatly hampered by inadequate medical facilities and training.

The United States has only a single hospital emergency room dedicated to treating patients exposed to radiation hazards, at Oak Ridge, Tenn. A credible threat to explode such a bomb in a U.S. city could have a powerful impact on the conduct of U.S. foreign and military policy, and could possibly have a paralyzing effect. Not only would the potential loss of life be considerable, but also the prospect of mass evacuation of dense urban centers would loom large in the minds of policy-makers.

Attack on Nuclear Power Plants

A terrorist attack on a commercial nuclear power plant with a commercial jet or heavy munitions could have a similar affect to a radiological bomb, and cause for greater casualties. If such an attack were to cause either a meltdown of the reactor core (similar to the Chernobyl disaster), or a dispersal of the spent fuel waste on the site, extensive casualties could be expected. In such an instance, the power plant would be the source of the radiological contamination, and the plane or armament would be the explosive mechanism for spreading lethal radiation over large areas.

Diversion of Nuclear Material or Weapons

The threat from radiological dispersion dims in comparison to the possibility that terrorists could build or obtain an actual atomic bomb. An explosion of even low yield could kill hundreds of thousands of people. A relatively small bomb, say 15-kilotons, detonated in Manhattan could immediately kill upwards of 100,000 inhabitants, followed by a comparable number of deaths in the lingering aftermath.

Fortunately, bomb-grade nuclear fissile material (highly enriched uranium or plutonium) is relatively heavily guarded in most, if not all, nuclear weapon states. Nonetheless, the possibility of diversion remains. Massive quantities of fissile material exist around the world. Sophisticated terrorists could fairly readily design and fabricate a workable atomic bomb once they manage to acquire the precious deadly ingredients (the Hiroshima bomb which used a simple gun-barrel design is the prime example).

Russia

A primary source of diverted weapons or material could be Russia. No Russian bombs have been officially reported missing, and Russian authorities maintain that no nuclear material has been lost. Rather, the outstanding question is whether a bomb, or fissile material in sufficient quantity to make one, has disappeared without Moscow's knowledge. While few outside observers dispute this, none are privy to the raw data that could validate or refute the Russian claim. One concern long has been

the allegations voiced by the former Secretary of Russia's Security Council, Gen. Alexander Lebed. After conducting an exhaustive inventory of Russian nuclear weapons in the 1990s, he found that 84 "suitcase" nuclear bombs had vanished from the Russian arsenal.

The prevailing judgment among Western experts is that Russia may have lost track of the paper trail for any number of bombs, but that the bombs themselves probably have been dismantled or tucked away in storage, rather than having been stolen. The infamous Russian accounting system using hand receipts stored in shoe boxes provides ample grist for this theory. While there is no reason to doubt the sincerity of the Russian military and civilian leaders who have shouldered the custodial duties for Russian nuclear weapons, it is nonetheless possible that Russian nuclear security has been compromised from the inside without detection.

As noted, such a bomb could be transported to the United States inside one of the countless containers arriving at American ports every day. This avenue seems especially easy to arrange by bin Laden's *al Qaeda* network, which has extensive business connections around the world. Such a container could accommodate a good-sized atomic bomb, which could be detonated in a harbor. Or it could be unloaded and carted off in a small truck or van to any destination in the lower 48 states. Indeed, once unloaded from a ship, one of Russia's 'missing' suitcase bombs, which are thought to weigh some 60 pounds and

measure the size of a small refrigerator, practically could be carried as a back-pack by a strong person.

Disconcertingly, it is conceivable that Russia may have built even smaller bombs, comparable to the truly attaché-class atomic bomb secretly built by the United States in the late 1970s. This U.S. bomb design was so compact and lightweight that it could have been covertly transported as innocent hand-luggage by any reasonably strong individual. In fact, a replica — with proxy nuclear material and conventional explosives in place of the real stuff — was disguised as a briefcase, and actually hand-carried on commercial airline flights from California to Washington in the early 1980s.

Pakistan

Another potential source of diversion is the Pakistani nuclear arsenal, estimated to number around 30-50 atomic bombs with explosive yields ranging from 1 to 15 kilotons. The weapons are probably assembled at Wah (50 miles from Afghanistan), and are stored primarily at Sargodha near a missile complex close to the border with India and only about 250 miles from Afghanistan. Pakistan's military government is walking a tightrope between pressure from the Bush administration on one side and anti-American Islamic militants on the other. Growing street opposition from the latter could certainly de-stabilize or even topple the regime, and in the midst of such dissolution, the weakening of nuclear security would inevitably occur.

The ranks of government and military personnel are also fairly riddled with sympathizers of the radical Islamic faction, posing a distinct risk of insiders colluding to spirit away a bomb or two for bin Laden or other terrorists. In any case, control over Pakistan's arsenal could all too readily buckle in a serious crisis inside the country. Pakistani weapons are believed to lack sophisticated locks and other safeguards to prevent their unauthorized use. Loose nukes in the region would have unpredictable consequences, almost all of which would militate against the U.S. cause, not to mention the safety of U.S. forces dispatched there.

U.S. Responses

With such a panoply of possible threats, there are a number of actions that could be taken in the near term to shore up nuclear security.

Pakistan

The Pakistani situation, in particular, deserves careful monitoring — using surveillance and intelligence assets in the region. The U.S. government could urge Pakistani authorities to further consolidate and/or disable their nuclear devices, and beef up security around storage sites — and even offer security equipment and guards. In fact, the U.S. government should be prepared to provide arsenal security even without Islamabad's permission if emergency circumstances dictate. The U.S. government also could begin drawing up contingency plans to 'rescue' the arsenal if the need arises. U.S. Special Operations

forces should be kept on high alert for quick, covert insertion to the sites to disable or even re-locate weapons to prevent their capture by unauthorized persons. It must be noted, however, that inserting commandos on short notice to gain control over the arsenal would put them in considerable jeopardy, and disarming the weapons could be dangerous indeed. Pakistani weapons are believed to have quite primitive safety devices — they almost certainly lack the "one-point" safety design of U.S. weapons — which means that a Pakistani nuclear weapon could more easily detonate if subjected to conventional firefights between soldiers using grenades or similar munitions.

Therefore, it would be highly desirable for nuclear experts from the Department of Energy to accompany any military troops in such a scenario. DoE nuclear response teams, known as Nuclear Emergency Search Teams (NEST), are formed in a crisis from nearly 1,000 highly trained and knowledgeable individuals, and could be dispatched to the region to assist in locating and disarming any weapons. The teams and their equipment, some on alert staging out of Nellis Air Force Base in Nevada, know the design of Pakistani weapons, and could x-ray the weapons and devise a disabling procedure on the spot.

Compared to the military's commandos, these experienced civilian teams would stand a better chance of blowing up the triggering mechanisms on Pakistani weapons without causing the bomb to go off. Another option for response in a crisis would be for such a joint military-civilian insertion mission to link up with a Russian counterpart to conduct search and disable missions

together in the region. The mutual benefits would be considerable, and such a joint U.S.-Russian operation would have lasting positive effects on future cooperation.

Russia

Joint operations between Russia and the United States could also be undertaken inside Russia itself to deal with a nuclear crisis. Russia's crack "Vympel" nuclear counter-terrorist commando units could work closely with U.S. Special Operations forces, augmented with a bilateral NEST group to respond to emergencies requiring the securing and disposing of real or dirty nuclear bombs. Tactical operational cooperation could be further enhanced by breaking new ground in intelligence sharing.

The likelihood that the Russian mafia would be involved in aiding terrorists in any theft of atomic or radiological bombs suggests that joint intelligence should also focus on criminal organizations in Russia. This is primarily a mission for the FBI/CIA and its Russian counterparts, but some joint military intelligence could also be necessary in emergency tactical situations. The pivotal role of Russia in the arena of 'loose nukes' and terrorism highlights the wisdom of the Cooperative Threat Reduction Program undertaken by the United States during the past decade.

Popularly known as the Nunn-Lugar program, after its original congressional sponsors, this effort has significantly strengthened the security of Russian nuclear weapons and fissile materials, as well as throughout the former Soviet Union. However, there is a

long way to go to bring Russian nuclear security up to international standards. Much more effort and resources need to be devoted to securing Russian nuclear weapons in storage at 123 sites in Russia, and nuclear waste that could be fashioned into radiological bombs. The reach of Nunn-Lugar has been limited, in part because of disagreements between the parties about access to facilities and sites.

It is now clear that Russia and the United States should work harder to overcome their differences and press ahead with the Nunn-Lugar agenda. A long list of priorities for the future can be drawn from some excellent studies of the program's strengths and weaknesses; for example, several recent efforts by the Russian American Nuclear Security Advisory Council (RANSAC).

Within the United States

The first steps to mitigate the possibility of nuclear terrorism would be serious and rapid effort to build intelligence capabilities that might warn of a potential attack, and as explained above, to take actions aimed at shoring up possible sources of nuclear material. In the meantime, increased monitoring at ports also must continue and be intensified, despite the negative ramifications on international trade. Inspection of containers up to Sept. 11 has been rather cursory, and infrequent.

This is changing, just as already the U.S. government and airlines are scrambling to beef up airline and airport security. Some of the additional security measures would include those

exported to Russia under the Nunn-Lugar program. A prime example is the transfer of nuclear materials detectors to Russia, which were then emplaced at strategic border crossings, ports and airports to detect diversion. The U.S. government might consider the use of such equipment at similar American locations, particularly ports, as a method to detect and intercept materials being smuggled into the country.

In addition, there are a number of methods to increase security around nuclear power plants that already are being discussed by U.S. authorities and nuclear plant operators, such as expanding the perimeters of restricted airspace. Such measures should be implemented as rapidly as possible. Finally, NEST operations would go into effect if a credible threat of a dirty bomb or a full-fledged nuclear weapon were to manifest itself. If the information available would allow the U.S. teams to locate the city affected, hundreds of team members would fan out along a matrix of the threat region to detect the bomb.

Carrying gamma- and neutron-detectors inside carrying cases to preserve secrecy, the NEST members would cover the suspect area on foot, in vans and helicopters — going in and out of buildings hoping to register the tell-tale signals of a hidden bomb. Once found, the bomb is x-rayed, "sniffed" and otherwise analyzed to determine its characteristics. Obviously, intelligence that helps localize the bomb is the main key to success. Just as obviously, intelligence of such quality is seldom available — as proven on Sept. 11. Such a search could be truly looking for a

needle in a haystack, as detection normally would succeed only if the detectors come within a few feet or so of the hidden bomb.

Disabling a bomb is easy by comparison. A radiological bomb might be surrounded by a tent enclosure several tens of feet in height and width, then filled with a special foam to contain the deadly radioactive material (such as Cesium 137) if the bomb explodes during further defusing attempts. For a nuclear device, a set of options for disabling the weapon are available including using explosives to wreck the bomb's wiring to prevent the triggering of the nuclear detonators. Because of the difficulty inherent in finding a nuclear weapon once it entered the country, near-term U.S. response efforts would be best focused on prevention and intervention to secure possible sources of nuclear terrorism.

Nuclear terrorism and dirty bombs

Nuclear threats or terrorists use of nuclear weapons or highly active radiation sources has become a possibility and needs to be addressed also in WHO’s response to radiation events. Such threats include:

- Dispersal of highly radioactive materials by means of "dirty bombs"
- Contamination of drinking water or food supplies with highly radioactive materials..
- Direct attacks on nuclear power plants or nuclear fuel reprocessing facilities.

- Use of nuclear weapons by countries.
- Locating radioactive sources in heavily populated areas

A "dirty bomb" combines conventional explosives, such as dynamite, with radioactive materials packed around the explosive core. The idea is to spread radioactive material into the area around the explosion and frighten people. Indeed, the main damage from a dirty bomb would be associated with the blast itself, while contamination with radioactive materials to people or the environment is expected to cause only limited harm.

Chapter 4

Combating Nuclear Terrorism

The Global Initiative

U.S. President Bush and former Russian President Putin launched the Global Initiative to Combat Nuclear Terrorism on July 15, 2006 in St. Petersburg, Russia to expand and accelerate the development of partnership capabilities to prevent, detect, and respond to the global threat of nuclear terrorism. On October 30-31, 2006, representatives from 13 governments met in Rabat, Morocco and reached agreement on a Statement of Principles, as well as a Terms of Reference for Implementation and Assessment. The International Atomic Energy Agency was invited to serve as an observer to the Initiative. In two short years, the Global Initiative has matured and garnered support from 75 partners, including all European Union members, and the EU as an observer.

The Global Initiative goals:

- Bring together experience and expertise from the nonproliferation, counter proliferation, and counterterrorism disciplines.
- Integrate collective capabilities and resources to strengthen the overall global architecture to combat nuclear terrorism.

- Provide the opportunity for nations to share information and expertise in a legally non-binding environment.

By endorsing the Global Initiative to Combat Nuclear Terrorism, partners are providing their political support and commitment to strengthening and implementing the Statement of Principles. The Initiative is open to nations that share in its common goals and are actively committed to combating nuclear terrorism on a determined and systematic basis. Partners implement the Principles by conducting various multilateral activities, workshops, and table-top and field exercises.

Reasons for controversy

The modern definition of terrorism is inherently controversial. The use of violence for the achievement of political ends is common to state and non-state groups. The difficulty is in agreeing on a basis for determining when the use of violence (directed at whom, by whom, for what ends) is legitimate. The majority of definitions in use have been written by agencies directly associated with a government, and are systematically biased to exclude governments from the definition. Some such definitions are so broad, like the Terrorism Act 2000, as to include the disruption of a computer system wherein no violence is intended or results.

The contemporary label of "terrorist" is highly pejorative; it is a badge which denotes a lack of legitimacy and morality. The

application "terrorist" is therefore always deliberately disputed. Attempts at defining the concept invariably arouse debate because rival definitions may be employed with a view to including the actions of certain parties, and excluding others. Thus, each party might still subjectively claim a legitimate basis for employing violence in pursuit of their own political cause or aim.

United Nations

While the United Nations has not yet accepted a definition of terrorism, the UN's "academic consensus definition," written by terrorism expert Alex P. Schmid and widely used by social scientists, runs:

Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby — in contrast to assassination — the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperilled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought.

UN short legal definition, also proposed by Alex P. Schmid: an act of terrorism is the "peacetime equivalent of a war crime."

On March 17, 2005, a UN panel described terrorism as any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act."

The General Assembly resolution 49/60, adopted on December 9, 1994, contains a provision describing terrorism:

European Union

The European Union employs a definition of terrorism for legal/official purposes which is set out in Art. 1 of the *Framework Decision on Combating Terrorism* (2002). This provides that terrorist offences are certain criminal offences set out in a list comprised largely of serious offences against persons and property which;

"given their nature or context, may seriously damage a country or an international organisation where committed with the aim of: seriously intimidating a population; or unduly compelling a Government or international organisation to perform or abstain from performing any act; or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation."

United States

The United States has defined terrorism under the Federal Criminal Code. Chapter 113B of Part I of Title 18 of the United States Code defines terrorism and lists the crimes associated with terrorism. In Section 2331 of Chapter 113b, terrorism is defined as:

...activities that involve violent... or life-threatening acts... that are a violation of the criminal laws of the United States or of any State and... appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and... (C) occur primarily within the territorial jurisdiction of the United States... [or]... (C) occur primarily outside the territorial jurisdiction of the United States..."

Edward Peck, former U.S. Chief of Mission in Iraq (under Jimmy Carter) and ambassador to Mauritania:

In 1985, when I was the Deputy Director of the Reagan White House Task Force on Terrorism, they asked us this is a Cabinet Task Force on Terrorism; I was the Deputy Director of the working group they asked us to come up with a definition of terrorism that could be used throughout the government. We produced about six, and each and every case, they were rejected, because careful reading would indicate that our own country had been involved in some of those activities. After the task force

concluded its work, Congress got into it, and you can google into U.S. Code Title 18, Section 2331, and read the U.S. definition of terrorism. And one of them in here says — one of the terms, "international terrorism," means "activities that," I quote, "appear to be intended to affect the conduct of a government by mass destruction, assassination or kidnapping." Yes, well, certainly, you can think of a number of countries that have been involved in such activities. Ours is one of them. Israel is another. And so, the terrorist, of course, is in the eye of the beholder.

United Kingdom

The United Kingdom defined acts of terrorism in the Terrorism Act 2000 as the use of threat of action where:

- the action falls within subsection (2),
- the use or threat is designed to influence the government or to intimidate the public or a section of the public and
- the use or threat is made for the purpose of advancing a political, religious or ideological cause.

(2) Action falls within this subsection if it

- involves serious violence against a person,
- involves serious damage to property,
- endangers a person's life, other than that of the person committing the action,

- creates a serious risk to the health or safety of the public or a section of the public or
- is designed seriously to interfere with or seriously to disrupt an electronic system.

Laws and government agencies

U.S. Code of Federal Regulations: "...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives"

Current U.S. national security strategy: "premeditated, politically motivated violence against innocents."

United States Department of Defense: the "calculated use of unlawful violence to inculcate fear; intended to coerce or intimidate governments or societies in pursuit of goals that are generally political, religious, or ideological."

USA PATRIOT Act: "activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state, that (B) appear to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping, and (C) occur primarily within the territorial jurisdiction of the U.S."

The U.S. National Counter Terrorism Center (NCTC) described a terrorist act as one which was: "premeditated; perpetrated by a subnational or clandestine agent; politically motivated, potentially including religious,

The potential for Nuclear Terrorism

Since the September 11 attacks on New York and Washington, concerns about the potential for nuclear terrorism have risen dramatically. The consequences of an act of nuclear terrorism would be devastating in many respects — human, social, psychological, economic, and political. Recent news reports have raised alarms. The Times of London reported in late October that one of the four airliners hijacked on September 11, the United Airlines flight that crashed in a Pennsylvania field, may have been headed for a nuclear power plant in that state, possibly the Three Mile Island facility.

The arrest and questioning by Pakistani authorities of three leading Pakistani scientists, two of them veterans of Pakistan's nuclear weapons program, with known sympathies for the Taliban, has raised concerns about the transfer of nuclear know-how or even nuclear materials to that regime or Osama bin Laden's Al Qaeda organization.

Long-standing concerns over the security of nuclear weapons and fissile materials in the former Soviet Union, and the whereabouts

of former Soviet weapons scientists are once again at the fore. Osama bin Laden has stated that acquiring nuclear weapons is a "religious duty" and the International Atomic Energy Agency has concluded that Al Qaeda is "actively seeking" an atomic bomb. Testimony by Jamal Ahmad al-Fadl, a former bin Laden associate, in the trial of those convicted in the 1993 World Trade Center bombing, recounted al-Fadl's extensive but unsuccessful efforts to acquire enriched uranium for Al Qaeda. Nuclear terrorism could take many forms, any one of which would be a disaster by any measure. But some would be potentially more devastating than others.

In this, International Physicians for the Prevention of Nuclear War (IPPNW), recipient of the 1985 Nobel Peace Prize, summarizes four of the scenarios that comprise the nuclear terrorist threat and concludes with some recommendations on how to prevent nuclear terrorism.

Types of Nuclear Terrorism

Each scenario has significant, if not enormous, public health implications and would, as in the case of the anthrax outbreak, place doctors and health professionals on the front lines of any attempted response. It is likely that many of these scenarios would immediately outstrip the abilities of even the most sophisticated and well-equipped national health system to respond.

Radiological Dispersion Weapons

From a technical perspective, a radiological dispersion weapon (often referred to in media reports as a "dirty bomb") would be the simplest for a terrorist to make and use. It would also be an effective weapon of terror. Severe disruptions would result from the widespread fear of radioactive contamination, and long-term health effects, particularly increased cancer deaths, would result. Low-level radioactive wastes, such as medical waste and some of the by-products of nuclear power generation, are abundant and relatively unsecured.

Using conventional explosives, such materials could be disseminated over a wide area causing panic, illness, and contamination that could cost billions to clean up. Bruce Blair, a nuclear weapons expert who now heads the Center for Defense Information in Washington, DC, estimates that a casket-sized radiological dispersion weapon loaded with spent fuel from a nuclear power plant and detonated in New York City at mid-day would cause 2,000 immediate deaths and injure thousands more, overwhelming medical facilities ill-equipped to manage a large number of radiation-related casualties. Of course, the amount of radioactive material, the amount of explosive, and the time and place of detonation could vary greatly.

An even more lethal radiological weapon could be made using the fissile materials needed for a nuclear weapon — highly enriched uranium (HEU) or plutonium. Even without building a device capable of creating a nuclear explosion, the dispersal of such

highly radioactive and lethal materials using a conventional explosive would be extraordinarily deadly. Although obtaining HEU or plutonium would be more difficult than obtaining low-level radioactive wastes, it is well known that Al Qaeda has on several occasions sought to purchase such material, believed to originate in the former Soviet Union (FSU).

Concern about the quality of safeguards for protecting HEU and plutonium in the FSU is widely shared by governments and non-governmental organizations working on nuclear proliferation issues. *Buying or Stealing a Nuclear Weapon* All of the technical and logistical obstacles involved in building a nuclear weapon can be avoided if a terrorist organization is able to procure an existing nuclear weapon. One especially disturbing scenario involves so-called “suitcase” bombs—compact one-kiloton nuclear weapons—made by the Soviet Union in the 1970s. There have been conflicting reports about whether all of these weapons are accounted for, and some concern that such weapons may have been sold by profiteers in the wake of the Soviet Union's collapse in the 1990s.

Some experts have suggested that the technical expertise of a Soviet scientist familiar with their construction would be required for detonation, and there is some question about whether such weapons would even work after decades without maintenance. But the unknowns about such mini-nukes, combined with their portability, are cause for deep concern. Procurement of an existing nuclear weapon from Pakistan is also a concern. Thought to weigh about 1,500 pounds each, but small

enough to fit inside a shipping container or truck, Pakistan's small nuclear arsenal is believed to comprise about 20 Hiroshima-sized (15-kiloton range) bombs. IPPNW's 1999 study Bombing Bombay?

Effects of Nuclear Weapons and a Case Study of a Hypothetical Explosion estimated that the explosion of a 15-kiloton nuclear weapon in Bombay would cause between 160,000 and 866,000 deaths, depending on where in the city the bomb was detonated. The Pakistani military, its intelligence services, and its nuclear establishment are known to be salted with supporters of the Taliban regime in Afghanistan and supporters of Osama bin Laden. Should social and religious unrest in Pakistan result in the overthrow of the Musharraf regime in favor of a fundamentalist government, there is concern that Pakistani nuclear weapons could fall into the hands of Al Qaeda.

Pakistan's nuclear weapons are known to lack many of the technical safeguards needed to prevent unauthorized detonation. A Hiroshima-sized nuclear bomb, though small by modern standards, is capable of killing hundreds of thousands of people or even more in an urban area and causing massive casualties in the aftermath from radiation sickness, epidemics, and contamination of water and food supplies. *Building a Nuclear Weapon* It is widely recognized that the highest hurdle for any nation or sub-national group seeking to build a nuclear weapon is obtaining the fissile materials needed to do so. There are vast quantities of such material in the world, but only a football-sized amount of the material, weighing perhaps 20 pounds or so, would

be sufficient. The Nonproliferation Policy Education Center estimates that there may be as much as 20 tons of "surplus" plutonium and 500 tons of "surplus" HEU in the former Soviet Union alone. There is considerable concern that Osama bin Laden could have obtained such materials from sympathizers within the Pakistani nuclear, intelligence, and/or military establishments, or from rogue elements of the Russian military or organized criminal elements in the FSU. The remaining materials required to construct a bomb are readily obtainable.

Indeed, according to Theodore Taylor, once one of the leading nuclear scientists in the United States, a knowledgeable nuclear scientist could do so with materials that could be purchased at a hardware store. Such a bomb would likely have an unpredictable yield. But even a so-called "fizzle yield" bomb (that is, a bomb packing the power of about 1,000 tons of TNT) would be powerful enough to level several city blocks and disperse radiation over a large area.

Key conclusions reached by IPPNW in its 1996 study *Crude Nuclear Weapons: Proliferation and the Terrorist Threat* are still valid today. Among them:

- A determined sub-national group can fabricate a simple and crude, yet highly lethal, nuclear device if it can obtain 28 pounds of HEU or as little as 18 pounds of plutonium.
- The break-up of the Soviet Union and the proliferation of nuclear technology has made the fissile materials

needed to make crude nuclear devices more accessible, removing one of the greatest obstacles to terrorists.

- Use of a crude nuclear device could kill and injure tens of thousands of people and cause massive social disruption and panic. Medical services would be overwhelmed by the injured.

Nuclear Power Plants and Nuclear Weapons Facilities

There are approximately 100 nuclear power stations in the United States (in 31 states) and dozens of other sites that are, or were, part of the US nuclear weapons production complex. Targeting such a site for terrorism requires none of conditions described above to produce radiation or nuclear weapons and presents none of the hurdles for acquiring or building a nuclear weapon. In mock exercises to test security at nuclear power plants before September 11, the failure rate was about 50 percent.

These tests were designed to test defenses against theft of nuclear materials and sabotage. Detailed information about the design and layout of US nuclear facilities, as well as their structural flaws and security weaknesses was widely available on the Nuclear Regulatory Commission (NRC) website before September 11. It has since been removed. After September 11, the NRC admitted that it had never considered the possibility that an airliner loaded with jet fuel might be used as a missile to try and destroy a nuclear power plant and that the effects of the impact of such a missile on a nuclear reactor's containment structure was not known.

What is known is that the breach of such a containment structure would be a major disaster on the scale of Chernobyl where the long-term health effects are still being measured and a huge area surrounding the plant remains uninhabitable. According to the Union of Concerned Scientists, a successful attack on the Indian Point nuclear power plant north of New York City could contaminate areas up to 100 miles away and require the evacuation of 20 million people, a practical impossibility. The long-term health effects would be staggering. According to David Kyd, a spokesman for the International Atomic Energy Agency, "a deliberate hit of that sort [an airliner loaded with fuel] is something that was never in any scenario at the design stage [of nuclear power plants].

These are vulnerable targets and the consequences of a direct hit could be catastrophic." Another related problem is the regular transport of low-level, high-level, and transuranic nuclear waste through major population centers by truck and by rail throughout the United States. Such transport provides tempting targets of opportunity for terrorists. What Must Be Done Efforts by the international community to contain the proliferation of nuclear weapons have not succeeded.

The Nuclear Non-Proliferation Treaty (NPT) of 1970 commits the officially recognized nuclear powers that signed the treaty (the US, the USSR, China, France, and the UK) to elimination of their nuclear arsenals in exchange for a promise from the non-nuclear states to refrain from acquiring nuclear weapons. Since the treaty was signed, many nations have acquired nuclear weapons or

made significant efforts to acquire them. This was perhaps inevitable in a world in which handful countries continued to insist that nuclear weapons were essential for their own national security, while they sought to keep other nations from coming to the same conclusion.

In short, the promise central to the NPT has not been kept. Whether the world is fortunate enough to pass through the current crisis, and crises to come, without an act of nuclear terrorism or the use of nuclear weapons by a state, there can be no higher priority for the international community than to reckon with the implications of nuclear weapons and nuclear proliferation by taking immediate and forceful steps to reduce the threat of nuclear weapons use.

Prevention will require a multi-faceted international effort that must include at least the following steps:

- A ban on the manufacture, transfer and sale of fissile materials.
- Establishment of international standards for the disposal and safeguarding of even low level radioactive wastes.
- Bringing all fissile materials under strict international control and safeguards with a rigorous system of accounting and international inspections.
- Increase funding for joint Russian-American programs already underway to help secure Russia's sprawling nuclear weapons complex. (Ironically, just prior to the

September 11 attacks the Bush Administration proposed to cut $100 million from the Russian-American Cooperative Threat Reduction Program which seeks to secure nuclear materials in the FSU.)

- Entry into force of the Comprehensive Test Ban Treaty (CTBT) long viewed by the international community as an essential step in halting the proliferation of nuclear weapons. This will require a reversal of the Bush Administration's policy of opposing the CTBT, and a change in direction by the US Senate which refused to ratify the CTBT during the Clinton Administration.
- Deep reductions in existing nuclear arsenals as a signal that the major nuclear powers, particularly Russia and the United States, will take more seriously the commitment made in the NPT to eliminate nuclear weapons. It is essential that nuclear weapons be de-legitimized as instruments of military and political power.
- Diversion of the billions of dollars to be spent on missile defense to programs designed to counter the far more immediate and real threat of nuclear terrorism, including programs to secure fissile materials, purchase and destroy or render unusable all known stocks of HEU and plutonium, monitor and detect the illicit trade in nuclear materials and technology, deter the illicit international transport of nuclear weapons of any type, and provide meaningful employment for nuclear weapons scientists from the FSU.

- Increase security measures around all nuclear power plants and other nuclear facilities, which represent major potential sources for nuclear proliferation and targets for would-be nuclear terrorists. Cease construction of all new nuclear power facilities and begin phasing out the approximately 430 plants still in operation.
- An international convention on nuclear terrorism based on a proposal by Russia in the United Nations that would define offenses deemed to be acts of nuclear terrorism, mandate sharing of information related to potential acts of nuclear terrorism among states, provide for extradition and prosecution measures for those perpetrating acts of nuclear terror, and establish standards for the handling of radioactive material, devices, or facilities seized following the commission of an offense.
- The negotiation of a Nuclear Weapons Convention (NWC), a treaty to ban the development, testing, production, stockpiling, transfer, use, and threat of use of nuclear weapons.

It is often argued that existing and proposed international treaties are useless against terrorist organizations such as Al Qaeda. But, as The Economist recently editorialized, "On the contrary, [treaties] establish the norms that make its [the terrorist organization's] threatened actions a crime. And Mr. Bin Laden is no Dr. No, with lavish weapons laboratories of his own; whatever he does have has been filched, one way or another, from

government-run programs." In short, the best hope for preventing nuclear terrorism lies with changing the behavior of the states that are the source, wittingly or through neglect, of the tools of nuclear terror.

Today's Threats

Terrorism and the proliferation of weapons of mass destruction, including the danger that terrorists may succeed in their effort to acquire these incredibly lethal weapons, represents the defining threat of our age. Irresponsible states are pursuing the capacity for weapons of mass destruction. North Korea has conducted a nuclear test, launched long-range ballistic missiles, and engaged in the proliferation of ballistic missiles and nuclear capabilities to other rogue states. Iran continues to support terrorist group, to engage in sensitive nuclear activities in defiance of United Nations Security Council resolutions, and to aggressively develop ever more capable ballistic missiles.

Syria also sponsors terrorism and came very close to completing a clandestine nuclear reactor, in violation of its IAEA obligations, that appeared designed specifically to produce plutonium for nuclear weapons. As these repressive governments pursue weapons of mass destruction and missile delivery systems, responsible states in their regions may be tempted to pursue their own weapons programs in self-defense, raising the specter of a cascade of proliferation. Clearly, the Nonproliferation Treaty regime that has served us well for almost 40 years is under great

strain. Severe though the threat from state proliferation is, the one from non-state actors is equally daunting. On the supply end, despite our success in shutting down the A.Q. Khan network and in strengthening international tools against non-state proliferators, many continue to ply their deadly trade wherever and whenever they can, through both illicit activities and manipulation of the legitimate worldwide economic and financial system.

We also continue to work hard to deal with the aftermath of Khan's activities through support for prosecutions of key network figures by a range of countries and other efforts to mitigate the threat posed by the spread of equipment and knowledge by that network. Meanwhile, on the consumer end of the supply chain, terrorist groups continue to seek weapons of mass disruption or mass destruction, including the ultimate threat of nuclear weapons. That threat would only be compounded if leading state supporters of terrorism like Iran or Syria succeed in their own proliferation efforts.

The Response

The terrorist attacks on September 11 underscored the new threats we face and that the institutions of the Cold War were not sufficient to provide security. Nowhere is that more evident than in meeting the threat posed by proliferation of WMD and terrorism. We have strengthened long-standing nonproliferation tools like the International Atomic Energy Agency and assistance programs to reduce and secure weapons of mass destruction,

related materials and technologies. We have also made new use of traditional international instruments, enlisting them for the first time in the fight against weapons of mass destruction proliferation and terrorism.

United Nations Security Council Resolution 1540, the strong Council resolutions against Iran's and North Korea's programs, and the General Assembly's International Convention for the Suppression of Acts of Nuclear Terrorism, are good examples. Finally and most notably, we have developed new instruments, such as the Proliferation Security Initiative, the G-8 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, and the Global Initiative to Combat Nuclear Terrorism. Under their auspices, the vast majority of the international community has united to counter proliferation and nuclear terrorism through innovative action that takes advantage of existing legal authorities and growing cooperative relationships.

Despite that progress, much more remains to be done by the international community to prevent irresponsible states and terrorists from acquiring and using weapons of mass destruction. We must continue to strengthen existing tools and develop new ones. We must also recognize that proliferation is truly a global threat; no region is immune.

In countering the threats posed by WMD proliferation and potential terrorist use of these weapons, we need to employ a systematic approach of "defense in depth" involving:

- Securing the potential sources of weapons of mass destruction;
- Dismantling the facilitating networks that could supply dangerous weapons to rogue states and terrorists;
- Interdicting illicit transfers of dangerous weapons, materials, technology and knowledge as they move through the avenues of global commerce: land, sea, air and cyberspace;
- Disrupting terrorist efforts to acquire WMD materials and to turn them into weapons of terror;
- Strengthening our defenses against a potential WMD attack; and
- Deterring the use of these weapons against any of our nations.

Reducing and Securing Weapons of Mass Destruction

At the end of the Cold War, former Soviet weapons of mass destruction, materials and expertise appeared to present the greatest proliferation threat. Through the U.S. programs initially sponsored by Senators Nunn and Lugar, and subsequently through partners' efforts under the G-8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction, the United States, Russia and other partners have marked major achievements in reducing former Soviet weapons of mass destruction, delivery systems and related materials, and securing those which remain. The United States and Russia are on track to meet the goals set in 2005 by Presidents Bush and Putin at Bratislava, to complete security upgrades at all

identified Russian nuclear warhead and fissile material facilities by the end of this year.

Since its inception in 2002 at Kananaskis, the G-8 Global Partnership has been central to expanding and accelerating our work to reduce, and prevent the proliferation of, former Soviet weapons of mass destruction, related materials, equipment and expertise. While that work is not yet finished, the Global Partnership must now address global WMD threats. Expanding the scope of the Global Partnership to address WMD threats worldwide is among our highest nonproliferation priorities for the upcoming G-8 Summit.

By doing so, the G-8 will provide concrete resources toward our shared objective to fight terrorism and proliferation around the world, including our commitments under the Global Initiative to Combat Nuclear Terrorism and United Nations Security Council Resolution 1540. We hope that the G-8 Leaders will explicitly expand the Partnership at next month's Summit, so that we can work together in 2009, under Italy's G-8 leadership, to attract new Global Partnership partners and resources and to better coordinate our global activities.

As its name implies, the U.S. Global Threat Reduction Initiative (GTRI) is already very active in reducing and securing nuclear and radiological materials worldwide. GTRI has returned to Russia over 500 kilograms of Soviet-origin highly enriched uranium from vulnerable sites around the world. It has also shut down four civilian research reactors using highly-enriched

uranium, and converted another 13 to operate on low-enriched uranium. Further, GTRI has upgraded physical security at 600 facilities in over 40 countries that contain high-risk radioactive material, containing over 9 million curies.

In addition to securing nuclear and radiological materials at their source, we are also working with other nations to improve our capability to detect and therefore better prevent illicit trafficking in nuclear materials through programs like the Second Line of Defense, which has put in place detectors along the southern tier of the former Soviet Union, and the Megaports and Container Security Initiatives, which put detectors at major ports. We have also deployed nuclear material detectors at ports, airfields, and land crossings into the U.S.

As an increasing number of states turn to nuclear energy in light of the growing cost of other energy sources and growing concerns about avoiding greenhouse gas emissions, we must play an active role to ensure that states pursuing the economic and environmental benefits of peaceful nuclear energy are moving forward in a manner that does not increase proliferation risks.

Almost one year ago, Presidents Bush and Putin issued a Joint Declaration on Nuclear Energy and Nonproliferation that aims at assisting states to acquire safe, secure nuclear power, encouraging proliferation-resistant nuclear technologies, and presenting viable alternatives to the spread of enrichment and reprocessing. Ambassador Berdennikov has been working closely with the U.S. Special Envoy for Nuclear Nonproliferation,

Ambassador Jackie Wolcott, to implement the ideas set forth in the Joint Declaration.

A key element in this effort is persuading states not to pursue enrichment and reprocessing. In this regard, the United States, Russia, other partners, and the IAEA are all working on means to ensure reliable access to nuclear fuel should there be a disruption in supply – in order to encourage states to choose the international fuel market in lieu of acquiring indigenous enrichment and reprocessing technologies. The United States recently signed Memoranda of Understanding with Jordan, Bahrain, the United Arab Emirates, and Saudi Arabia, in which each of those governments set themselves as counter-examples to Iran by expressing their intent to choose the international market rather than pursue enrichment and reprocessing. We are also seeking to set tough criteria on enrichment and reprocessing transfers at the Nuclear Suppliers Group.

Stymieing Proliferation

A key requirement for the international community is to interdict proliferation shipments before they reach their intended destination. A landmark in that effort was the creation five years ago of the Proliferation Security Initiative (PSI). As you know, PSI is designed to be a flexible complement to formal treaties and nonproliferation regimes.

In five years, PSI has grown substantially — both in terms of the number of nations participating and in the depth and

sophistication of activities. Just last month, I was pleased to host a meeting of the group in Washington, which included over 90 partner nations. A declaration was adopted that notes the developments of the last five years and reaffirms the commitment of the PSI participating states to respond to new proliferation challenges. These meetings also served to share information about the PSI and revitalize states' active participation in it.

Since its inception, PSI partner nations have successfully conducted dozens of interdictions of sensitive materials for nuclear, chemical, and biological weapons and ballistic missiles en route to countries like Iran and Syria. And they have done so in a manner that is consistent with national legal authorities and relevant international law and frameworks. PSI nations continue to build the capacity of partners to act in a coordinated fashion. For example, PSI partners have conducted 35 exercises involving over 70 nations to improve interdiction capabilities around the world.

Much PSI activity is very quiet; successful interdictions are usually not publicized. A major exception was the October 2003 interdiction of the BBC China, carrying A.Q Khan-supplied centrifuge components destined for Libya. That cooperation, involving the United States, United Kingdom, Germany and Italy, was an important factor leading to Libya's abandonment of its weapons of mass destruction and longer-range missile programs and to the dismantling of the A.Q. Khan proliferation network. Today, Libya has come full circle abandoning WMD and long-

range ballistic missiles as well as support for terror. In fact, Libya is now a participant in PSI.

The activities of the A.Q. Khan network also highlighted the importance of global economic, financial and law enforcement action to counter the global sources of support to proliferation. One response was United Nations Security Council Resolution 1540, requiring all member states to criminalize proliferation by non-state actors and to adopt and enforce effective export controls. The recent renewal of Resolution 1540 for another three years, with a focus on international financial transactions, demonstrates its continued importance.

In Resolutions 1718, 1737, 1747 and 1803, the Security Council has also acted to deny international financing to North Korea's and Iran's WMD and missile programs. The United States and several friends and allies have also taken firm national action to disrupt the financial flows that feed proliferation. With the adoption of Executive Order 13382 in 2005, the President authorized targeted financial sanctions against proliferation networks, modeled on those against terrorist networks. To date, the United States has designated 52 entities and 12 individuals under this Executive Order.

Countering Nuclear Terrorism

Recognizing the need for a multilateral approach to countering the threat of nuclear terrorism, Presidents Bush and Putin launched the Global Initiative to Combat Nuclear Terrorism in

July 2006. Less than two years later, the Initiative has grown to include 73 partner nations, including all 27 member nations of the EU, as well as both the IAEA and EU as observers. Member states are committed – on a voluntary basis – to countering nuclear terrorism by building partner-nation capacity across the elements of physical protection, detection, search and confiscation, denial of safe haven, law enforcement, response, and investigation.

The private sector controls and operates the bulk of the facilities and technology for the movement of people and material around the globe. This supply chain includes airports, ports, railroads, telecommunications, banking and finance networks and other key infrastructure that terrorists might exploit. In Madrid, we hosted a panel with private-sector and local government representatives on ways to integrate the private sector into ongoing efforts to combat nuclear terrorism through a variety of activities. Partner nations agreed to develop additional plan of work activities and exercises that promote private-sector cooperation with national, state, and local governments in combating nuclear terrorism.

Looking ahead, the partner nations will expand the counterterrorism work of the Global Initiative. Morocco has done excellent work in the Global Initiative on denial of terrorist safe haven and countering the root causes of terrorism. Partner nations in Madrid committed to deepening participation by further integrating the counter proliferation and counterterrorism communities. Partner nations will also strive to develop

additional robust capabilities for attribution, nuclear forensics, and detection of nuclear materials.

Defending Against WMD Proliferation and Nuclear Terrorism

Even as we expend maximum effort at denying irresponsible states and terrorists access to nuclear and other weapons of mass destruction, we must be prepared to defend ourselves if they should succeed. Improved chemical and biological defenses are essential. Another central requirement to defend against potential WMD attack is effective missile defenses. Such defenses discourage proliferation, give us an important tool to deter a WMD attack delivered by missile, and give us a means to defeat an attack if necessary.

The number of states possessing ballistic missiles has nearly tripled in the last three decades, from nine in 1972 to over two dozen today. The presence of missile defenses undermines the ability of irresponsible states to use the threat of ballistic missile attack to coerce states and actually makes it far less likely that an adversary would ever use missiles during a conflict. We are working closely with NATO, and particularly with Poland and the Czech Republic, to augment cooperation on missile defense.

North Korea and Iran

In the case of North Korea, we are pursuing implementation of agreements we have reached at the Six Party Talks calling for

North Korea to abandon all existing nuclear programs and its nuclear weapons. We have made progress through the disabling of facilities at the Yongbyon nuclear complex. The tough work of verifying North Korea's declaration and proceeding to dismantle its nuclear programs remains ahead.

In Iran, we are also pursuing diplomatic action within a group of 6 nations, the P5+1. This group recently made a renewed offer of incentives to Iran. We continue to urge Iran's leaders to accept this generous offer, meet the requirements of the UN Security Council Resolutions, and sit down to negotiations with these six countries. If Iran does not accept the proposal, we will pursue the other track of our dual-track approach and increase pressure on the regime, including through sanctions. The possibility of a nuclear-armed Iran represents a profound threat to the security of the United States and other nations around the globe.

Chapter 5

The Potential for Nuclear Terrorism

Global Network of Partners

Nuclear terrorism is one type of WMD terrorism and involves terrorist use or threat of use of nuclear weapons or materials. Strictly speaking, nuclear terrorism refers to the creation and detonation of a device in which a sustained fission reaction takes place. This restricts nuclear terrorism to bombs using highly enriched uranium (HEU) or plutonium (Pu). However, some people use the term "nuclear terrorism" to refer to any terrorist weapon using a radioactive substance. This includes the use of radiation dispersal devices (RDDs). RDDs use conventional explosives to spread radioactive material over a wide area. Examples of materials that could be used in RDDs are cesium-137, strontium-90, and cobalt-60, all of which are commonly used and often weakly protected in civilian research laboratories and medical facilities. Attacks by terrorists on nuclear power plants or research reactors, intended to cause a nuclear accident that would release radiation, can also be considered nuclear terrorism.

It is very doubtful that any terrorist group could produce a nuclear weapon on its own without assistance from a state

nuclear program. Acquiring and enriching uranium, or creating plutonium in a nuclear reactor, is an extremely expensive and difficult process, requiring expensive equipment and sophisticated techniques. Even if a terrorist group were able to acquire enough weapons-grade HEU or plutonium, it is still a technically demanding and expensive task to put together even a simple nuclear device. Producing a chemical or biological weapon would be far easier for terrorists to accomplish than creating a nuclear weapon.

Terrorists could attempt to acquire a complete, working nuclear weapon from a state. In this case terrorists would either steal a nuclear device, receive one from a state sponsor, or bribe military or political officials to acquire a device. Concerns about this possibility increased after the collapse of the former Soviet Union, as doubts were raised about the security of Soviet nuclear weapons, one example being the debate over so-called "suitcase nukes." Even if a nuclear weapon were successfully stolen, terrorists would have to defeat built-in mechanisms that are designed to prevent the unauthorized detonation of a nuclear weapon. The U.S. Department of Defense, through its Cooperative Threat Reduction Program (CTR), has been working with the Russian Ministry of Defense to increase the security of Russian nuclear weapons.

A nuclear explosion, even though difficult to achieve, would be extremely attractive to terrorists if they wanted to cause mass casualties. This is because of the devastating effects of nuclear explosions (heat, blast effects and radiation contamination) and

also the shock value this would have on the target population. While the probability of terrorists acquiring and using a nuclear fission weapon is quite low, there is a much greater likelihood of terrorists using a radiological dispersal device (RDD). Highly radioactive substances are far more readily available than HEU or plutonium. These substances cannot be used to make a nuclear weapon, and the destruction caused by an RDD would be much less than that caused by a nuclear weapon. While much less technically challenging than building a nuclear weapon, building a so-called "dirty bomb" is not easy.

Terrorists would have to work with highly radioactive materials while assembling the device. They would have to have training and knowledge to design the device in such a way as to maximize its impact. If a conventional bomb were used to disperse the radioactive material, the primary cause of death would be the conventional explosive. It would be very difficult to create an RDD that would cause immediate mass casualties, since it is hard to maintain high concentrations of radioactive materials while dispersing them over a wide area. Illnesses and deaths due to the radioactive component of an RDD probably would not appear for a substantial period of time. An RDD could, however, be an effective terror weapon because fear of radiation might induce panic and overreaction within the population.

For example, the nuclear terrorism alerts in late 2001 and the May 2002 arrest of Jose Padilla, an alleged Al-Qaeda affiliate believed to have studied how to make radiological weapons, increased public anxiety and prompted many people to purchase

Geiger counters and potassium iodide pills in anticipation of a radiological attack. Decontaminating the affected area may also be a difficult and expensive process, depending on the type of explosive and radioactive material used, topography, and a number of other factors.

An attack on a nuclear facility, with the aim of causing a massive release of radioactive material, is also a credible possibility for terrorists who cannot get their hands on sufficient amounts of radioactive material. Most nuclear facilities have security measures to counter a terrorist attack, such as well-trained guards and safety mechanisms to prevent or mitigate release of radioactivity. However, many critics argue that these are insufficient to prevent the entry into critical areas of a nuclear facility by highly trained, well-armed terrorists, sabotage by insiders, or the deliberate crashing of a hijacked airliner into a nuclear facility. There is also some debate as to how likely a large-scale release of radioactivity would be in such a case. The U.S. government is attempting to increase security at nuclear facilities in order to prevent this.

In July 2006, Russia and the United States launched the Global Initiative to Combat Nuclear Terrorism to improve cooperation on measures to protect nuclear materials, prevent nuclear trafficking, deny safe haven to nuclear terrorists, mitigate the effects of a terrorist attack, and adopt strong national legislation to punish terrorists. This new effort supplements UN measures to prevent WMD proliferation and terrorism, including UN Resolution 1540. Once a largely theoretical threat, bioterrorism

has become a reality since October 2001. Letters containing the deadly anthrax bacterium *Bacillus anthracis* were sent through the mail to prominent politicians and people in the media. Eleven people were diagnosed with inhalation anthrax, five of whom died. Another 14 people were diagnosed with the cutaneous, or skin, form of the disease; none of these persons died. The victims included postal workers and other individuals who came into direct contact with the letters as well as cases of cross-contamination.

DNA analysis of the anthrax spores used in the letters narrowed the investigation down to the Ames vaccine strain, acquired in the early 1980s by Fort Detrick's Army Medical Research Institute of Infectious Diseases, the primary U.S. bioterrorism research facility. The Ames strain has been shared with about a dozen other labs in the United States, Canada, and Great Britain for research purposes. Despite a massive investigation by the Federal Bureau of Investigation (FBI) and postal inspectors, no arrest has been made in the case dubbed "Amerithrax." The investigation has focused on 20-30 "persons of interest" within the United States who may have had access to and experience with anthrax, particularly scientists connected with Fort Detrick, Maryland.

The anthrax letters were an entirely new phenomenon. Despite hundreds of anthrax hoaxes prior to 2001, this was the first time that actual anthrax spores had been used in the United States. These anthrax incidents were small-scale, and apparently intended to frighten rather than kill large numbers of people.

Since 2001, there have been many hoaxes, where the senders claim to be sending anthrax, but actually enclose a harmless white powder. In many cases, hazardous material teams respond to the hoaxes at great cost to the public and disruption to businesses. The U.S. government has allocated billions of dollars to detecting and combating anthrax and other biological weapons. The U.S. Postal Service has installed machines across the country that monitor the mail for anthrax or other biological agents. Some experts argue that the huge U.S. spending on bioterrorism is out of proportion to the threat.

If 9/11 proved anything to America, it's that the terrorists mean it. But the lesson has not yet been learned fully. It's dangerous for Americans to assume that nuclear weapons and materials around the world are secured in vaults, guarded day and night, beyond the reach of those who would use them without conscience or fear of death. They are not. The mission of Citizens to Stop Nuclear Terrorism is to ensure that nuclear weapons and nuclear materials worldwide are locked away safely. CSNT is working diligently to raise public awareness of the threat of a nuclear 9/11 and with members of Congress to take steps to prevent the unthinkable.

The United States, the target of history's most devastating terrorist attack, must do whatever is necessary to avert a catastrophe that doesn't have to happen. "Nuclear terrorism remains a real and urgent danger," said a report prepared by the Belfer Center for Science and International Affairs at the John F. Kennedy School of Government at Harvard University, "Securing

the Bomb 2007." "Terrorists are actively seeking nuclear weapons and the materials to make them. With enough plutonium or highly enriched uranium (HEU), a sophisticated and well-organized terrorist group could potentially make at least a crude nuclear bomb that could incinerate the heart of any major city."

CSNT embraces that report's chief recommendations to thwart a nuclear terrorist strike against the United States or its allies, namely:

- A U.S.-led global campaign "to lock down every nuclear weapon and every significant cache of potential nuclear bomb material worldwide" as rapidly as possible.
- Create effective nuclear security standards worldwide.
- Remove weapons-usable material from the world's most vulnerable sites as rapidly as possible.

The 9/11 terrorists didn't have access to nuclear materials. Others might, unless the world acts now to lock them down. A successful nuclear attack by terrorists would be catastrophic. Intense fears of nuclear terrorism have led to a search for a perfect defense: destroying all terrorist groups that threaten the United States, sealing U.S. borders against loose nukes, or locking up all existing nuclear weapons and materials. Yet none of these strategies is a silver bullet. It is fantasy to believe that terrorism can be eliminated or that thousands of miles of U.S. borders -- not to mention the borders of U.S. allies -- can be sealed. Initiatives to secure nuclear weapons and materials are vital, but they will always fall short, too.

Rather than search for a perfect defense, which will never exist, counterterrorism strategists must use the many imperfect tools at their disposal to confront the many imperfect terrorist groups that they face. To pull off a nuclear attack, a group would need to acquire nuclear materials or a weapon, build a bomb or unlock an existing one, move that weapon to its target, and detonate it. Securing nuclear weapons and materials, although critical, confronts only one part of a plot and cannot eliminate the threat entirely. Strategists must build on this one defense to develop an integrated defensive system that also draws on border security, law enforcement, intelligence operations, military and diplomatic initiatives, and emergency response efforts. To do so properly, they must develop a more realistic picture of nuclear terrorism that draws on a careful understanding of how terrorist groups work and how their plots can fail.

When strategies for preventing nuclear terrorism rely on silver bullets, less dramatic -- but nonetheless crucial -- measures are neglected. The search for a perfect defense is partly driven by outsized fears of terrorists' capabilities and the assumption that a worst-case, or "perfect storm," scenario will occur. But terrorists do not have superhuman powers; their plots are imperfect and contingent and can be derailed. Consider the analogy of a police department seeking to prevent bank robberies. If the department assumes that all thieves have cars that travel 200 miles per hour, the department will give up on planning carefully for car chases and focus almost entirely on guarding the banks. If it instead realizes that many thieves will have cars that

travel only 100 miles per hour, it will also carefully develop tactics for chasing down robbers.

Realistically assessing the full spectrum of possible threats -- in this case, from Ferraris to Ford Escorts -- spurs broader and more careful planning by the police department. The same would be true of the U.S. government's homeland security and counterterrorism policies if Washington adopted a more nuanced view of the nuclear terrorist threat. Moving away from worst-case assessments of the capabilities of nuclear terrorists will require strategists to rethink many basic assumptions. Terrorist groups are limited in their capabilities. Some terrorist groups, for example, lack expert personnel but have extensive resources.

Over the last 15 years, the nuclear threat to the United States and our friends and allies has changed dramatically. We no longer face a single adversary with thousands of missiles threatening our national existence. Rather, we now live in a world where transnational terrorist networks, motivated by violent and extreme ideologies, have declared their intent to use nuclear weapons against us. We also confront a growing nuclear threat from state sponsors of terrorism, who either possess a nuclear capability or are in the process of developing one. And finally, we are confronted with the prospect of non-state networks that are willing to sell nuclear technology and material to the highest bidder, and through whom terrorists may seek a nuclear weapon.

In addition, we are living in an era of globalization, which has yielded gains in economic prosperity and efficiency, as private

enterprises have outsourced business functions, made investments abroad, and developed global supply chains. These trends have, at the same time, exposed us to new risks, such as the potential for terrorists to exploit cyberspace, financial networks, and the shipping and air transport industry to plan and carry out attacks against our population centers, including with weapons of mass destruction.

We must act to counter these emerging threats. On Saturday in St. Petersburg, Presidents Bush and Putin announced the Global Initiative to Combat Nuclear Terrorism, an effort that will establish a partnership among nations committed to developing their individual and collective capabilities to detect and defeat the most dangerous threat we face – nuclear weapons in the hands of a terrorist.

The attacks of September 11 taught us that terrorists will stop at nothing to attack us and our way of life. Not satisfied with the killing of thousands of innocent civilians, Osama Bin Laden has declared his intention to acquire and use nuclear weapons against the United States with the potential to kill hundreds of thousands. Prior to 9/11, one member of Al Qaeda spoke directly to this point: "It's easy to kill more people with uranium."

Along with the nuclear threat from terrorist groups such as Al Qaeda, we are confronted with a growing nuclear threat from state sponsors of terrorism like Iran and North Korea who violate their obligations under the nonproliferation regimes. In addition, we know that non-state actors such as A.Q. Khan have entered

the black market to sell nuclear technology to the highest bidder. The coming together of these trends – on the one hand, the increasingly lethal goals of today's terrorists and on the other, the illicit trafficking in nuclear material and technology – makes nuclear terrorism both the most serious international security challenge of our time, and the most urgent.

Many American leaders have called attention to the threat of nuclear terrorism. President Bush has described this threat as the central national security challenge of our era. Other leaders have voiced similar views. 9/11 Commission Chairman Thomas Kean and Vice Chairman Lee Hamilton pointed to nuclear terrorism as the most dangerous risk we face, and urged more focused action against the threat. The President's WMD Commission also emphasized that more must be done to improve our intelligence capabilities to combat this urgent threat. Both of these commissions concluded that Al Qaeda has taken concrete steps to acquire a nuclear weapon by attempting to buy nuclear material on the black market.

Fortunately, Bin Laden's agents likely fell victim to a scam. Many academics and authors have also identified nuclear terrorism as the preeminent threat requiring more focused efforts to counter. All agree that, to defend against this threat, we cannot afford to wait until after an attack before we take corrective action. The consequences could be catastrophic. To be wrong once is to have lost one of our cities. We do not have a second chance; we must take steps now to avert that dark future. The Global Initiative to Combat Nuclear Terrorism is the first initiative of its kind, one

that takes a comprehensive approach to dealing with all elements of the challenge.

The Initiative is consistent with, and builds on, existing legal frameworks such as the Nuclear Terrorism Convention and UN Security Council Resolutions 1540 and 1373. It provides a flexible framework that will enable sustained international cooperation to prevent, detect, and respond to the threat of nuclear terrorism. It offers an opportunity for the United States, Russia, and our international partners to speak – and to act.

The Global Initiative builds on the Bush Administration's unprecedented record of accomplishment to combat the threat of weapons of mass destruction. For example, in 2002 the President launched the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction at the G8 Summit. In December 2002, the President approved the National Strategy to Combat Weapons of Mass Destruction, the first comprehensive strategy of its kind.

The National Strategy outlined the importance of integrating the traditional tools of nonproliferation with next generation counter proliferation efforts. Since the promulgation of that strategy, focused efforts have produced results and led directly to operational successes in the field. For example, the Proliferation Security Initiative (PSI), launched by President Bush in 2003 to strengthen international cooperation to disrupt the trade in WMD proliferation now counts over seventy-five partner nations and has played a key role in helping to interdict more than 30

shipments, including the interdiction of centrifuge parts that led to Tripoli's decision to abandon its chemical and nuclear weapons programs.

Under the President's leadership, a number of departments and agencies are taking a leadership role in implementing the National Strategy to Combat WMD. The Department of Defense promulgated its National Military Strategy to Combat WMD in February of 2006 and assigned U.S. Strategic Command with the responsibility for the combating WMD mission. Strategic Command, in turn, has established a Combating WMD Center at the Defense Threat Reduction Agency to bring together the expertise and resources in the Department of Defense to combat this urgent threat. Earlier, as recommended by the WMD Commission, President Bush signed a new Executive Order to ensure that we have the tools to stop the financing of proliferation related activity, a mission led by the Department of the Treasury in consultation with the Department of State. And the Departments Homeland Security and Energy have been active in establishing detection capabilities at ports abroad and at key land borders.

At the Department of State, Secretary Rice spearheaded a reorganization of the bureaus under my direction to focus attention on the entire combating WMD mission, as well as the nexus of WMD and terrorism. Finally, the standing up of the National Counter Terrorism Center, as well as the National Counter Proliferation Center, are bringing additional vigor to our planning and intelligence efforts. We are now ready to take the

next step – to build the partnerships abroad that are necessary to achieve our strategic goal to protect the American people and citizens of partner nations against nuclear terrorism.

The central objective of the Global Initiative to Combat Nuclear Terrorism is to establish a growing network of partner nations that are committed to taking effective measures to build a layered defense-in-depth that can continuously adapt to the changing nature of the threat. While many individual programs and efforts have approached one element or aspect of the nuclear terrorism threat, the Global Initiative provides a capacity building framework for establishing new partnerships with those nations that wish to take similar action. In carrying out this new initiative, we will also cooperate with the IAEA and invite them to participate.

The approach begins with protecting material at the source. Here, the Global Initiative will build on activities underway through the Cooperative Threat Reduction (CTR) and International Counter proliferation Programs and the Department of Energy's many nonproliferation assistance programs. Our goal is to galvanize our partners to invest greater resources in their own capabilities to protect nuclear material on their territories. We will also seek to develop new partnerships with the private sector to reduce the risk of nuclear terrorism, including through innovative DHS programs such as the Customs Trade Partnership Against Terrorism (C-TPAT). Since our efforts to secure nuclear material can never be fail-safe we must develop a robust international detection architecture.

Here the Global Initiative will build on and sustain the successes of the Megaports Program and the Domestic Nuclear Detection Office, and catalyze new partnerships between these programs and their counterparts among partner nations. Our architecture must enable fixed and mobile detection across the air, land, and maritime domains and be flexible enough to ensure that our partners can develop interoperable and complementary capabilities. A comprehensive architecture must also include capabilities to detect the movement of funds and the growing threat posed by terrorists seeking to procure nuclear technology through cyberspace.

Here the Global Initiative will build on efforts underway at the Department of the Treasury to block the assets of terrorists and proliferators. To protect cyberspace, we must build on efforts underway in the Department of Homeland Security to protect our critical cyber infrastructure, including the relationship to critical nuclear facilities. We must develop new approaches to stop terrorists from using the virtual safe haven of cyberspace for planning attacks with nuclear weapons. The Global Initiative will also strengthen our response capabilities to stop imminent attacks and mitigate their consequences should they occur. In this area, we must build on the capabilities of the Department of Energy's emergency response teams. At the same time, we must acknowledge that U.S. capabilities alone cannot meet this challenge.

Rather, through the Global Initiative, we will foster partnerships with counterpart programs among Global Initiative partner

nations, and develop cooperative concepts of operations for emergency response and consequence management. By joining the Global Initiative, partner nations will have the opportunity to participate in joint exercises that support the development of their own capabilities, and under certain circumstances, call on the assistance of partner nations for emergency response, consequence management, and criminal justice functions.

Transforming Diplomacy to Combat WMD Terrorism

In launching the Global Initiative, we will also be taking an important step to implement transformational diplomacy outlined by Secretary Rice. Through new, flexible partnerships, as well as stronger bilateral and regional ties, the Global Initiative will ensure that our strategies for combating nuclear terrorism are tailored to the conditions prevailing with our partner nations. In bringing to bear all instruments of national power against this threat, the Initiative will bring diplomats together with first responders, forensic and technical experts, law enforcement officers, the military, and others in the public and private sectors who shape the present and future risks of nuclear terrorism. The Global Initiative will not only reinforce our national efforts, but it signals to all participating nations the importance of developing comprehensive approaches to combat the threat of WMD terrorism.

The Initiative can help partners improve their understanding of the intentions of terrorists seeking to carry out attacks. It can help us develop the tools to prevent terrorists from gaining

access to nuclear and radiological materials. Through the Initiative, we will employ in partnership with others new concepts of denial that are tailored to the specific facts, circumstances, and motivations of nuclear terrorists and their facilitators. The Global Initiative can also serve as the necessary platform for implementing the provisions of the Nuclear Terrorism Convention to ensure that we bring terrorists seeking to carry out nuclear attacks to justice, including through enhanced forensics techniques, as well as through strengthened legal processes.

As we proceed, we will build on the success of the Proliferation Security Initiative and the flexible partnerships it has established. However, we will also fill important gaps. For example, while PSI has focused on the interdiction of all WMD and related delivery systems, the Global Initiative brings a special focus to the operational and technical challenges associated with combating the nuclear terrorism threat. While PSI focuses on the proliferation trade among state actors, the Global Initiative will be focused on those pathways of nuclear proliferation that lead to terrorist end users. While PSI has strengthened our interdiction capabilities, the Global Initiative will move beyond interdiction within the nuclear and radiological area, to cooperation on tasks related to material protection, detection, emergency response, consequence management, attribution, and criminal justice.

Public-Private Partnerships

While the announcement of the Global Initiative shows diplomatic leadership by the United States and Russia, this effort must extend beyond the diplomatic realm to achieve success. In detecting nuclear material coming into our ports and urban areas and sharing best practices with foreign port operators, the Department of Homeland Security and its foreign counterparts must play a central role. In protecting our nuclear facilities from sabotage and exercising such capabilities with foreign partners, the Department of Energy and equivalent agencies abroad must play a central role. In stanching the flow of funds to terrorists seeking to buy nuclear material on the black market, the Department of Treasury and its fellow finance ministries must work closely.

In all these areas, all departments and agencies participating in the Global Initiative will have to improve their sharing of information, whether law enforcement, operational, or technical. There is also a large role for the private sector to play in mitigating the risk of nuclear terrorism. In the United States as in other countries, a substantial portion of the nuclear infrastructure is controlled by private sector utilities, laboratories, or university research centers or institutes. By working closely with these private entities, as well as those that supply and insure them, we can stimulate the development of best practices, risk management approaches, and codes of conduct.

Getting Results

As we move forward to implement the comprehensive vision of the Global Initiative, we must take care to identify specific ways to assess our efforts and measure our success. The Initiative offers the United States and other partners committed to taking a leadership role in combating nuclear terrorism an opportunity to raise the bar, to hold ourselves accountable for results, and in turn, to expect results from our partners. Building on the example set by the United States and Russia at the Bratislava Summit regarding nuclear security, we believe it will be useful to report every six months on the implementation of the Global Initiative.

Let me suggest four initial questions we should ask, as we seek to judge the success of the initiative from now until the end of 2008:

- How many countries will have joined the initiative as partners? PSI has secured the endorsement of nearly eighty partners, and its capabilities have improved as its partnership has expanded.
- How many multinational training exercises involving operational, technical, or other forms of global or regional cooperation will the Global Initiative have sponsored among its respective partners?
- What specific steps will we have taken to improve the security of nuclear material at the source? We will expect partner nations to field a nuclear materials

information database capability with inventory information regarding all material subject to their jurisdiction and to cooperate with information sharing requests from partners through Global Initiative activities.

- To what extent will Initiative partner nations have expanded their nuclear and radiological detection or scanning of cargo coming to and leaving their ports and airports, as well as crossing their borders? Increasing the amount of total cargo scanned could serve as a worthy goal. We should also take steps to ensure that all partners exchange detection information in a near real-time manner with other partners.

Let me emphasize that we are still in the early stages of developing more precise performance measures of success for the Initiative, and some measures may ultimately be adopted by some partners, while they are not by others. This flexibility can be a valuable strength in an initiative, when it allows those partners who seek to do more to run ahead, while acknowledging the important contributions of others that are not as fully capable. In the coming months, Global Initiative partners will convene an initial meeting to agree not only to the guiding principles for this initiative, but also to establish a specific Plan of Work to implement these principles.

All of us live close enough to nuclear power plants that it is a viable issue to consider. With the potential capability of terrorists to create smaller nuclear weapon in the range of 20

Kiloton Improvised Nuclear Devices (IND) to 150 Kiloton (KT) Mulistage Nuclear Device, a surprise nuclear attack is not impossible. The most important and different aspect is such potential terrorist nuclear weapons would be more localized and are survivable beyond the immediate area of attack. But nuclear fallout does spread via wind, and the after affects would be necessary to protect your family from.

Typically, there is a wider range of fallout DOWNWIND from a nuclear device or explosion, so that would be a possible consideration in an evacuation plan. With largest nuclear explosure ever measured (huge 15 Megaton bomb), Government identified fallout pattern reached downwind for 320 miles, but there was only a WIDTH of cross section in downwind fallout of 40 miles. If you are thinking a 150 KT nuclear explosion, you could extrapolate estimate of 32 miles fallout downwind, and 4 mile fallout width downwind. So if you are not NORTH of a nuclear attack, and you are south or downwind of it, try to be at least 4 miles away from downwind, and make effort to be 20 miles - so if you go SOUTH - you would try to go SOUTHEAST or SOUTHWEST of nuclear attack, not just directly South, if possible.

To play it safe, you would want to get 50 miles away quickly from an attack. Bottom line in a nuclear attack is DISTANCE = IMPROVED SAFETY. Terrorists have tried to obtain weapons of mass destruction: chemical, biological, radiological, and nuclear weapons. Hearings and media articles since September 11 have highlighted radiological dispersal devices, or "dirty bombs,"

which would use standard explosives or other means to disperse radioactive materials. Dirty bombs would be quite feasible for a terrorist group to make, given the limited expertise needed and the availability of explosives and radioactive material.

An attack with such a weapon likely would kill or injure few people and cause little property damage, though it could cause panic and might require closing some areas for an undetermined time. While a terrorist attack using a nuclear weapon (a device that caused a substantial nuclear explosive yield, as distinct from a dirty bomb) has much lower feasibility, it merits consideration because it would have much higher consequence. The September 11 attacks, as well as earlier and later analyses, showed that many U.S. facilities could be attractive targets for terrorist attack. One set of targets that has attracted attention from Congress is the nation's seaports.

If terrorists smuggled a Hiroshima-sized bomb into a port and set it off, the attack would destroy buildings out to a mile or two; start fires, especially in a port that handled petroleum and chemicals; fallout over many square miles; and disrupt commerce. It could kill many thousands of people. Terrorists might attempt to smuggle a bomb into a U.S. port in many ways, such as in a tanker or a dry bulk freighter, but sea containers may provide them a particularly attractive route. A container is "[a] truck trailer body that can be detached from the chassis for loading into a vessel, a rail car or stacked in a container depot." Much of the world's cargo moves by container.

The U.S. Customs Service processed 5.7 million containers entering the United States by ship in 2001.3 It screens data for all these containers, though it inspects "only about 2 percent of the total volume of trade entering the country each year." Containers could easily accommodate a nuclear weapon. U.S. Customs Commissioner Robert Bonner believes that with an attack using a bomb in a container, "the shipping of sea containers would stop," leading to devastating consequences for the global economy, bringing some countries to the edge of economic collapse. On the other hand, people can find ways to minimize economic problems.

The Y2K computer bug did not result in disaster, in part because organizations using computers took steps to ward off the problem. German production of tanks, aircraft, and artillery pieces increased in 1943 and 1944 despite Allied bombing.7 Because of concern for port vulnerability, Congress is considering S. 1214, Port and Maritime Security Act of 2001; a conference is pending.

Chapter 6

Terrorist Nuclear Weapons

Russia

A terrorist group (as distinct from a nation) might obtain a nuclear bomb by several plausible routes. In each case, a reasonable estimate of explosive yield is that of the Hiroshima bomb, 15 kilotons, equivalent to the explosive force of 15,000 tons of TNT.

Strategic nuclear weapons (long-range weapons the Soviet Union would have used to attack the United States) are reportedly well guarded on missiles or, thanks in part to U.S. assistance, in storage. In contrast, thousands of lower-yield weapons intended for use in combat are less well secured, and numbers and locations are uncertain. Terrorists might buy or steal one of these weapons. The weapons might (or might not) have devices to prevent unauthorized use, or terrorists might lack confidence that they could make a weapon work. Without such confidence, terrorists might "mine" the weapon for nuclear materials and components to make their own device.

Pakistan

Other nations have nuclear weapons. U.S., British, French, and Israeli weapons are thought to be well guarded. Chinese weapons

are also thought to be well guarded, though less is known on this point. Control is less certain for India and Pakistan. Of the two, it appears more likely that terrorists might obtain a bomb from Pakistan. That nation asserts that it has complete control over its weapons, but that could change if Pakistan were taken over by Islamic fundamentalists sympathetic to al-Qaeda and other terrorist groups. In this scenario, the "donors" would presumably give the terrorists detailed instructions for operating the bombs.

The Hiroshima bomb was a "gun assembly" weapon. Its nuclear explosive component was a gun barrel about 6 inches in diameter by 6 feet long. It was capped at each end, with standard explosive at one end, a mass of uranium highly enriched in the isotope 235 (highly enriched uranium, or HEU) at the other end, and a second HEU mass in the middle. Detonating the explosive shot one mass of HEU into the other, rapidly assembling a mass large enough to support a fission chain reaction. (Plutonium cannot be used.) This is the simplest type of nuclear weapon. U.S. scientists had such high confidence in the design that they did not test the Hiroshima bomb.

Many experts believe that a terrorist group having access to HEU and the requisite skills, but without the resources available to a nation, could build such a weapon. Five former Los Alamos nuclear weapons experts held that a crude nuclear weapon "could be constructed by a group not previously engaged in designing or building nuclear weapons, providing a number of requirements were adequately met." The requirements they list, though, are substantial. They include detailed design drawings and

specifications; individuals skilled in a wide range of weapons skills; the necessary equipment; and extensive preparations to create a bomb quickly once in possession of HEU so as to reduce the risk of detection.

A National Research Council study presents another view. The basic technical information needed to construct a workable nuclear device is readily available in the open literature. The primary impediment that prevents countries or technically competent terrorist groups from developing nuclear weapons is the availability of SNM [special nuclear materials, i.e., HEU and plutonium-239], especially HEU. It would be difficult for a terrorist group to obtain enough HEU for a weapon. Many nations have gone to great lengths to protect it. The International Atomic Energy Agency has safeguards to protect, among other things, HEU in nuclear reactors.

The United States has had a number of programs over the past decade to help former Soviet republics protect nuclear weapons, material, and knowledge. Perhaps the best evidence that these efforts have succeeded so far is that terrorists have not detonated a nuclear weapon. At the same time, some are concerned that terrorists could obtain HEU. For example, the National Research Council study noted above rated the threat level from SNM from Russia as "High" large inventories of SNM are stored at many sites that apparently lack inventory controls and indigenous threats have increased.

Vulnerability of ports and shipping

Ports may be attractive targets for terrorists. With many of the largest ports in or near major cities, a nuclear bomb detonated in a port could kill many thousands of people, interrupt flows of U.S. commerce, and perhaps cause a global economic disruption. Ports are vulnerable. Manyare flat, being at the ocean's edge, so would offer little shielding against weapon effects. Some have great quantities of inflammable material, such as fuel; fires could extend the area of destruction and release toxic gases. While ports may stretch on for miles, a 15-kiloton weapon would have enough force to destroy many key facilities of a typical port.

Current front-line capability to detect nuclear weapons is exceedingly limited. CRS visits to the U.S. Customs Service in Baltimore in July 2002 and to the U.S. Coast Guard in Philadelphia in August 2002 produced the following information. Customs' Container Security Initiative seeks to improve security at foreign ports for U.S.-bound containers, but Customs inspectors do not inspect cargo there and do not control personnel selection or port operations. The Coast Guard cannot open containers at sea for various reasons. For example, they are tightly packed and the door is part of a container's structure, so a container under other containers might crumple if the door were opened. Technology is lacking. A Coast Guard officer wrote, "our method of detecting nuclear and biological weapons is... our eyes, ears, and brains. We currently have no more sophisticated equipment than that." At Baltimore, Customs inspects about 2 percent of containers. For some, it uses a sophisticated machine

that x-rays entire containers; for others, it unloads all items from a container, may x-ray them, and searches some items. Customs agents have pager-size radiation detectors. Problems are obvious. Terrorists could infiltrate foreign ports as inspectors or longshoremen, and pass a container with a weapon into a secured zone. The Coast Guard almost certainly could not detect a bomb in a container or in the structure of a ship. Customs targets containers for inspection based on cargo manifest data, port of last call, shipping line, etc. Terrorists, however, could be expected to go to great lengths to make a bomb-carrying container appear normal. Small radiation detectors might detect highly radioactive isotopes that might be used in dirty bombs, but could not be sure of detecting less-radioactive uranium-235. Once a ship arrives in port, any inspection could be too late.

Responses and Countermeasures

The central approach to reducing vulnerability to a terrorist nuclear attack is "defense in depth," in which multiple methods are used to detect and interdict a terrorist nuclear weapon. Many existing technologies could assist the search for nuclear bombs, and others are under development. Intelligence can seek clues that terrorists were seeking or had obtained HEU, or were trying to make or smuggle a bomb. The United States can reach agreements with foreign governments.12 Coast Guard and Customs inspections might help, especially if personnel had more and better equipment. Although no one method is perfect, together they can increase the odds of detecting a weapon. For example, it would be harder to evade several means of detection

than just one, as attempts to reduce what one sensor detects may make the bomb more visible to another sensor using a different signature, or may reduce the likelihood that the bomb would work. Further, a terrorist group would not know the limits of detection capability, so would have to assume a capability greater than what existed. Defense in depth could involve outfitting every port, airport, and border crossing with several types of sensors and the personnel to operate them, expanding intelligence capabilities with new sensors and analysts, placing U.S. agents in foreign ports, and upgrading Coast Guard and Customs equipment and adding personnel. Such steps would involve large costs.

While press articles focus on how the United States can augment its detection capabilities, the struggle is two-sided. If we deploy a new sensor at some ports, terrorists might detonate a weapon before it is inspected, or hide it in a container bound for another port. If foreign ports screened containers before being loaded onto U.S.-bound ships, they could infiltrate the port. If we secured the world's largest ports, they could use smaller ones. If we assured the security of every U.S.-bound container, they might smuggle a weapon in a freighter or supertanker. If we secured all U.S.-bound containers, they might ship a bomb to Mexico and bring it into the United States in a small boat or airplane. In short, despite overwhelming advantages that the United States and its trading partners possess in technology and organization, terrorists have other advantages.

Securing nuclear materials

The possibility that a terrorist group could make a nuclear weapon given enough HEU, and the difficulty of preventing terrorists from smuggling a weapon into a U.S. port, show the value of the effort to secure nuclear weapons and materials in Russia and elsewhere. Are current efforts sufficient?

Forensics

The United States can often identify the origin of nuclear material used in a bomb. This forensic capability strengthens the value of controlling Russian nuclear weapons and materials: finding that material for a bomb detonated in the United Statescame from Russia, a likely source, would in all probability lead to the conclusion that the material was stolen rather than that Russia conducted the attack. At the same time, augmenting already-excellent forensic capability through technology and intelligence could help deter other nations from giving nuclear materials to a terrorist group.

Ports in major cities

The terrorist weapons discussed earlier have much less explosive yield than nuclear weapons carried by bombers and long-range missiles, and a smaller destructive radius. Blast damage might extend 1 to 2 miles. (Fire and fallout might extend beyond that range.) Accordingly, it might be argued that ports with the greatest number of people living or working within a mile or two

of cargo docks, such as Philadelphia and New York, should have highest priority in receiving security resources.

Overseas inspections

Inspection of ships in U.S. ports would be too late to prevent a nuclear explosion, so the United States might require screening of U.S.-bound cargo by U.S. personnel in ports originating shipments. Other nations might view such a requirement as an infringement on their prerogatives, but the size of the U.S. market would presumably make exporting nations more willing to consider such measures.

Ameliorating economic consequences

Civil defense studies over decades examined how to ameliorate the destructive effects of a large nuclear attack. This effort, and more recent emergency preparedness efforts, provides a template for response and recovery following a terrorist attack using one 15-kiloton weapon. This work does not, however, address possible global economic consequences and how to predict and mitigate them.

These issues could benefit from further study and analyses. What level of effort? While the United States is increasing its efforts to counter nuclear terrorism, the current level of effort might stop only an unsophisticated attempt to smuggle a nuclear weapon into the United States. Terrorists who might acquire a nuclear weapon, though, would surely go to great lengths to deliver it. A

massive U.S. counterterrorism effort would increase security, but would require many more security personnel, large-scale diversion of technology resources, possible civil liberties concerns, and high cost. A low level of effort appears politically untenable. At issue is whether a moderate level of effort is effective, and whether a high level of effort is supportable.

U.S. Customs chief raises nuke threat on containers

The head of the U.S. Customs Service, in announcing a new security initiative, raised the specter of a nuclear bomb being shipped to and detonated in a United States seaport. "Of greater concern are the possibilities that international terrorists such as al Qaeda could smuggle a crude nuclear device in one of the more than 50,000 (shipping) containers that arrive in the U.S. each day. One can only imagine the devastation of a small nuclear explosion at one of our seaports," said Customs Commissioner Robert Bonner in a speech prepared for delivery at the Center for Strategic and International Studies, a Washington think tank. Bonner raised the concern in announcing a new container security initiative intended to enable officials to have more data on what's in international shipping containers and enhance the ability of the United States to stop suspicious containers before they arrive at an American seaport.

"First and foremost, we concentrate our efforts on the 'mega-ports' of the world -- the largest container ports -- and specifically those ports that send the highest volumes of container traffic into the United States," Bonner said.

Bonner said the top 10 international ports account for almost half of all the container traffic coming into the United States. One idea, he said, is to have the latest X-ray machines and radiation detectors at foreign "mega-ports" to catch worrisome containers on the outbound trip. He said the idea of delivering a nuclear device by container to the United States was "by no means far-fetched" and said Italian authorities in October had found an al Qaeda operative bound for Canada in a container outfitted with a bed and bathroom.

Aside from the human toll, Bonner also said a nuclear attack via a shipping container would also exact a huge cost economically. "The detonation of a nuclear device smuggled by way of a sea container would have a far greater impact upon global trade and the global economy. Even a two-week shutdown of global sea container traffic would be devastating, costing billions," he said.

On Dec. 18, 1998, an official of Russia's successor agency to the KGB, the Federal Security Service (FSB), said that agents under his command had broken up a conspiracy by employees of a major nuclear facility in the Chelyabinsk region to steal 18.5 kilograms of weapons-usable material. If it had gone through, the theft would have caused "significant damage to the [Russian] state," local media quoted FSB Maj. Gen. Valeriy Tretyakov as saying.

Chelyabinsk is home to some of Russia's most important nuclear facilities, including a nuclear-weapons assembly and disassembly plant at Trekhgorny, and a weapons-design lab at Snezhinsk. If a

group of insiders at one of these sensitive sites had decided to steal fissile material - well, that would be a highly serious matter. Furthermore, the material involved was apparently not some useless radioactive slurry. It was weapons-usable - meaning 18.5 kilograms might be enough to make an entire nuclear weapon.

This incident is not included on most lists of the most important nuclear trafficking incidents, for the simple reason that it was quashed in its initial phases. But it remains one of the most troubling apparent cases of attempted proliferation of all - because it matches almost exactly the US nightmare scenario for a fissile-material theft. It wasn't ancient history. It occurred in 1998, after many facilities in the region had received US money for protection upgrades. It involved lots of stuff. And it involved a conspiracy of the knowledgeable.

"Multiple insiders are the hardest thing for any security system to address," says Mr. Bunn of the Managing the Atom project. Consider the ramifications. Russia has a "three-man rule" in regard to its nuclear weapons. Individuals are forbidden from working alone on warheads, as are twosomes. But if two scientists are in cahoots, they might be able to overpower the third. To guard against this, security might have to institute a four-man, or even five-man rule. Perimeter guards might need to be doubled. The cost and complexity of protection systems escalates exponentially. And what would be the genesis of such a conspiracy? Perhaps a group of disillusioned scientists or guards would try such a thing on their own, but that may be unlikely,

given the difficulties of marketing the stuff. It's more likely that such a theft might come in response to an enticing overture. Such as Saddam Hussein, perhaps, offering enough money for everyone in the group to buy a South Seas island. "What I worry about is state intelligence agencies contacting these people," says Scott Parrish, an analyst at the Center for Nonproliferation Studies at the Monterey Institute.

If the Chelyabinsk conspiracy is the No. 1 worrisome incidence of potential trafficking in nuclear material, the Prague seizure might be judged No. 2. In December 1994, an anonymous tip led Czech police to a marked car. In it, they found 2.7 kilograms of HEU enriched to 87.7 percent. The amount and purity of the recovered material was highly troubling. Worse, in two instances in 1995, Czech authorities recovered small amounts of additional HEU that appeared to be from the same source.

This suggests that there is a stock of weapons-grade HEU out there, of unknown quantity, in unknown hands. New worries about so-called "dirty bombs," conventional explosives used to spread deadly radioactive material over a wide area, are also making some incidents of trafficking seem important in retrospect.

Earlier this year, for instance, the Russian news agency Itar-Tass reported the seizure of 5 kilograms of cesium 137 from Chechen rebels, who were allegedly loading the material into mortar shells. Most experts do not consider this incident confirmed, but the Chechens have threatened to use radiological material before.

And cesium 137 is nasty stuff. Its radiation was the cause of many of the fatalities associated with the Soviet-era explosion of the Chernobyl nuclear plant.

In fact, once worries about dirty bombs multiply, the potential sources of dangerous material rapidly multiply as well. Radioactive material is used in many medical and industrial applications. Eastern Europe and the nations of the former Soviet Union even used trace amounts of plutonium in smoke detectors. "I used to joke that if Saddam Hussein placed an order in Russia for 500 million smoke detectors, we should get worried," says Dr. Parrish of the Monterey Institute.

What the U.S. is doing Preventing a nuclear terrorist attack on the US will require a comprehensive effort far into the future, say US officials. It will be one part - arguably the most important part - of the overall commitment to homeland defense. More narrowly, it may necessitate redoubled cooperation with the most likely source of loose nukes in the world: Russia. Warming relations between President Bush and his Russian counterpart, Vladimir Putin, today offer a window of opportunity for such intensification, say its advocates.

There is a decent foundation of mutual effort to build on. Initiated by Sen. Richard Lugar (R) of Indiana and former Sen. Sam Nunn (D) of Georgia in 1991, the Cooperative Threat Reduction (CTR) program has grown into a $1 billion-plus effort overseen on the US side by the Departments of Energy, State, and Defense. "These programs have achieved impressive results

for a relatively minor investment," says Stephen LaMontagne, a nuclear analyst at the Council for a Livable World Education Fund.

CTR funds pay for the destruction and dismantling of Russian ballistic missiles and submarines, for instance. Last year, $57 million of US funds went toward completion of the first wing of the Mayak Fissile Material Storage Facility, which will ultimately have the capacity to protect 6,250 dismantled warheads.

The Department of Energy's Material Protection, Control, and Accounting program has so far improved physical security at 13 Russian Navy nuclear sites and 24 civilian nuclear installations. But there are some 58 more Russian nuclear sites that need security upgrades, according to DOE figures. A program to blend HEU down into less dangerous civilian reactor fuel is moving slowly. Efforts to replace three Russian nuclear reactors that produce both desperately needed energy and plutonium have stalled in a swirl of politics.

And the Bush administration, in its first crack at drawing up a national- security budget, has slashed the funding of much of the non-proliferation effort. Bush's budget took $100 million out of the Department of Energy's side of the effort, alone. The needs, according to the Secretary of Energy's advisory board task force headed by Mr. Baker and Mr. Cutler, include: a real strategic plan; a high-level position within the White House devoted to the issue, perhaps within the National Security Council; more money, and more urgency.

Nuclear Shelter Expedient Options

Two expedient sheltering options you could do very quickly. Amongst expedient last-minute sheltering options at home, even just simply pushing a heavy table or pool table (one you can get under) into the corner of a below ground basement, ideally the corner with the grade (earth) highest up the wall on the other side of it, can be surprisingly effective.

You would then pile atop it and all around it (on the two exposed sides), any additional available mass (such as books, wood, cordwood, bricks, sandbags, heavy furniture, full file cabinets, or boxes full of anything heavy, like earth) before then crawling in under it. Have a small entrance and more mass that can be easily pulled in after you to seal it up. Leave two little 4" air spaces, one high at one end and one low at the other, and with a small piece of cardboard you can help fan fresh air in if the natural rising warmer air convection needs an assist bringing in more fresh air. Also, cover up any basement windows or other openings anywhere in the basement where you can see light shining through with sandbags or solid masonry blocks or cordwood, etc.

A basement already provides a 10 to 50 PF (Protection Factor) and then hunkering down under a sturdy table packed and surrounded by extra mass can add another 2-4 PF which would give you a total of 20 to 200 PF. That means that if there was an initial 1,000 R/hr radiation intensity outside you would have under that table only 5 – 50 R/hr. And, remember, with every

passing hour that fallout would be decaying and quickly losing its energy to where 7 hours later, it would only be 1/10th of that strength. Adding more mass on the floor above and outside against those walls opposite your shelter inside, can add even more sheilding protection. As cramped as that might be, you would have achieved a Protection Factor (PF), in less than half an hour of moving some mass into place, that could clearly be the difference between exposure to a lethal dose of radioactive fallout outside or survival for your family.

Think what you could accomplish if you started now, well before any nuclear emergency, to explore your available options and built (or at least acquired and pre-positioned the materials for) a mass encased small fallout shelter there in your own basement. Clearly, this is too cheap and easy not to have fully explored it. Or, you could do a combination tornado/fallout shelter in the backyard, if the ground isn't now frozen where you are. With 30" of earth covering alone you would achieve a PF of 300 and occupants would receive less than 1/300th of the gamma-ray dose of fallout radiation that they would otherwise have received out in the open.

A fairly expedient (pretty cheap/fast) option for outside shelter building, especially for all those without basements, is to acquire a section of, under the road rated, corrugated culvert pipe of at least 4' diameter. It's very common, cheap, and you might even find some for next to nothing at your local metal junk yard that you could take home in the back of a long-bed pick-up (if 12' long or less) or on a boat trailer. Have a hole dug at least as deep as

half the diameter of the pipe in an area without a high water table that has good drainage. Roll it in and wall up the ends with cemented block, railroad ties, or even a couple sheets of reinforced plywood a little longer than the diameter, but leaving you an entrance/exit and air shaft at both ends at the top half that's still above ground. (If you've got the expertise/welder or money, and time, you could go ahead and have 10 gauge steel bulkheads welded on each end instead.)

Whatever you use, have these end walls extend up past and above the culvert for 2' - 3' for holding back the dirt at the ends you'll later put atop the shelter. You won't have enough excavation dirt (from the hole you created) to cover the shelter back over to a 2-3' level and still assure the grade atop is gradual enough to thwart future erosion, so you'll need to get some more from elsewhere in your yard or bring in some with pick-up truck loads, etc. You'll also need sandbags full or solid masonry blocks to pre-position them at one end to pull/lift/push into place when you all get inside. Have one end already stacked solid with them, except for a small air gap at top and have the other end sealed up, too, except for enough room to wiggle in for the largest member of your family.

The reason we have created two potential entrances, with removable blocks or bags, is so we also have two potential exits, if part of your house or a tree later fell on one end. There's a lot of refinements that can make this more permanent, and better assure water doesn't get into the shelter before you do, etc. But, the point is, you can get creative with encasing mass all around

your family for little time/money/effort. Cramped and miserable for a couple days, yes, assuredly, but it'll be a story of survival your family will be around for to recount for years ahead together, especially when compared to the alternative fate of being above ground and exposed to the full intensity of radioactive fallout in those most dangerous first couple days.

Nuclear Incidents

There are two fundamentally different threats in the area of nuclear terrorism. One is the use, threatened use, or threatened detonation, of a nuclear bomb. The other is the detonation, or threatened detonation, of a conventional explosive incorporating nuclear materials. It is unlikely that any terrorist organization could acquire or build a nuclear device, or acquire and use a fully functional nuclear weapon. The greatest potential terrorist threat for a nuclear weapon would be to use such a device as a form of extortion.

The Nuclear Environment

Prepare yourself to survive in a nuclear environment. Know how to react to a nuclear hazard.

Effects of Nuclear Weapons

The effects of nuclear weapons are classified as either initial or residual. Initial effects occur in the immediate area of the

explosion and are hazardous in the first minute after the explosion. Residual effects can last for days or years and cause death. The principal initial effects are blast and radiation.

Blast

Defined as the brief and rapid movement of air away from the explosion's center and the pressure accompanying this movement. Strong winds accompany the blast. Blast hurls debris and personnel, collapses lungs, ruptures eardrums, collapses structures and positions, and causes immediate death or injury with its crushing effect.

Thermal Radiation

The heat and light radiation a nuclear explosion's fireball emits. Light radiation consists of both visible light and ultraviolet and infrared light. Thermal radiation produces extensive fires, skin burns, and flash blindness.

Nuclear Radiation

As stated above, nuclear radiation breaks down into two categories - initial radiation and residual radiation. Initial nuclear radiation consists of intense gamma rays and neutrons produced during the first minute after the explosion. This radiation causes extensive damage to cells throughout the body. Radiation damage may cause headaches, nausea, vomiting, diarrhea, and even death, depending on the radiation dose

received. The major problem in protecting yourself against the initial radiation's effects is that you may have received a lethal or incapacitating dose before taking any protective action.

Personnel exposed to lethal amounts of initial radiation may well have been killed or fatally injured by blast or thermal radiation. Residual radiation consists of all radiation produced after one minute from the explosion. It has more effect on you than initial radiation. A discussion of residual radiation takes place in a subsequent paragraph.

Types of Nuclear Bursts

There are three types of nuclear bursts - airburst, surface burst, and subsurface burst. The type of burst directly affects your chances of survival. A subsurface burst occurs completely underground or underwater. Its effects remain beneath the surface or in the immediate area where the surface collapses into a crater over the burst's location. Subsurface bursts cause you little or no radioactive hazard unless you enter the immediate area of the crater. No further discussion of this type of burst will take place.

An airburst occurs in the air above its intended target. The airburst provides the maximum radiation effect on the target and is, therefore, most dangerous to you in terms of immediate nuclear effects. A surface burst occurs on the ground or water surface. Large amounts of fallout result, with serious long-term

effects for you. This type of burst is your greatest nuclear hazard.

Nuclear Injuries

Most injuries in the nuclear environment result from the initial nuclear effects of the detonation. These injuries are classed as blast, thermal, or radiation injuries. Further radiation injuries may occur if you do not take proper precautions against fallout. Individuals in the area near a nuclear explosion will probably suffer a combination of all three types of injuries.

Blast Injuries

Blast injuries produced by nuclear weapons are similar to those caused by conventional high-explosive weapons. Blast overpressure can produce collapsed lungs and ruptured internal organs. Projectile wounds occur as the explosion's force hurls debris at you. Large pieces of debris striking you will cause fractured limbs or massive internal injuries. Blast over-pressure may throw you long distances, and you will suffer severe injury upon impact with the ground or other objects. Substantial cover and distance from the explosion are the best protection against blast injury. Cover blast injury wounds as soon as possible to prevent the entry of radioactive dust particles.

Thermal Injuries

The heat and light the nuclear fireball emits causes thermal injuries. First-, second-, or third-degree burns may result. Flash blindness also occurs. This blindness may be permanent or temporary depending on the degree of exposure of the eyes. Substantial cover and distance from the explosion can prevent thermal injuries. Clothing will provide significant protection against thermal injuries. Cover as much exposed skin as possible before a nuclear explosion. First aid for thermal injuries is the same as first aid for burns. Cover open burns (second-or third-degree) to prevent the entry of radioactive particles. Wash all burns before covering.

Radiation Injuries

Neutrons, gamma radiation, alpha radiation, and beta radiation cause radiation injuries. Neutrons are high-speed, extremely penetrating particles that actually smash cells within your body. Gamma radiation is similar to X rays and is also a highly penetrating radiation. During the initial fireball stage of a nuclear detonation, initial gamma radiation and neutrons are the most serious threat. Beta and alpha radiation are radioactive particles normally associated with radioactive dust from fallout. They are short-range particles and you can easily protect yourself against them if you take precautions.

Residual Radiation

Residual radiation is all radiation emitted after 1 minute from the instant of the nuclear explosion. Residual radiation consists of induced radiation and fallout.

Induced Radiation

It describes a relatively small, intensely radioactive area directly underneath the nuclear weapon's fireball. The irradiated earth in this area will remain highly radioactive for an extremely long time. You should not travel into an area of induced radiation.

Fallout

Fallout consists of radioactive soil and water particles, as well as weapon fragments. During a surface detonation, or if an airburst's nuclear fireball touches the ground, large amounts of soil and water are vaporized along with the bomb's fragments, and forced upward to altitudes of 25,000 meters or more. When these vaporized contents cool, they can form more than 200 different radioactive products.

The vaporized bomb contents condense into tiny radioactive particles that the wind carries and they fall back to earth as radioactive dust. Fallout particles emit alpha, beta, and gamma radiation. Alpha and beta radiation are relatively easy to counteract, and residual gamma radiation is much less intense than the gamma radiation emitted during the first minute after

the explosion. Fallout is your most significant radiation hazard, provided you have not received a lethal radiation dose from the initial radiation.

Bodily Reactions to Radiation

The effects of radiation on the human body can be broadly classed as either chronic or acute. Chronic effects are those that occur some years after exposure to radiation. Examples are cancer and genetic defects. Chronic effects are of minor concern insofar as they affect your immediate survival in a radioactive environment. On the other hand, acute effects are of primary importance to your survival. Some acute effects occur within hours after exposure to radiation. These effects result from the radiation's direct physical damage to tissue. Radiation sickness and beta burns are examples of acute effects. Radiation sickness symptoms include nausea, diarrhea, vomiting, fatigue, weakness, and loss of hair. Penetrating beta rays cause radiation burns; the wounds are similar to fire burns.

Recovery Capability

The extent of body damage depends mainly on the part of the body exposed to radiation and how long it was exposed, as well as its ability to recover. The brain and kidneys have little recovery capability. Other parts (skin and bone marrow) have a great ability to recover from damage. Usually, a dose of 600 centigrams to the entire body will result in almost certain death. If only your hands received this same dose, your overall health

would not suffer much, although your hands would suffer severe damage.

External and Internal Hazards

An external or an internal hazard can cause body damage. Highly penetrating gamma radiation or the less penetrating beta radiation that causes burns can cause external damage. The entry of alpha or beta radiation-emitting particles into the body can cause internal damage. The external hazard produces overall irradiation and beta burns. The internal hazard results in irradiation of critical organs such as the gastrointestinal tract, thyroid gland, and bone.

A very small amount of radioactive material can cause extreme damage to these and other internal organs. The internal hazard can enter the body either through consumption of contaminated water or food or by absorption through cuts or abrasions. Material that enters the body through breathing presents only a minor hazard. You can greatly reduce the internal radiation hazard by using good personal hygiene and carefully decontaminating your food and water.

Symptoms

The symptoms of radiation injuries include nausea, diarrhea, and vomiting. The severity of these symptoms is due to the extreme sensitivity of the gastrointestinal tract to radiation. The severity of the symptoms and the speed of onset after exposure are good

indicators of the degree of radiation damage. The gastrointestinal damage can come from either the external or the internal radiation hazard.

Countermeasures against Penetrating External Radiation

Knowledge of the radiation hazards discussed earlier is extremely important in surviving in a fallout area. It is also critical to know how to protect yourself from the most dangerous form of residual radiation - penetrating external radiation.

The means you can use to protect yourself from penetrating external radiation are time, distance, and shielding. You can reduce the level of radiation and help increase your chance of survival by controlling the duration of exposure. You can also get as far away from the radiation source as possible. Finally you can place some radiation-absorbing or shielding material between you and the radiation.

Time

Time is important to you, as the survivor, in two ways. First, radiation dosages are cumulative. The longer you are exposed to a radioactive source, the greater the dose you will receive. Obviously, spend as little time in a radioactive area as possible. Second, radioactivity decreases or decays over time. This concept is known as radioactive half-life. Thus, a radioactive element decays or loses half of its radioactivity within a certain time. The

rule of thumb for radioactivity decay is that it decreases in intensity by a factor of ten for every sevenfold increase in time following the peak radiation level. Even an untrained observer can see that the greatest hazard from fallout occurs immediately after detonation, and that the hazard decreases quickly over a relatively short time. As a survivor, try to avoid fallout areas long enough for most of the radioactivity to decay, you enhance your chance of survival.

Distance

Distance provides very effective protection against penetrating gamma radiation because radiation intensity decreases by the square of the distance from the source. Thus, when you double the distance, radiation decreases to (0.5)2 or 0.25 the amount. While this formula is valid for concentrated sources of radiation in small areas, it becomes more complicated for large areas of radiation such as fallout areas.

Shielding

Shielding is the most important method of protection from penetrating radiation. Of the three countermeasures against penetrating radiation, shielding provides the greatest protection and is the easiest to use under survival conditions. Therefore, it is the most desirable method. If shielding is not possible, use the other two methods to the maximum extent practical. Shielding actually works by absorbing or weakening the penetrating radiation, thereby reducing the amount of radiation reaching

your body. The denser the material, the better the shielding effect. Lead, iron, concrete, and water are good examples of shielding materials.

Special Medical Aspects

The presence of fallout material in your area requires slight changes in first aid procedures. You must cover all wounds to prevent contamination and the entry of radioactive particles. You must first wash burns of beta radiation, then treat them as ordinary burns. Take extra measures to prevent infection. Your body will be extremely sensitive to infections due to changes in your blood chemistry. Pay close attention to the prevention of colds or respiratory infections. Rigorously practice personal hygiene to prevent infections. Cover your eyes with improved goggles to prevent the entry of particles.

Shielding Materials

The thickness required to weaken gamma radiation from fallout is far less than that needed to shield against initial gamma radiation. Fallout radiation has less energy than a nuclear detonation's initial radiation. For fallout radiation, a relatively small amount of shielding material can provide adequate protection. Generally, the denser or heavier the material, the better shielding it offers. The degree of protection afforded by a fallout shelter is expressed as a "protection factor," or a "transmission factor." The protection factor is simply the fraction of available radiation dose which penetrates the shelter and

reaches those inside compared to the radiation received by an unprotected person. Thus, a protection factor of 2 indicates that an individual in the shelter receives one-half of the radiation dose they would receive if unprotected. A protection factor of 100 (associated with about six half-value thicknessess) indicates that only 1/100 or 1 percent of the radiation dose reaches those inside. Transmission factors are expressed in percentages, or in decimals. Either refers to that fraction of the ambient unshielded dose that is received by personnel within the shelter.