Global Security - Howard H. Baker Jr. Center for Public Policy

The Risks of Nuclear Facility Incidents

Dr. Brandon Prins & Dr. Krista Wiegand
Howard H. Baker Jr. Center for Public Policy
University of Tennessee, Knoxville

THE HOWARD H. BAKER JR CENTER FOR PUBLIC POLICY

Executive Summary

In this report, we provide an overview of the security environment confronting countries with sensitive nuclear facilities. First, we detail deliberate attacks on nuclear facilities and the vulnerabilities that expose these facilities to internal and external threats. Then, we review terrorist violence cross-nationally and over time, focusing specifically on attacks against critical infrastructure, such as chemical plants, oil pipelines, and ports. We find that infrastructure remains an atypical target of extremist groups in most countries. But, we also observe significant terrorist violence in a small sub-set of countries, some of which possess sensitive nuclear materials, including Pakistan, Nigeria, India, and Russia. In South Asia, in particular, we see substantial terrorism proximate to sensitive nuclear facilities. Next, we evaluate the risk of an accident at a nuclear facility before concluding with key takeaways and policy recommendations.

Table of Contents

1. Introduction

The purpose of this report is to examine the potential economic and political consequences of an incident at a nuclear facility, as well as to investigate terrorist activity worldwide as it relates to critical infrastructure. We present an overview of known incidents, a discussion of contrived scenarios, and an assessment of the probability of events and outcomes/consequences. Specifically, we examine the costs and consequences of insider/outsider attacks, sabotage, terrorism, accidents, and natural disasters. We provide analysis of how such incidents would affect other sites in the same region and internationally and the country where incidents occur, economically and politically. We conclude the report with policy recommendations.

Most of the focus on nuclear security is about the technical aspects of accident prevention, securing facilities (guards and gates), and responding to accidents, sabotage, insider threats, and terrorist attacks on nuclear facilities. Governments and employees working at nuclear facilities are trained on accident threat programs, they run through scenarios and exercises, and are familiar with the technical consequences of such threats or incidents. Here, we focus on the indirect costs of such threats and incidents from an economic and political perspective.

2. Overview of Deliberate Incidents

Extremist groups targeting nuclear sites or appropriating fissile material illicitly remains a paramount concern of security experts and intelligence analysts. Osama bin Laden sought material for a nuclear explosive device or dirty bomb and breaches at nuclear facilities demonstrate that these installations are not as secure as once thought. So, how vulnerable to terrorist attacks and security breaches are nuclear facilities and what would be the consequences of a successful attack or breach? In this section of the report, we assess the threat of nuclear terrorism, detail incidents of terrorism against infrastructure, consider public reports on nuclear facility breaches, and evaluate the policy implications of nuclear facility vulnerability to extremist group targeting.

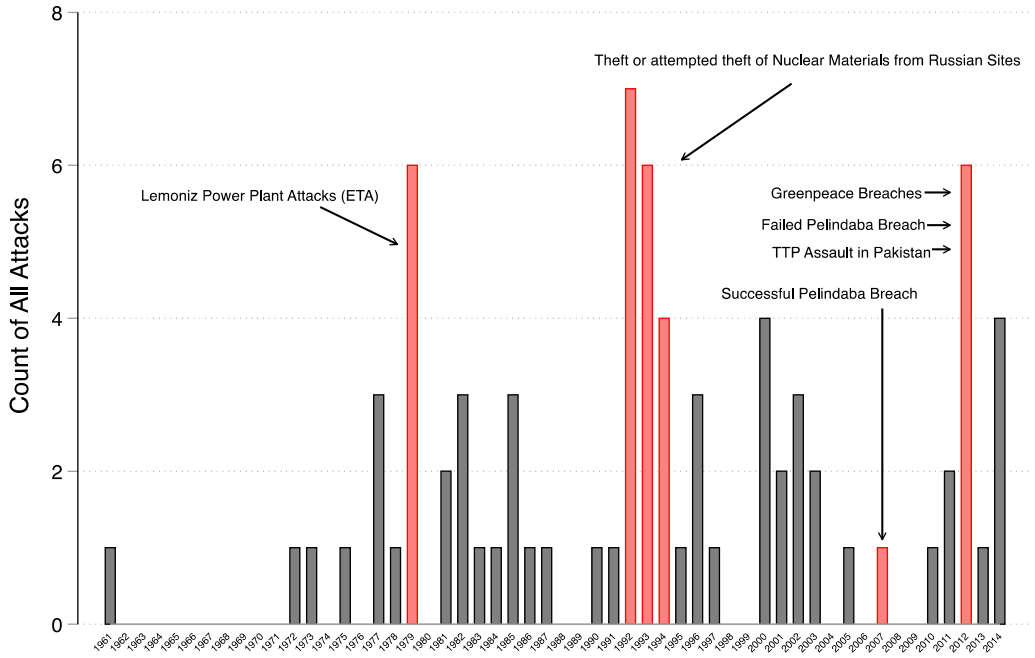
2.1 Attacks against Nuclear Facilities (NuFAD Data)

The START program at the University of Maryland collects data on security breaches at all facilities that house or are designed to house fissile material. Between 1961 and 2014 a total of 80 attacks have been recorded (see Figure 1).[1] Many of these attacks were designed to draw attention to the environmental costs associated with nuclear power, such as the attack against the Trojan nuclear power plant in Ranier, Oregon in October of 1977 by an anti-capitalist, California-based group called the New World Liberation Front. A bomb was detonated near the plant's visitor center. Other breaches have been more serious. For example, a breach took place in 1992 at the Ignalina nuclear plant in Visaginas, Lithuania. Employees of the plant smuggled a fuel assembly unit out of the plant that contained approximately 100kg of low-enriched uranium. The perpetrators were apprehended by authorities and most of the nuclear material recovered. However, the very fact that a 500-pound assembly unit could be smuggled out of the plant triggered security concerns among experts and political elites.

Some of the most serious breaches occurred at facilities in Russia in the early 1990s following the collapse of the Soviet regime. Between 1991 and 1994, at least 16 incidents occurred at facilities in Russia or former Soviet satellite countries, such as Lithuania and Moldova. Most of the breaches involved employees surreptitiously removing nuclear material from facilities for resale on the black market. In 1992, an employee of the Luch nuclear facility in Podolsk, Russia, which is located about 22 miles from Moscow, removed approximately 1.5 kilograms of highly enriched nuclear material

over a five-month period (NuFAD; Atomic Archive). The missing nuclear material had not been noticed when the perpetrator was arrested by Russian authorities for unrelated criminal activity (PBS). In another incident, a naval officer and partners stole approximately four kilograms of HEU from the Severomorsk Naval Yard in Russia. The perpetrators were caught and served prison time. More recently, Moldovan authorities arrested six individuals attempting to sell 2 pounds of highly enriched uranium (BBC).

Figure 1: Attacks against Sensitive Nuclear Facilities, 1961-2014 (NuFAD[2])



Perhaps the most dangerous breach of a nuclear facility occurred in South Africa in 2007. Four armed men broke into a nuclear facility that held hundreds of kilograms of highly enriched nuclear material. The attackers ultimately failed to acquire any of the nuclear material from the storage vault, but the very fact that they successfully entered the facility remains concerning (Washington Post). The 2007 Pelindaba incident is one of only two attacks recorded by the Global Terrorism Database at the University of Maryland. The only other attack listed in the GTD is a rocket assault by Hamas against the Dimona nuclear reactor site in Israel in 2014 (NTI).

2.2. Identifying Countries with Sensitive Nuclear Material

At least 32 countries historically have held militarily relevant nuclear material according to Fuhrmann and Tkach's Nuclear Latency Dataset (Fuhrmann and Tkach 2015).[3] Approximately 19 currently possess these materials. Militarily relevant refers to the ability to enrich uranium and or separate plutonium for a weapon. The sites in the NL dataset include the hot cell facility in Algeria, reprocessing facilities in Argentina, and an enrichment laboratory in Japan. All of these sites are designed to contain sensitive nuclear material that could be used by extremists to fashion a nuclear explosive device (although admittedly nuclear material was not introduced to some of the sites). Several facilities in the five nuclear weapons states (and India, Pakistan, and North Korea) are un-

regulated by the IAEA and thus not subject to safeguards and international inspections. While facilities in the non-nuclear weapons states are theoretically regulated by the IAEA, staffing and resource shortages at times mean that some of the 700+ facilities and other sites are not inspected. Some facilities are particularly vulnerable to outside and inside threats. The Nuclear Threat Initiative ranks 22 countries with at least 1 kilogram or more of weapons-usable nuclear material (both highly enriched uranium and separated plutonium) for security surrounding their nuclear facilities. South Africa, for example, ranks in the bottom quarter of countries ranked (17 out of 22). NTI notes significant weaknesses when it comes to the transit of nuclear materials, insider threat prevention, onsite physical protection of facilities, and an ineffective security culture (see Table 1 below). The NTI also finds many of Pakistan's nuclear facilities vulnerable to insider threats and notes a heightened risk environment driven by political instability, corruption, and extremist group activity. Clearly, more needs to be done to reduce the vulnerability of nuclear sites and facilities to internal and external threats.

Table 1: Countries with Militarily Relevant Nuclear Materials and Nuclear Security Rank, 2020

Country (# of Militarily Relevant nuclear facilities)	Year Joined IAEA	Operational as of 2012	Number Regulated by IAEA	Militarily Relevant (Uncertain)	NTI Nuclear Security Rank
Algeria (1)	1963	1	1	0 (1?)	
Argentina (4)	1957	2 (no material)	1	1 (1?)	
Australia (2)	1957	0	2	0 (1?)	1
Belgium (1)	1958	0	1	0	8
Brazil (7)	1957	3	5	5	
Canada (3)	1957	0	1	2	2
China (18)	1984	11	4	9 (2?)	14
Czech Rep. (1)	1993	0	1	0	
Egypt (1)	1957	1	1	1	
France (24)	1957	4	6	15	12
Germany (8)	1957	3	8	0	4
India (10)	1957	9	0	2 (4?)	19
Iran (10)	1958	5	10	10	21
Iraq (9)	1959	1 (no material)	0	9	
Israel (4)	1957	4	0	4	16
Italy (4)	1957	0	4	0	11
Japan (9)	1957	2	9	0	6
Libya (3)	1963	0	0	3	
Netherlands (5)	1957	2	5	0	5
North Korea (3)	1974-94	2	1	3	22
Norway (2)	1957	0	0	0	7
Pakistan (8)	1957	6-8	1	8	20
Romania (1)	1957	0	0	1	
Russia (33)	1957	11-12	1	30 (2?)	17
South Africa (5)	1957	1	3	3 (1?)	17

South Korea (4)	1957	1	1	0 (2?)	
Spain (1)	1957	0	0	0 (1?)	
Sweden (2)	1957	0	0	2	
Taiwan (3)	NPT bound	1 (no material)	3	3	
U.K. (21)	1957	5-6	12	7 (3?)	9
U.S. (44)	1957	10	5	31 (2?)	9
Serbia (4)	2001	0	0	4	

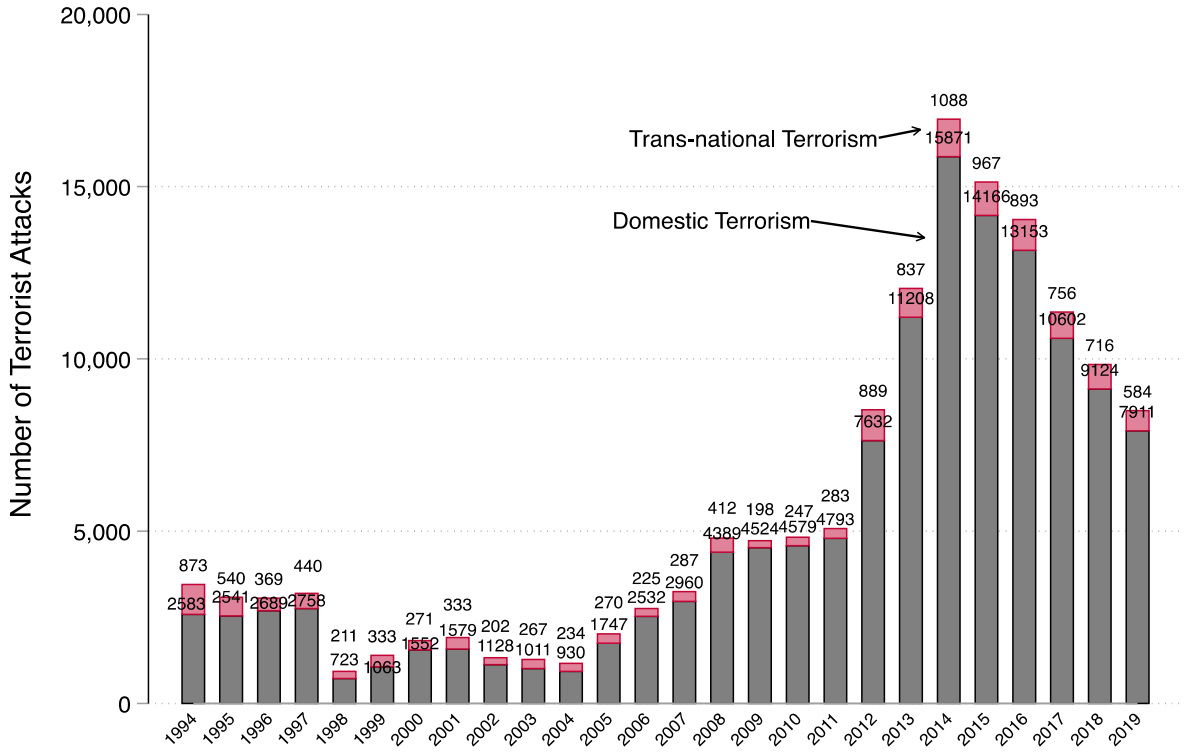
3. Trends in Extremist Violence

Extremist group attacks against nuclear infrastructure have heretofore been rare. As noted above, only two instances are recorded in the Global Terrorism Database: one against the Pelindaba nuclear facility in South Africa in 2007 and the rocket attack against the Dimona nuclear reactor by Hamas in 2014. The targeting of other infrastructure has been more common, even if still unlikely. But, it may be useful to assess terror attacks against important infrastructure to gauge how common such targets are and whether certain groups find infrastructure targets useful in their anti-state campaigns.

3.1 Terrorist Attack Trends, 1994-2019

Since 1994, terrorism has increased substantially, driven largely by conflicts in Iraq, Syria, Afghanistan, Nigeria, Pakistan, and India. The vast majority of this extremist violence remains associated with domestic insurgencies and therefore has little to do with the U.S. or other international actors. Transnational terrorism represents only a small subset of all extremist violence, but this type of attack has also increased since 2011 (see Figure 2 below).

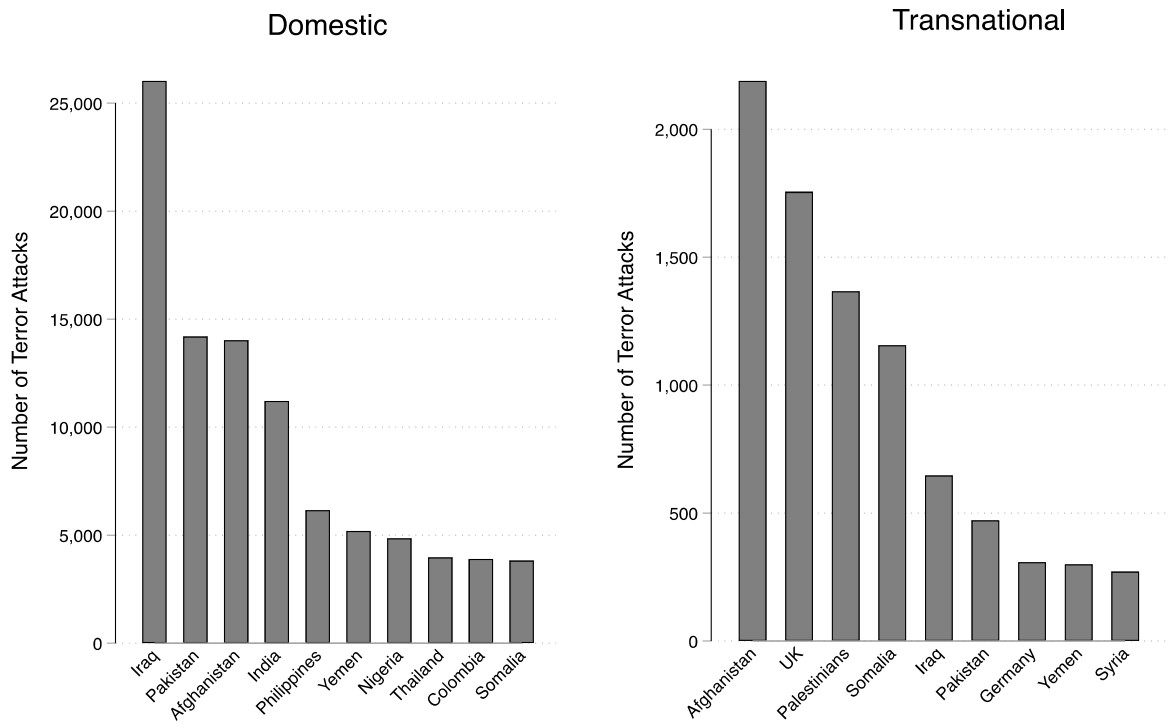
Figure 2: Domestic and Transnational Terrorism Attacks, 1994-2019



3.2. Domestic vs. Transnational Terrorism

The Taliban in Afghanistan and the Houthi rebels in Yemen have engaged in some of the most extensive transnational violence over the past decade. Beginning in about 2005, the Taliban began targeting US and NATO forces stationed in the country using improvised explosive devices (IEDs) and suicide bombings; tactics modeled after similar actions used by insurgents in Iraq. The targeting of foreign soldiers by Islamic extremists was also evident in Iraq and Somalia (see Figure 3 below). Houthi rebels have targeted Saudis with both rocket attacks and bombings meant to impose costs on Saudi regime and end the foreign military intervention into Yemeni territory.

Figure 3: Domestic and Transnational Terrorism, 1994-2019[4]

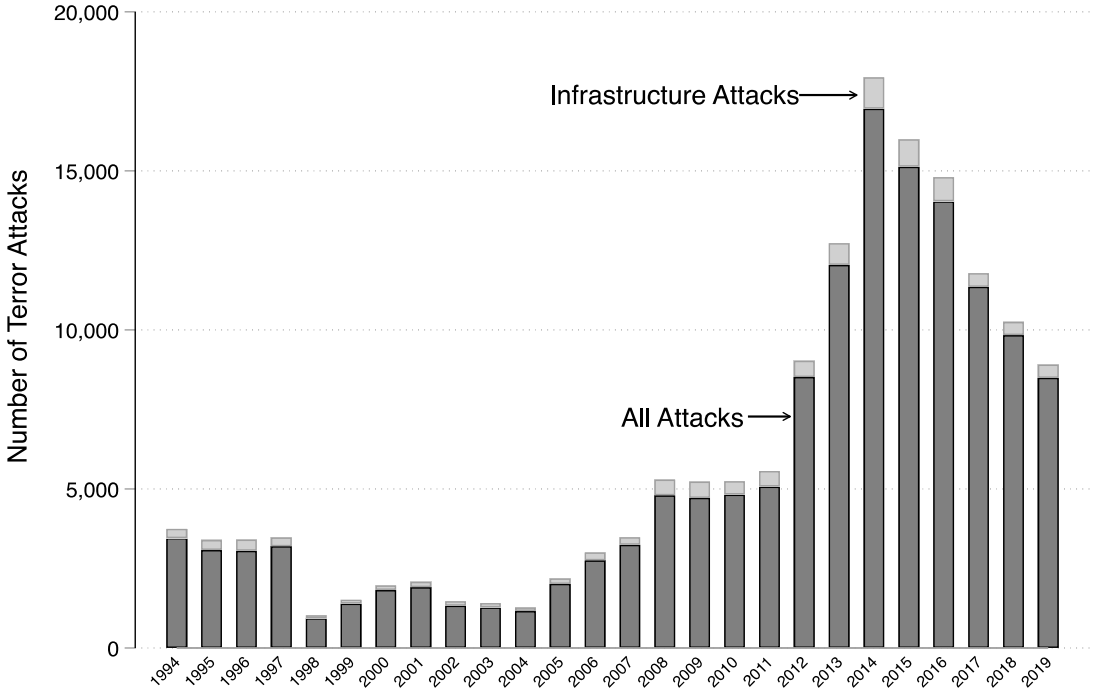


Because the occurrence of terrorist violent against nuclear sites is so low, a better measure might be to examine attacks against critical infrastructure more generally. As noted above, only two recorded attacks against nuclear facilities by terrorist groups have been recorded by the Global Terrorism Database at the University of Maryland. The Pelindaba attack in 2007 and the rocket attack against the Dimona reactor in 2014. However, exploring terrorist attacks against critical infrastructure, such as chemical plants, electrical grids, and gas pipelines, might provide useful information about the willingness of certain groups to target a nuclear facility. Further, it could help identify extremist organizations that have the tactical capacity to launch such attacks.

3.3 Terrorist Violence Targeting Infrastructure

Infrastructure remains an atypical target of terrorist groups (see Figure 4 below). Only about 7% of terrorism incidents recorded by GTD from 1994-2019 were directed against infrastructure, including airports, telecommunications, ports, bus and train depots, utilities, roads and bridges. Most infrastructure targeting has arisen in countries suffering from civil war and is part of an anti-state strategy by rebels to impose harm on the regime and its leaders and perhaps provoke regime over-reaction. Colombia, India, Iraq, and the Philippines have witnessed the largest share of infrastructure-directed terrorism, and much of this violence has targeted utilities, such as oil and gas facilities, and electrical transformers and wires. About 22% of the terrorist attacks in Colombia targeted infrastructure, compared to only 7% globally. As a percentage of all terrorism incidents, Iraqi infrastructure attacks is considerably lower than what Colombia has experienced. But because Iraq has suffered so much more terrorism, the total number of attacks against infrastructure targets remains the second highest over the 1994-2019 period (at nearly 1200 incidents). Only Pakistan has endured more terrorism directed against its infrastructure over the same 26-year period.

Figure 4: Terrorist Attacks Targeting Infrastructure, 1994-2019



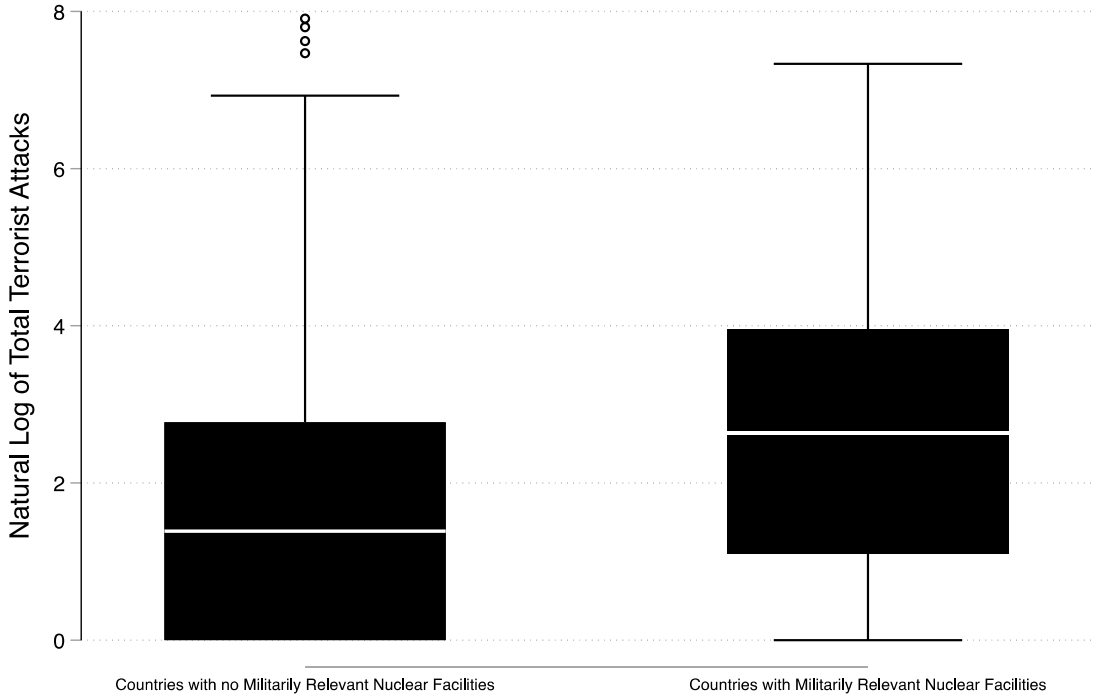
3.3.a. Types of Infrastructure Targeted by Extremist Groups

Similar to nuclear facilities, terrorist targeting of chemical plants and oil pipelines remains rare. From 1994-2019 there have been only 19 recorded attacks against chemical plants, factories, and weapons facilities worldwide. In the early 1990s, FARC in Colombia targeted petro-chemical facilities in two instances, and 10 years after that the ETA in Spain hit two chemical plants. In 2015, Ukrainian separatists struck several chemical plants. There appears to be only one incident of a chemical facility being hit by an Islamic extremist group; this occurred in Iraq in 2015 when a chemical facility was hit by ISIL, killing at least 22 Iraqis. While chemical plants do not appear to be targets of choice for Jihadi groups, fashioning some type of chemical explosive device was an objective of ISIL when it dominated parts of Iraq and Syria and may still be an objective of the group today. ISIL may have obtained chemical munitions from the extensive supply found in both Iraq and Syria. Territory around Mosul, Iraq, controlled previously by ISIL, did include facilities where chemical weapons were produced and stored. While some Islamic extremist groups may contemplate a chemical attack against a western target, the overall risk of such an event transpiring remains quite low. The lethality of such an attack, if it were to occur, is also expected to be modest.

Oil pipelines have been a more common target of some violent non-state actors. FARC in Colombia and Niger Delta groups in Nigeria have been the most active in targeting oil pipelines as part of their insurgencies. However, ISIL also targeted oil pipelines and natural gas plants in Iraq several times between 2004 and 2016.

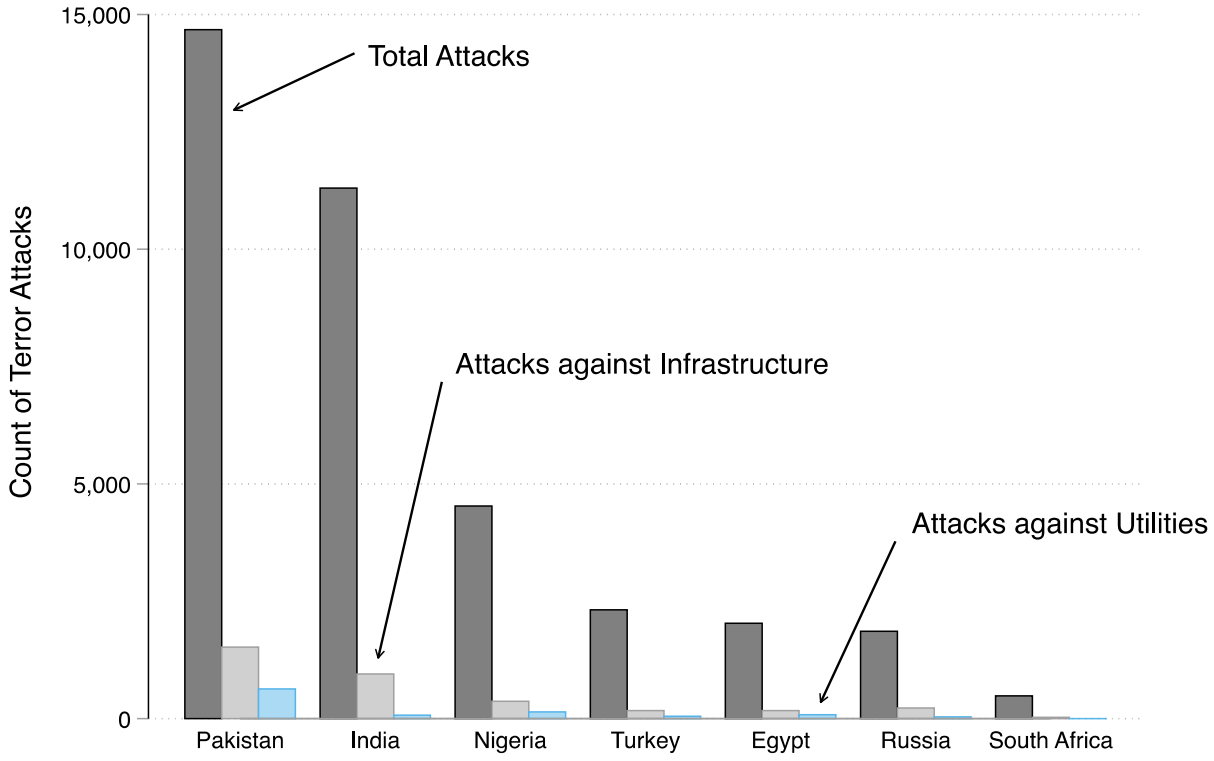
While evidence currently suggests infrastructure remains an unlikely target of extremist violence, countries with militarily relevant nuclear facilities do experience more terrorism than countries without such facilities. Figure 5 below plots the number of terrorist attacks in countries with and without militarily relevant nuclear facilities. To reduce the variance in the terrorism data, the natural log of the data series is shown. There are approximately twice as many terrorism incidents in countries with sensitive nuclear material than countries that don't possess such materials.

Figure 5: Number of Terrorist Attacks in Countries with and without Militarily Relevant Nuclear Facilities, 1994-2019



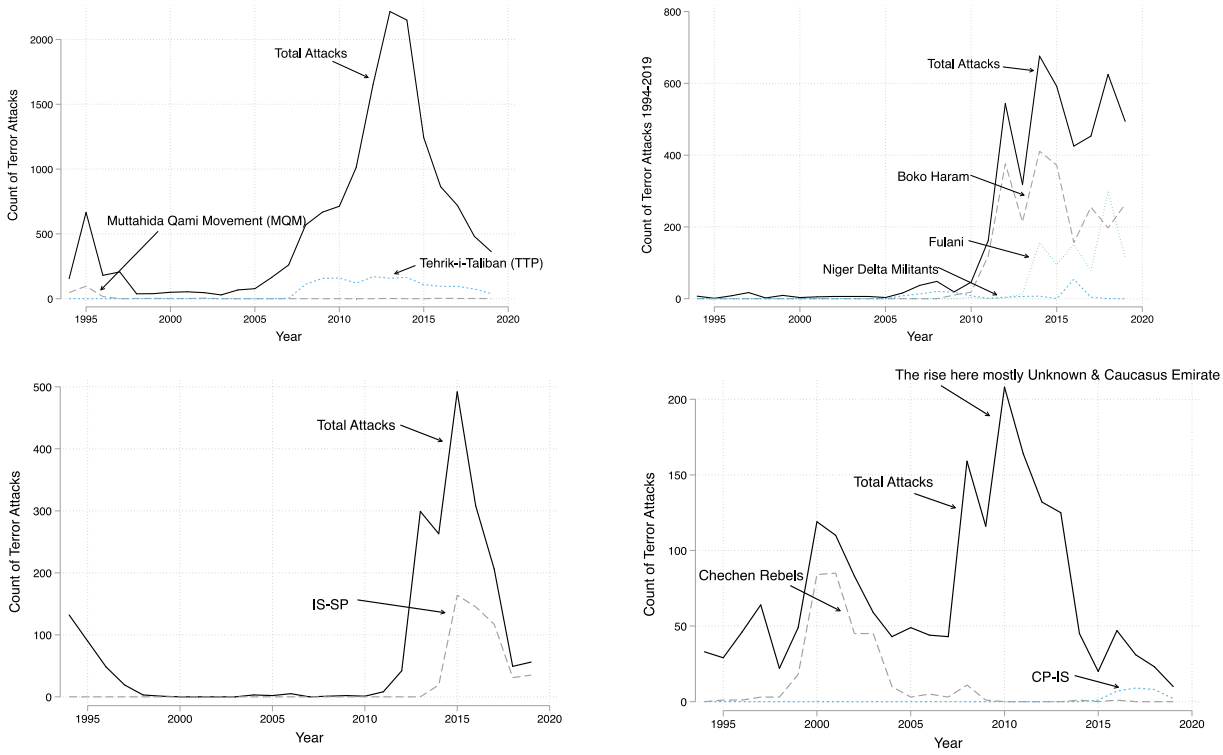
While nuclear facilities have not been the targets of extremist groups, the amount of extremist violence in countries with facilities to enrich uranium or extract plutonium is concerning. In fact, four of the countries identified by NTI as having nuclear facilities vulnerable to insider and external threats experience significant terrorist violence. These countries include Pakistan, India, Russia, and Nigeria (see Figure 6 below).

Figure 6: Vulnerable Countries to Terrorist Violence



Pakistan represents a clear threat to nuclear security given its combination of nuclear material and violent extremism. But other Jihadi, or Jihadi-inspired groups, remain dangerous and have increased their activity in several countries with nuclear material or nuclear ambitions. Boko Haram in Nigeria, IS-SP in Egypt, IS-CP in Russia, and numerous Islamic extremist groups in India persist and represent clear and present dangers (see Figure 7 below). To be clear, these groups largely have local grievances and they mostly focus their efforts domestically. They do not strike targets abroad. Still, nuclear material located locally may be attractive for raising revenue or in negotiations with regime elites. Hardening facilities, improving insider threat awareness, and eliminating superfluous nuclear materials must be a core goal of political elites worldwide. Matt Bunn, Associate Professor at Harvard University and one of the principal investigators for Harvard's project on Managing the Atom maintains that all nuclear stockpiles everywhere need to be protected from insider and outsider attempts to steal them.

Figure 7: Dangerous Extremist Groups in Pakistan, Nigeria, Egypt and Russia 1994-2019

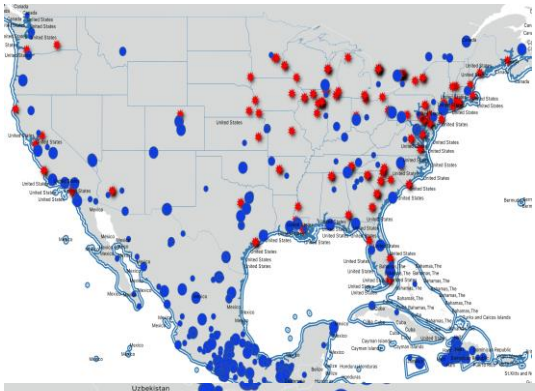


3.3.b. Location of Nuclear Reactors and Terrorist Violence

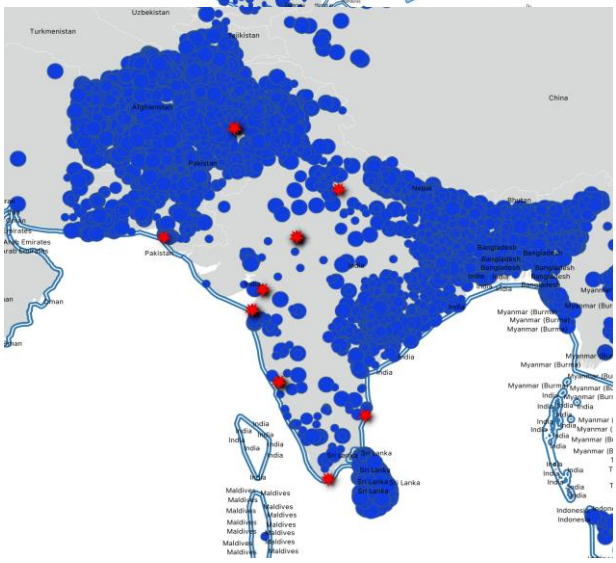
Importantly, while nuclear facilities have generally not been targets of terrorist groups, terrorist violence occurs proximate to nuclear reactors in many countries. This is concerning and reinforces Matt Bunn's call to secure all nuclear material from internal as well as external threats. Figure 8 below shows the location of 443 nuclear reactors in operation worldwide in 2021. Thirty countries currently have operational nuclear reactors, some located nearby to active extremist groups engaged in insurgent campaigns that target the government.

Figure 8: Location of Nuclear Reactors (red dots) and Terrorist Attacks (blue dots)[5]

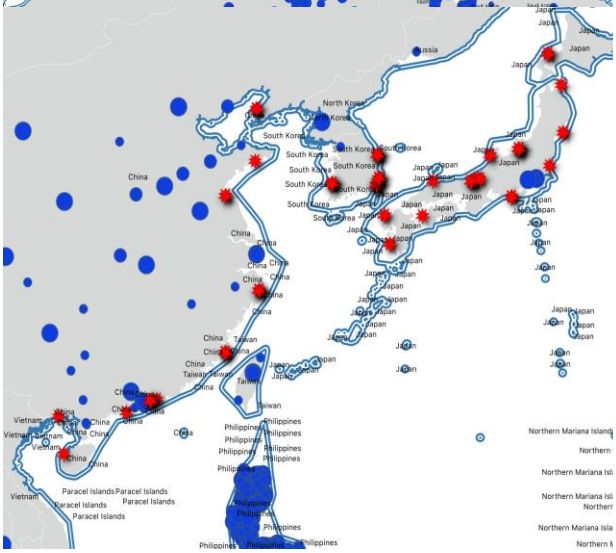
a. United States



b. Europe, Russia, and Asia Minor



c. South Asia



d. East Asia

3.3.c Cyber Attacks by Violent Non-State Actors

Cyber-attacks against critical infrastructure have arguably been increasing over the past several years. On July 22, 2021, for example, a state-owned company in South Africa experienced an attack against its IT networks. The company, Transnet, manages important infrastructure in South Africa, such as rail and port facilities, as well as oil pipelines. The attack disrupted cargo operations at ports in Cape Town and Durban. Little is known yet about the perpetrator, but the attack was costly and exposes how vulnerable domestic infrastructure may be to cyber-attacks. Ports in Barcelona, Spain, San Diego, California and Antwerp, Belgium have also been subject to cyber criminals. One cyber-security firm, Mission Secure, reported a 900% increase in maritime network attacks between 2018 and 2020, and other critical infrastructure, such as oil pipelines and electrical grids, have been targeted in ransomware attacks over the past few years.

Despite fears that extremist groups might employ hackers to damage critical infrastructure, so far terrorists have not employed this tactic in their operations. This may seem odd since terrorist groups arguably might exploit vulnerable networks to cause damage and generate media attention. The ransomware attack on the Colonial pipeline disrupted fuel supplies in the Southeast United States and created a mild shortage panic that led to runs on fuel at local gas stations. Extremists might also use

cyber-attacks to raise needed revenue for their operations. Targeting airports, dams, and water supplies might produce even more fear and disorder. No publicly-available datasets currently exist on cyber-attacks by extremist groups. This means that we really don't know much about whether this tactic is attractive to terrorist groups. More prevalent, though, are cyber-attacks by states, or state-sponsored non-state groups, that target companies, infrastructure, and government agencies of rival states. The U.S. government accuses both Russia and China of cyber-operations that are directed at disrupting economies, spreading disinformation, and espionage.[6] Countering such state efforts needs to be a core focus of the U.S. and its allies.

4. Accidental Incidents at Nuclear Facilities

In addition to deliberate attacks at nuclear facilities, the other type of incident to consider is accidents caused by internal errors and natural disasters. Though there is human involvement, these incidents are unintentional and difficult to prevent with certainty. While there have been very few large-scale accidents at nuclear facilities – Three Mile Island, Chernobyl, and Fukushima being the exceptions, there have been many small-scale accidents that have caused temporary or in some cases permanent shutdown of facilities. Between 1994 and 2011, there were 38 accidents at nuclear power plants in 10 different countries (France, Germany, Hungary, India, Japan, Russia, Slovenia, Sweden, US, UK), resulting in 29 fatalities.[7] All of these accidents cost more than $1 million (in 2010 dollars), and many costs in the tens and hundreds of millions of dollars. A team of scholars from MIT estimated that between 2005 and 2055 there would be four major nuclear accidents based on expected growth of nuclear facilities.[8]

There is a significant debate about the reliability and safety of hazardous technologies such as nuclear material based on differing interpretations and assumptions about how organizations work. On one side is the belief that solid processes based on design features and protocols should prevent accidents.[9] The line of thinking is that because major accidents have happened so infrequently, the likelihood of other major accidents occurring is very unlikely. The assumption is that complex organizational designs compensate for potential human error, and "can therefore be significantly more rational and effective than can individuals."[10] On the other side of the debate, there are experts who argue that accidents are inevitable due to the complexity of organizations that control nuclear material.[11]

While most of the debate about accident probability in hazardous technologies like nuclear materials is focused on technical safety design, complex interactions, redundancy, and other organizational issues, several political factors can influence the likelihood of an accident occurring in a nuclear facility. In order for organizational designs to work, reliability and safety must be prioritized by not only the managers of the organizations, but also by political leaders. If there are conflicting objectives and interests between the management of the nuclear facilities and politicians and policy makers who hold the purse strings, this could have detrimental impact on the safety and security of nuclear facilities. There are also concerns about political leaders' unwillingness to provide sufficient funding for security for hazardous technologies like nuclear power plants. As Stanford's Scott Sagan notes, "even if political leaders desire increased safety, differences in prioritization of goals between an organization and its ostensible political authority can continue.[12]

Organizations will seek to maintain their autonomy against outside pressures and numerous studies have noted the degree to which tensions exist between an industry and a regulatory agency created by the political authorities to monitor its behavior." Without full support for funding security and training from politicians and policy makers, the organization cannot effectively operate in a way that can reliably reduce the possibility of an accident. Another concern could be conflicting interests of

the organization and political interests, which could impact funding for operating a facility, and more importantly security and prevention of accidents. Lastly, with the record of nuclear incidents being uncommon, especially large accidents like Chernobyl or Fukushima, nuclear operators and governments may become less vigilant, more complacent, reduce attention to nuclear security and safety.[13]

A broader political factor that could influence the potential for accidents in nuclear facilities is the political and economic stability of a country. In countries where there is political and social unrest and domestic instability, the stability of who controls nuclear materials could be problematic.[14] This is particularly concerning if a coup d'état takes place, in which a leader is removed, or civil war breaks out and rebel groups take temporary or permanent control of the government[15]. For example, in May 2014, the Islamic State of Iraq & the Levant (ISIL) captured a Syrian nuclear reactor site. In failing or failed states, and with unstable or transitional governments, the security and adequate funding for nuclear facilities could be put at risk, which could affect the potential for accidents.

Accidents are also more likely to occur in countries without previous experience with nuclear materials or newly acquired nuclear capabilities, particularly those with weapons potential.[16] Similarly, in some countries that have authoritarian regimes, corrupt governments, and governments that flout international law and respect for international institutions, the IAEA may not be able to conduct inspections of nuclear facilities. Without significant oversight and with the presence of corrupt officials, the potential for accidents could increase. In countries where corruption is a significant condition, human reliability assessments may be moot, with employees and management of nuclear facilities providing preference to certain contractors that are not effective with safety and security measures, for example. Even in countries with stable, democratic governments with sufficient oversight, inspections, and assessment, the relationship between the utility companies or governments that run nuclear facilities and politicians or lobbying groups could affect the safety and security protocols and spending at nuclear facilities. If actors - lobbying groups, firms, utilities, governments, the public - are promoting different interests, these could clash. Similarly, it is important to consider that there are different levels of influence at different levels of government, whether local, regional/state, or national. Understanding who is making energy policy decisions about nuclear safety and security at which government level is important. There are also issues of bureaucracy, with overlapping units within one government pushing for certain policies, the utility or facility itself pushing for other policies, in addition to standards set by the IAEA at the international level.

Another major political concern about the potential for accidents in nuclear facilities is that some governments lack both organizational and financial resources that are necessary to provide adequate technical and security features for nuclear facilities.[17] Without adequate funding for the necessary design, training, security, and redundancy systems needed to prevent accidents, the chances of human or technical error increase. Governments may need to weigh the costs of nuclear safety with increased energy costs because of public pressure.

5. Policy Implications & Key Takeaways

Overall, the probability of deliberate or accidental incidents occurring at nuclear facilities is fairly low. However, if and when these incidents occur, the consequences would likely be quite serious. Therefore, there is no question that it critical for the security of nuclear facilities and the training of employees be highly prioritized. The Nuclear Threat Initiative maintains a security index of countries with at least one kilogram of weapons-usable nuclear material. Currently, 22 states qualify for NTI's index. A number of countries that confront violent non-state actors also struggle to protect and secure their nuclear facilities and materials. Pakistan once again is at the top of list of countries that are vulnerable to nuclear sabotage and theft. Despite recent improvements, Pakistan still suffers from one

of the riskiest political environments, it possesses significant quantities of HEU and separated Plutonium, and refuses to join important global nuclear security initiatives, such as the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. Egypt is a concern as well. It does not suffer from the same risk environment as Pakistan, although the political environment remains dangerous. But, Egypt has work to do on insider threat detection and physical hardening of sites that house nuclear material.

Most infrastructure terrorism occurs in countries experiencing significant political violence. In 2019, Afghanistan, Yemen, India, Iraq, Nigeria, the Philippines and Pakistan accounted for the vast majority of these types of attacks. In these countries we also find some of the most dangerous extremist groups, some that may seek materials for an improvised nuclear explosive device. In 2016, President Barack Obama exclaimed that the risk of ISIS or another extremist group acquiring nuclear weapons remains "one of the greatest threats to global security." And Harvard's Graham Allison (2018) continues to maintain that the odds of an extremist group acquiring and detonating a nuclear device is about 50% over the next decade. Securing nuclear materials and loose nukes must be a focus of US efforts. But focusing on specific countries with the greatest risk environment should center these efforts. South Asia remains the most critical area, but Iran and North Korea cannot be ignored. These countries may be considered as high priority countries for the US to work with regarding nuclear security training. Still, physical protection and insider threat initiatives only get us so far. Global efforts must also focus on resolving the political conflicts driving nuclear development.

Unlike the lower probability of deliberate attacks on nuclear facilities as discussed above, the probability of accidents at nuclear facilities is higher. In addition to accidents that result from internal errors, natural disasters are increasingly impacting facilities, demonstrated by the Fukushima disaster. Together with the potential for deliberate attacks, the likelihood of some type of accident at a nuclear facility is overall fairly low. However, if and when these incidents occur, the political and economic consequences can be quite severe.

Notes

[1] The orange-colored bars in Figure 1 are meant to highlight some of the most salient breaches of nuclear facilities.
[2] The NuFAD database can be obtained for the University of Maryland's START program (https://www.start.umd.edu/nuclear-facilities-attack-database-nufad).
[3] The dataset can be obtained here: http://www.matthewfuhrmann.com/datasets.html.
[4] Data on terrorist violence comes from the Global Terrorism database created by the START program at the University of Maryland (https://www.start.umd.edu/gtd/). Transnational terrorism is defined by the different nationalities of perpetrators and victims, which GTD codes. So, attacks by Syrian terrorists against Americans qualifies as transnational terrorism, while attacks by Syrians against Syrians is domestic terrorism. The sizable scale differences in Figure 3 above are due to the much higher number of domestic terrorism events that are recorded each year. Terrorist violence as part of civil war struggles is much more common than attacks involving different nationalities for perpetrators and victims.
[5] Nuclear reactor data comes from the IAEA (pris.iaea.org). Terrorism data taken from the Global Terrorism Database.
[6] Holcomb, Franklin. 2020. "Countering Russian and Chinese Cyber-Aggression." CEOA. https://cepa.org/countering-russia-and-chinese-cyber-aggression/
[7] Sovacool, Benjamin K. and Scott Victor Valentine. 2012. *The National Politics of Nuclear Power: Economics, Security, and Governance*. Routledge Global Security Studies. Milton Park, Abingdon, Oxon: Routledge.
[8] Beckjord, E., S. Ansolabehere, J. Deutch, M. Driscoll, P. Gray, J. Holden, P Joskow, R. Lester, and E. Moniz. 2003. *The Future of Nuclear Power: An Interdisciplinary MIT Study*. Cambridge, MA: MIT Press.
[9] This is referred to as the *high reliability theory.* See La Porte, Todd R. and Paula M. Consolini. 1989. "Working in Practice but Not Theory: Theoretical Challenges of 'High Reliability Organizations,'" *Journal of Public Administration Research and Theory* 1 (1): 19-47; Marone, Joseph, G. and Edward J. Woodhouse. 1986. *Averting Catastrophe: Strategies for Regulating Risky Technologies*. Berkeley: University of California Press; Roberts, Karlene H. 1989. "New Challenges in Organization Research: High Reliability Organizations," *Industrial Crisis Quarterly* 3 (2): 111-125.
[10] Sagan, Scott D. 1993. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton: Princeton University Press, p. 16.
[11] Perrow, Charles. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books; Sagan 1993.
[12] Sagan, 1993, p. 38.
[13] Pidgeon, Nick, Irene Lorenzoni, and Wouter Poortinga. 2008. "Climate Change or Nuclear Power No Thanks! A Quantitative Study of Public Perceptions and Risk Framing in Britain," *Global Environmental Change* 18(1):69-85.
[14] Sagan, Scott D. 1995. "More Will Be Worse." In Scott D. Sagan and Kenneth N. Waltz, *The Spread of Nuclear Weapons: A Debate*. New York: Norton, 47-91.
[15] Seng, Jordan. 1997. "Less is More: Command and Control Advantages of Minor Nuclear States," *Security Studies* 6 (4): 50-92.
[16] Feaver, Peter D. 1997. "Neooptimists and the Enduring Problem of Nuclear Proliferation," *Security Studies* 6 (4): 93-125.
[17] Sagan 1995.