Hacking Nuclear Command and Control

Jason Fritz BS (St. Cloud), MIR (Bond)

Executive Summary

This paper will analyse the threat of cyber terrorism in regard to nuclear weapons. Specifically, this research will use open source knowledge to identify the structure of nuclear command and control centres, how those structures might be compromised through computer network operations, and how doing so would fit within established cyber terrorists' capabilities, strategies, and tactics. If access to command and control centres is obtained, terrorists could fake or actually cause one nuclear-armed state to attack another, thus provoking a nuclear response from another nuclear power. This may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves. This would also act as a force equaliser, and provide terrorists with the asymmetric benefits of high speed, removal of geographical distance, and a relatively low cost. Continuing difficulties in developing computer tracking technologies which could trace the identity of intruders, and difficulties in establishing an internationally agreed upon legal framework to guide responses to computer network operations, point towards an inherent weakness in using computer networks to manage nuclear weaponry. This is particularly relevant to reducing the hair trigger posture of existing nuclear arsenals.

All computers which are connected to the internet are susceptible to infiltration and remote control. Computers which operate on a closed network may also be compromised by various hacker methods, such as privilege escalation, roaming notebooks, wireless access points, embedded exploits in software and hardware, and maintenance entry points. For example, e-mail spoofing targeted at individuals who have access to a closed network, could lead to the installation of a virus on an open network. This virus could then be carelessly transported on removable data storage between the open and closed network. Information found on the internet may also reveal how to access these closed networks directly. Efforts by militaries to place increasing reliance on computer networks, including experimental technology such as autonomous systems, and their desire to have multiple launch options, such as nuclear triad capability, enables multiple entry points for terrorists. For example, if a terrestrial command centre is impenetrable, perhaps isolating one nuclear armed submarine would prove an easier task. There is evidence to suggest multiple attempts have been made by hackers to compromise the extremely low radio frequency once used by the US Navy to send nuclear launch approval to submerged submarines. Additionally, the alleged Soviet system known as Perimetr was designed to automatically launch nuclear weapons if it was unable to establish communications with Soviet leadership. This was intended as a retaliatory response in the event that nuclear weapons had

decapitated Soviet leadership; however it did not account for the possibility of cyber terrorists blocking communications through computer network operations in an attempt to engage the system.

Should a warhead be launched, damage could be further enhanced through additional computer network operations. By using proxies, multi-layered attacks could be engineered. Terrorists could remotely commandeer computers in China and use them to launch a US nuclear attack against Russia. Thus Russia would believe it was under attack from the US and the US would believe China was responsible. Further, emergency response communications could be disrupted, transportation could be shut down, and disinformation, such as misdirection, could be planted, thereby hindering the disaster relief effort and maximizing destruction. Disruptions in communication and the use of disinformation could also be used to provoke uninformed responses. For example, a nuclear strike between India and Pakistan could be coordinated with Distributed Denial of Service attacks against key networks, so they would have further difficulty in identifying what happened and be forced to respond quickly. Terrorists could also knock out communications between these states so they cannot discuss the situation. Alternatively, amidst the confusion of a traditional large-scale terrorist attack, claims of responsibility and declarations of war could be falsified in an attempt to instigate a hasty military response. These false claims could be posted directly on Presidential, military, and government websites. E-mails could also be sent to the media and foreign governments using the IP addresses and e-mail accounts of government officials. A sophisticated and all encompassing combination of traditional terrorism and cyber terrorism could be enough to launch nuclear weapons on its own, without the need for compromising command and control centres directly.

1. Cyber Terrorism

Cyber terrorism is a disputed term, just as terrorism itself has no universally accepted definition. Kevin G. Coleman of the Technolytics Institute defines cyber terrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives" (Cyber Operations and Cyber Terrorism 2005). This may include using the internet to recruit terrorists, gather information, disrupt infrastructure, or cause physical real-world harm, as they all lead to the ultimate goal of political change through fear and violence. At its most basic, cyber terrorism is the use of computer network operations to aid terrorism. Theoretical examples of cyber terrorism include hacking into the air traffic control system in order to cause two planes to collide, or causing severe financial loss by disrupting banks or the stock market (Denning 1999).

It is difficult to establish an act of cyber terrorism from similar and overlapping terminology. There are many individuals and groups who cause damage by using computers illegally; however they are not all cyber terrorists. Hackers, or more precisely blackhat hackers, exploit vulnerabilities in computer networks for fun,

profit, or bragging rights. They may steal sensitive data, or cause disruption, financial loss, and real-world physical damage, yet they typically do not intend to cause violence or severe social or economic harm. Hackers seem more interested in the technical capability, as though it were a game. Hactivists are activists who enhance their capabilities through computer skill. They may organise protests, deface websites, or use any number of techniques designed to disseminate their message. Cyber criminals are an extension of organised crime, and they are particularly interested in profit, such as extortion or credit card fraud. State sponsored (military) hackers, non-state sponsored political hackers, industrial espionage, and insiders also fall into their own subsets of cyber crime. These classifications can alter quickly. A cyber criminal or hacker could cross over into the realm of cyber terrorism by selling their services to terrorists, just as a hacker could become classified as a cyber criminal if they turn their focus to financial gain. The distinction between groups who use computer network operations is not of primary concern to this paper. What is of concern is whether or not these techniques could be used to compromise nuclear command and control.

Modus Operandi

Terrorists have a history of using asymmetric warfare to compete against their more powerful enemies. Computer network operations fit within this modus operandi. As nuclear capable states become more and more dependant on interconnected information technology for the military and civilian infrastructure, they become an increasingly viable target. Cyber terrorism offers multiple asymmetric benefits. It is relatively low cost, only requiring an off the shelf computer and an internet connection. A wide range of pre-written, automated, hacking tools are readily available on the internet and require little to learn. Cyber terrorism allows greater anonymity than traditional terrorism, as tracking the source of attacks is hindered by proxies, spoofed IP addresses, botnets, and legal hindrances. In terms of stealth, cyber terrorism allows for the silent retrieval of information from a computer, or the remote use of someone else's computer to conduct activities. Cyber terrorists can strike an enormous number of targets around the globe without having to be physically present, thereby reducing the risk of death or injury to the attacker. This enhances the speed of operations and eliminates the logistical problems of crossing borders. Reducing the risk of death, and the physical or psychological demands, makes it easier to recruit new members for their cause. Cyber terrorism has the potential to cause damage beyond the scope of traditional tactics, and when used in combination with traditional tactics, it can create synergy.

Enhancing Traditional Operations

In much the same way that the Information Revolution has enhanced the methods and capabilities of individuals, industry, and government, it has also enhanced the methods and capabilities of terrorism. Information gained on the internet can yield maps of installations, bus schedules to and from those installations, operating hours, photographs, telephone/e-mail directories, and so on. Much of this may be considered non-sensitive information on its own, but when pieced together it can reveal a picture which may have been deemed classified. A simple Google search can reveal valuable information such as lock picking, hacking software, bomb construction, or fake identification, all of which may play a role in the goal of acquiring a nuclear weapon.

The internet's ability to identify specific groups based on ethnicity, belief, or affiliation has enhanced the ability to recruit and target. This can be used to identify individuals who may possess pertinent knowledge, such as nuclear scientists or military personnel, who can be targeted with spoofed e-mails containing malicious code. In terms of recruitment, many terrorist organisations operate their own websites, complete with propaganda, donation collection, and information on how to join their cause. Examples include Hamas, Hezbollah, and FARC. Sunni insurgents in Iraq have used the internet to post articles and video which undermine coalition forces by glorifying terrorism, demonizing the coalition, and promoting their interpretation of events (Carfano 2008). Due to the global nature of the internet, authorities have difficulty in shutting down these sites as the web host may be located in foreign states with varying laws, and alternative hosts can be set relatively easily if one is shut down. This allows them to reach a worldwide audience.

Terrorists can use the internet as a covert means of communication. Even the most basic chat programs provide a level of anonymity. Additionally, encryption may be used all the way down to planting messages within the code of jpeg (image) files posted on image boards and comment threads. Telephone conversations routed through computers may also be encrypted. Some of the 9/11 hijackers booked their airline reservations online and used internet-based telephone services and chat software in the build up to the attack (Wilson 2003). Using the internet for communications circumvents many government controls, and allows easy access, high speed, and low cost. Online psychological warfare and the spreading of disinformation can instil fear, deliver threats, and destroy morale, such as the video release of captured soldiers, beheadings, and crashed helicopters posted on terrorist websites, which subsequently reach mass media. Recruitment, research, fund raising, propaganda, and communication have always been a part of terrorist activities, but they have been enhanced with the advent of the internet.

Hacker Skills

In order to see how hackers could penetrate nuclear command and control, it is important to examine some of the basic tactics of hacking. Payloads, such as viruses, worms, and Trojan horses, can infect a computer simply by getting a user to click on a link, open an e-mail attachment such as a pdf file, or run an executable program. Spoofing, or making something appear to be something it is not, is often used to accomplish this. Once one or several of these payloads are installed, they can spread to other computers; log all keystrokes, gaining passwords and usernames; download all of the contents on the hard drive; delete or re-write files; activate the microphone or webcam, sending that information back to the attacker; or shut down and possibly destroy the computer. Essentially a hacker can gain complete control of a computer from a remote location without the owner's knowledge. These exploits may also cause the computer to become a part of a botnet. Botnets are large numbers of computers (zombies) under illicit control which are banded together. These may be used in coordination to cause Distributed Denial of Service (DDoS) attacks. DDoS attacks are capable of shutting down web sites or portions of a network by flooding the server with data requests. These massive floods of data requests can cause buffer overflow, and jam the server, rendering it unusable. An exercise conducted by the US National Security Agency (NSA), named Eligible Receiver, showed that much of the private sector infrastructure in the US could be hacked, including telecommunications

and electronic grids. Hackers working in this exercise were also able to penetrate dozens of critical Pentagon computer systems and the US Pacific military's command and control system, were they could reformat hard drives, alter data, or shut systems down (Weimann 2004, Wilson 2003).

SCADA Systems

Supervisory Control and Data Acquisition (SCADA) systems are computer systems used for critical infrastructure such as energy grids, water management, waste treatment, transportation systems, emergency services, and communications. These systems "automatically monitor and adjust switching, manufacturing, and other process control activities, based on feedback data gathered by sensors" (Wilson 2003). These systems were intended to remain separate from the internet; however as organisations grew, and so did the internet, it became more cost effective to tie them together. In particular, with deregulation it became more important for offsite maintenance and information sharing. This makes them a valuable target for terrorists. In 2001, an "individual used the internet, a wireless radio, and stolen control software to release up to 1 million litres of sewage into the river and coastal waters of Queensland, Australia. The individual had attempted to access the system 44 times, prior to being successful in his 45th attempt, without being detected" (Cyber Operations and Cyber Terrorism 2005). Other examples of cyber attacks which have been conducted against these types of key infrastructure include: the disruption of emergency response by embedding malicious code into e-mail; disrupting air traffic control, including the ability to activate runway lights on approach; using a worm to corrupt the computer control systems of a nuclear power plant in Ohio; using a Trojan horse to gain control of gas pipelines; and using a worm to degrade utility companies and the power grid (Cyber Operations and Cyber Terrorism 2005, Lourdeau 2004, Wilson 2008, Denning 2000, Wilson 2003, and Poulsen 2004).

Is the threat real?

As of May 2009, no major cyber terror event has occurred. Policy makers, media organisations, and security companies often use the threat of cyber terrorism to further their own agendas. The entertainment industry has also capitalized on cyber fears, creating exaggerated and over simplistic scenarios, such as the films *War Games* and *Die Hard 4*. Additionally, the media often reports cyber criminals, hackers, state-sponsored hackers, and hacktivists all under the heading of cyber terrorists. Sensitive government, military, and intelligence information tend to be maintained on closed networks, networks separated from the broader internet. While these systems may be compromised, they are far from simple. Governments are aware of the cyber threat, and have been taking steps to increase personnel screening, inspections, inter-agency communication, emergency response, scrutiny of sensitive hi-tech foreign parts production, and overall computer network defence.

SCADA systems may be more robust than some reports have indicated. These systems are designed to be distributed, diverse, redundant, and self-healing, in part because weather systems and natural disasters pose a continual threat of disruption. A cyber attack against SCADA systems may require a sustained assault against multiple targets to have a significant effect. Additionally, humans remain in the loop. For example, reports that a terrorist could change the levels of iron in children's breakfast

cereal to toxic levels, neglects to account for the manual checks of assembly line workers, or the accounting procedures for the amount of iron in stock (Denning 1999). Al Qaeda computers recovered in Afghanistan revealed information on water systems and nuclear power plants. However this was more relevant to reconnaissance in support of a traditional physical attack. The degree to which these systems could cause massive disruption or death is debatable, as traditional explosives remain a more potent tool for that task. It may take years to prepare an attack against advanced networks, including the identification of exploits, development of tools, and the implementation of a plan, yet technology is rapidly advancing and networks continually updating, possibly disrupting those plans. Terrorist organisations may not be able to keep up with the massive financial backing of nation states. State-sponsored hackers have this problem themselves (Wilson 2003).

Despite the possibility of exaggerated claims, a threat remains. Computer network operations do pose an asymmetric weakness, one which terrorist could use to further their agenda, and one which fits within their doctrine. Just as the 9/11 attacks were an unprecedented attack with unconventional weapons, so too could a major cyber attack. Multiple cyber attacks on infrastructure have been documented, as mentioned in the SCADA Systems section above. A successful cyber attack requires finding only one vulnerability, whereas a successful cyber defence requires finding all possible vulnerabilities. As younger, more computer savvy, individuals are recruited into the ranks of terrorists, they may begin to recognise its potential. Just as the reliance on the internet is rapidly growing, so too are the weapons capable of damaging it. The 2005 Cyber Operations and Cyber Terrorism Handbook No. 1.02, notes:

> The Melissa virus that infected networks in 1999 took weeks to have an effect. However, the Code Red worm that infected the internet in July 2001 took only hours to flood the airways, while the Slammer worm that appeared in January 2003 took only minutes to infect thousands of hosts throughout the world. To further demonstrate the complexity of attacks, it took Code Red 37 minutes to double in size, but only took Slammer 8.5 seconds to do the same.

While government and corporate organisations have begun to publicly recognise the need for a strong cyber defence, it is uncertain to what degree they have taken action. Progress in developing the tools to track cyber terrorists runs into conflict with citizen's right to privacy—terrorists do not have such legal or social hindrances. Further, potential targets are not unified. For example, the financial sector, the commercial sector, home users, universities, and government networks are all attractive targets for terrorists, yet there is no coordination between these groups. Corporations and home users may not find stringent security measures to be worth the cost. In the event of an attack, there would also be considerable confusion as to the coordination of a relief effort (Carfano 2008, Lewis 2002).

Outsourcing

Cyber terrorists may not need sophisticated hacking skills themselves, they may be able to purchase them for cyber criminals. Insiders, such as Vitek Boden, who released sewage into the Australian waterways, could be identified through traditional cyber activities (Smith 2001). In 2000, Japan's Metropolitan Police Department reported that they had obtained an illicit software program that could track police vehicles. The program was developed by The Aum Shinryko cult, the group

responsible for the 1995 sarin gas attacks on the Tokyo subway system. Additionally, the cult had developed software for 80 Japanese firms and 10 government agencies, leading to concerns that they had installed Trojan horses to launch or facilitate cyber terrorist attacks at a later date. (Cyber Operations and Cyber Terrorism 2005, Weimann 2004, Denning 2000). Insiders can use flash drives, such as thumb drives, portable gaming devices, mobile phones, or mp3 players, for the clandestine and rapid downloading of information, or the rapid uploading of a malicious payload used to aid in future attack.

Botnets can be rented from cyber criminals, known as botherders, for as little US$200 to $300 per hour. And the nature of botnets, being composed of hundreds or thousands of computers around the globe, makes the source difficult to track. The number of zombie computers in the world grew by 12 million in the first 4 months of 2009 alone (Zetter 2009). Identity theft can also be purchased online, including valuable items for terrorism, such as stolen credit card numbers, driver's licences, birth certificates, reference letters, and bank accounts. The Provisional Irish Republican Army hired hackers to acquire the personal information of law enforcement and intelligence officers, which they intended to use in assassination plans if the British government did not meet their terms for a cease fire (Denning 2000). Evidence of a link between cyber criminals and terrorists is continuing to grow. For example, three British citizens used stolen credit card data to purchase night vision goggles, tents, GPS devices, prepaid mobile phones, and airline tickets to "assist fellow jihadists in the field" (Wilson 2008). In 1998, Khalid Ibrahim, a member of the militant separatist group Harkat-ul-Ansar, attempted to buy military software from hackers who had penetrated the US Department of Defense, and in 2008, it was revealed that a principal software engineer for Yahoo India was also the head of internet operations for the Indian Mujahedeen (Rahman 2008, Denning 1999).

2. Nuclear Command and Control

In order to see how cyber terrorists could detonate a nuclear weapon it is important to identify the structures which they would be attempting to penetrate. Nuclear command and control (NC2), sometimes referred to as nuclear command and control and communications (NC3) includes the personnel, equipment, communications, facilities, organisation, procedures, and chain of command involved with maintaining a nuclear weapon capability. A Command and Control Centre is typically a secure room, bunker, or building in a government or military facility that operates as the agency's dispatch centre, surveillance monitoring centre, coordination office and alarm monitoring centre all in one. A state may have multiple command and control centres within the government and military branches which can act independently or, more commonly, be used in the event a higher node is incapable of performing its function. A minimum of eight states possess a nuclear arsenal, providing eight varying nuclear command and control structures for cyber terrorist to target. The eight states which possess nuclear weapons are, in order of acquisition, the US, Russia (former Soviet Union), the UK, France, China, India, Pakistan, and North Korea. South Africa formerly possessed nuclear weapons, but has since dismantled its arsenal. Israel is also widely believed to have nuclear weapons, but has not officially confirmed their status as a nuclear state. There are approximately 20,000 active nuclear weapons in the world. The vast majority of these belong to the US and Russia, stemming from the Cold War.

Nuclear command and control has inherent weaknesses in relation to cyber warfare. The concept of mutually assured destruction means a state must have the capability to launch nuclear weapons in the event of a decapitating strike. This requires having nuclear weapons spread out in multiple locations (mobility and redundancy), so an enemy could not destroy all of their capabilities. Examples of this include land based mobile launch platforms and submarine-launched ballistic missiles (SLBM). This provides terrorists with multiple locations for attaining access to these weapons. Further, under NATO nuclear weapons sharing, the US has supplied nuclear weapons to Belgium, Germany, Italy, the Netherlands, and Turkey for storage and possible deployment. This further increases the number of access points for terrorists, allowing them to assess not only installations and procedures, but also which borders and state specific laws may be easier to circumvent. The weapons themselves may all be under the complete control of the US, but the operational plans of terrorists may include items such as reconnaissance, social engineering, and crossing borders which remain unique between states. The potential collapse of a state also presents a challenge. Following the collapse of the Soviet Union, Belarus, Kazakhstan, and Ukraine were in possession of nuclear weapons. These have since been transferred to Russia, but there was, and still is, considerable concern over the security and integrity of those weapons, especially in the face of a destabilized government and civilian hardship. Mutually assured destruction also promotes a hair trigger launch posture and the need for launch orders to be decided on quickly. The advent of SLBMs increased this high pressure tension, as the ability of a submarine to sneak up close to a state's border before launch significantly reduced response time. These short decision times make it easier for terrorists to provoke a launch as little time, and little discussion, is given to assess a situation in full. The desire to reduce the time it takes to disseminate plans to nuclear forces may expand the use of computers in nuclear command and control, or lead to the introduction of fail-deadly and autonomous systems.

This chapter is by no means comprehensive, However it sheds some light on the operations of nuclear command and control and the difficulties in defending those systems from cyber terrorism. Many of the details of nuclear command and control are classified, so the information provided below may be outdated. However it points towards a pattern, and there is no certainty these systems and procedures have been updated since entering open source knowledge. Further, terrorists do not have to restrict themselves to unclassified data, and therefore may be able to obtain up to date information.

The United States

The US employs a nuclear deterrence triad consisted of nuclear-capable long range bombers, SLBMs, and land based intercontinental ballistic missiles (ICBMs), as well as an arsenal of nonstrategic (tactical) nuclear weapons. US nuclear command and control covers a geographically dispersed force with the US President, as Commander in Chief, being the highest authority in the decision to make a nuclear launch. There is a hierarchy of succession in the event the President cannot perform this duty, such as if the President were killed in an attack. Additionally, once the order to launch is given, it travels down a chain of command; the President does not press the button, so to speak, nor is the President physically present at the launch location. These

locations would be targets in a nuclear war, so it is imperative that the leader not be there. Additionally, multiple independent launch locations make this impossible (except for cases in which multiple missiles are tied together in a Single Integrated Operational Plan). So it is theoretically possible to subvert this control by falsifying the order at any number of locations down that chain of command. The infrastructure that supports the President in his decision to launch nuclear weapons is the Nuclear Command and Control System (NCCS). "The NCCS must support situation monitoring, tactical warning and attack assessment of missile launches, senior leader decision making, dissemination of Presidential force-direction orders, and management of geographically dispersed forces" (Critchlow 2006).

Key US nuclear command centres include fixed locations, such as the National Military Command Center (NMCC) and the Raven Rock Mountain Complex (Site R), and mobile platforms, such as the E-4B National Airborne Operations Center (NAOC) and the Mobile Consolidated Command Center (MCCC). The US seeks to integrate its nuclear forces into its vision of command, control, computers, communications, intelligence, surveillance, and reconnaissance (C4ISR) hinting towards a greater reliance on computer technology in maintaining and upgrading its nuclear force, not only to combat against Cold War style nuclear war, but also against perceived emerging threats from China, Iran and North Korea. In particular the US recognises these states' potential to use nuclear weapons detonated at high altitude to create an electromagnetic pulse (EMP). The threat of EMP was known during the Cold War, and a considerable amount of attention has been paid to hardening nuclear systems (Critchlow 2006).

The Minimum Essential Emergency Communications Network (MEECN) links to the ICBMs, bombers, and submarine forces. Information widely available on the internet shows the US is seeking to upgrade the MEECN's satellite communications capability through Advanced Extremely High Frequency and the Transformational Communications Satellite programs. Cyber terrorists may use this knowledge to research these new forms, or to expose weaknesses in the old system before upgrades are completed. Early warning systems and communications are essential to assessing whether a nuclear launch has been made and communicating the orders to launch a retaliatory strike. Falsifying the data provided by either of these systems would be of prime interest to terrorists. Commands emanating from the NAOC for example, include Extremely High Frequency and Very Low Frequency/Low Frequency links, and its activation during a traditional terrorist attack, as happened on 9/11, could provide additional clues as to its vulnerabilities. Blogging communities have also revealed that the 9/11 terrorist attacks revealed insights into the US continuity of operations plan as high level officials were noted heading to specific installations (Critchlow 2006).

One tool designed by the US for initiating a nuclear launch is the 'nuclear football'. It is a specially outfitted briefcase which can be used by the President to authorize a nuclear strike when away from fixed command centres. The President is accompanied by an aide carrying the nuclear football at all times. This aide, who is armed and possibly physically attached to the football, is part of a rotating crew of Presidential aides (one from each of the five service branches). The football contains a secure satellite communication link and any other material the President may need to refer to in the event of its use, sometimes referred to as the 'playbook'. The attack

options provided in the football include single ICBM launches and large scale pre-determined scenarios as part of the Single Integrated Operational Plan. Before initiating a launch the President must be positively identified using a special code on a plastic card, sometimes referred to as 'the gold codes' or 'the biscuit'. The order must also be approved by a second member of the government as per the two-man rule (Pike 2006).

In terms of detecting and analysing a potential attack, that is, distinguishing a missile attack from the launch of a satellite or a computer glitch, the US employs dual phenomenology. This means two different systems must be used to confirm an attack, such as radar and satellite. Terrorists trying to engage a launch by falsifying this data would need to determine which two systems were being used in coordination at the target location and spoof both systems. Attempting to falsify commands from the President would also be difficult. Even if the chain of command is identified, there are multiple checks and balances. For example, doctrine recommends that the President confer with senior commanders. The Chairman of the Joint Chiefs of Staff is the primary military advisor to the President. However, the President may choose to consult other advisors as well. Trying to identify who would be consulted in this system is difficult, and falsification may be exposed at any number of steps. The 2006 Quadrennial Defense Review emphasizes that new systems of command and control must be survivable in the event of cyber warfare attacks. On the one hand, this shows that the US is aware of the potential danger posed by computer network operations and are taking action to prevent it. On the other hand, this shows that they themselves see computer network operations as a weakness in their system. And the US continues to research new ways to integrate computer systems into their nuclear command and control, such as IP-based communications, which they admit, "has not yet been proven to provide the high degree of assurance of rapid message transmission needed for nuclear command and control" (Critchlow 2006).

The US nuclear arsenal remains designed for the Cold War. This means its paramount feature is to survive a decapitating strike. In order to do so it must maintain hair-trigger posture on early warning and decision-making for approximately one-third of its 10,000 nuclear weapons. According to Bruce G. Blair, President of the Center for Defense Information, and a former Minuteman launch officer:

> Warning crews in Cheyenne Mountain, Colo., are allowed only three minutes to judge whether initial attack indications from satellite and ground sensors are valid or false. Judgments of this sort are rendered daily, as a result of events as diverse as missiles being tested, or fired — for example, Russia's firing of Scud missiles into Chechnya — peaceful satellites being lofted into space, or wildfires and solar reflections off oceans and clouds. If an incoming missile strike is anticipated, the president and his top nuclear advisors would quickly convene an emergency telephone conference to hear urgent briefings. For example, the war room commander in Omaha would brief the president on his retaliatory options and their consequences, a briefing that is limited to 30 seconds. All of the large-scale responses comprising that briefing are designed for destroying Russian targets by the thousands, and the president would have only a few minutes to pick one if he wished to ensure its effective implementation. The order would then be sent immediately to the underground and undersea launch crews, whose own mindless firing drill would last only a few minutes (Blair 2003).

These rapid response times don't leave room for error. Cyber terrorists would not need deception that could stand up over time; they would only need to be believable for the first 15 minutes or so. The amount of firepower that could be unleashed in these 15 minutes, combined with the equally swift Russian response, would be equivalent to approximately 100,000 Hiroshima bombs (Blair 2008).

Russia

Russia maintains the world's largest nuclear stockpile with approximately 10,000 nuclear weapons. The authority to launch can be obtained within 10 minutes from the President, the Defense Minister, or the Chief of the General Staff. The unlock and launch authorization codes can be sent directly to individual weapons commanders who would execute the launch procedures, or the General Staff could direct missile launches directly from multiple command centres. Russia maintains a significant satellite network and radar for early warning and identification of an incoming nuclear strike. However, this system is not as robust as it was during the Cold War. Since the collapse of the Soviet Union, some command system and communications networks have become past due for overhaul and modernization (Aftergood 2000). Similarly, many analysts have expressed concern over the safety, security, and control of Russia's nuclear arsenal, especially the integrity of the facilities where nuclear weapons were stored. The US provided assistance and aid under the Nunn–Lugar Cooperative Threat Reduction Program. This included the installation of fencing, monitors, alarms, and comprehensive accounting systems to keep track of materials. These concerns have somewhat eased as Russia's economy has regained strength. However, it shows the risk involved should any nuclear state suffer collapse (Woolf 2002).

Similar to the US football, Russia employs a nuclear briefcase known as Cheget. It accompanies the President at all times and provides secure communication and authorization codes for the order to launch a nuclear strike. It is connected to Kavkaz, a communications network for senior government officials, which is in turn connected to the broader nuclear command and control communication network Kazbek. Some reports state that the Minister of Defence and the Chief of the General Staff are also issued nuclear briefcases. Mikhail Gorbachev was separated from Cheget during an attempted coup in August of 1991. However, reports state that the two remaining nuclear briefcases were deactivated once Gorbachev's had disappeared. Had Gorbachev died or been removed from power, a backup Cheget would have been assigned to the Vice President. However, the General Staff would still wield power in the ultimate decision to launch. Control of Cheget has become a symbol of pride, strength, and authority (Tsypkin 2004).

Despite claims that the order for a nuclear launch can only come from the leader of a state, there are examples which show this decision can rest on personnel who are far from the top of the chain of command. In 1983, Soviet Air Defence Forces lieutenant colonel Stanislav Yevgrafovich Petrov deviated from doctrine when he positively identified an incoming missile attack as a false alarm. According to procedure, he should have sent the alert for an incoming attack, which would have set off the high-pressure race to decide on a response, but instead he took it upon himself to dismiss what he saw, believing a US first-strike nuclear attack would involve hundreds of missiles rather than one. This may have prevented an accidental retaliatory nuclear

attack on the United States. Another example occurred during the Cuban Missile Crisis. A group of US Navy destroyers and an aircraft carrier had trapped a nuclear-armed submarine near Cuba and started dropping practice depth charges. Allegedly, the captain of the submarine, Valentin Grigorievitch Savitsky, believing that a war might already have started, prepared to launch a retaliatory nuclear torpedo. Three officers were authorized to launch the torpedo if they agreed unanimously in favour of doing so. An argument broke out among the three, in which only Vasili Alexandrovich Arkhipov was against the launch, eventually persuading Savitsky to surface the submarine and await orders from Moscow (Philips 1998).

The United Kingdom

The UK retains a weapons stockpile of around 200 operational nuclear warheads. Trident ballistic missiles aboard four Vanguard class nuclear-powered submarines are currently the UK's only nuclear deterrent system. The UK has maintained significant support from the US under the Mutual Defence Agreement. The UK relies on US owned and controlled Ballistic Missile Early Warning System (BMEWS) and Defense Support Program (DSP) satellites for warning of a nuclear attack. The UK permits the US to deploy nuclear weapons from its territory, possibly including tactical nuclear weapons. Information about the suspected location of these bombs can be found online, possibly providing terrorists with insight into vulnerabilities. The UK has not employed the US Permissive Action Link (PAL) system, Trident CCDs, or their equivalent in order to lock out unauthorized activation. This decision was made so that a retaliatory strike could still be launched in the event that the British chain of command was destroyed before a launch order could be sent.

The decision to launch nuclear weapons rests with the Prime Minister. Declassified reports on the Polaris system, the predecessor of the Trident system, indicate a closed circuit TV system was set up between 10 Downing St and the Polaris Control Officer at the Northwood headquarters of the Royal Navy. If the link failed, an authentication code could be sent and verified at the headquarters. The Commander in Chief would then broadcast a firing order to the Polaris submarines via the Very Low Frequency radio station at Rugby. The Prime Minister's decision can be vetoed by the Chief of Defence Staff and the Queen (or Monarch). Once a launch order is sent, only the submarine captain can access the firing trigger, and only after two safes have been opened with keys held by the ship's executive and weapons engineering officers. If a captain believes the UK's chain of command has been destroyed, a determination of which rests on multiple verifications, such as establishing that BBC Radio 4 remains broadcasting, then a captain opens a hand-written order prepared in advance by the Prime Minister. The content of the notes of last resort are at the discretion of the current Prime Minister and seen by their eyes only. These may order a retaliatory strike, leave it up to the captain's discretion, order the captain to place himself under the command of Her Majesty's Government of Australia, or alternatively of the President of the United States, or any number of possibilities (Cheng 2006, Plesch 2006).

France

France maintains a dual delivery system with submarine-launched ballistic missiles and medium-range air-to-surface missiles. The French military is currently thought to

retain a weapons stockpile of around 350 operational nuclear warheads, making it the third-largest in the world. In January 2006, President Jacques Chirac stated a terrorist act or the use of weapons of mass destruction against France would result in a nuclear counterattack (France would use nuclear arms 2006). The French have two rotating crews for each of their missile boats, which they call Rouge (red) and Bleu (blue). French policy has been to maintain three SSBNs ready at all times, with two at sea on patrol. Each SSBN carries several predetermined target dossiers on magnetic disks. The entire complement of 16 M-4 missiles can be fired in three to four minutes. In addition to missile submarines and ground-based strike aircraft, the French retain a nuclear capability based on their two aircraft carriers (Flaherty 2002).

China

China possesses nuclear triad capability and currently maintains a nuclear stockpile of approximately 200 warheads. China's perceived primary threat is from the US, in particular in relation to the status of Taiwan. China maintains retaliatory strike capability with a widely dispersed, redundant, and mobile arsenal, as well as hardening, bunkers, and tunnels capable of maintaining continuance of governance in the event of nuclear war. China uses the same missiles to launch nuclear weapons as they use to launch conventional weapons. Further, they place these alongside each other in firing units of the Second Artillery Corps. This increases the risk of mistaking a traditional launch for being a nuclear launch. China has also invested heavily in cyber warfare, with several military publications postulating that it could be used to disable US early warning sensors. Putting these together, terrorists could route a cyber attack through China against a US carrier group while simultaneously launching a conventional missile attack, in the hope that the US would respond as if it were under nuclear attack.

The Second Artillery Corp is responsible for securing communication with firing units. Direct orders to launch come from the Central Military Commission. Chinese forces use increasing stages of readiness corresponding to nuclear threat assessment. Despite a no-first-use policy, some analysts believe China's ambiguous doctrine could warrant the use of a pre-emptive nuclear strike. The order to launch goes from the commander in chief, to the command organizations of the military departments, to the missile bases, to the firing units. In this regard it is concerning to consider the reputation of Chinese commanders who have frequently subverted national level orders in favour of regional preferences. Unless safeguards are in place to prevent this, the chain of command could be compromised. China has stated that it prefers human confirmation for launch orders rather than relying on technology. However these same reports emphasize the need for speed and encryption which lend themselves to a reliance on technology (Wortzel 2007, Kristensen, Norris, and McKinzie 2006).

India

As of September 2005, India was estimated to have had a stockpile of around 100–140 warheads. It is estimated that India currently possesses enough separated plutonium to produce and maintain an arsenal of 1,000–2,000 warheads. India's primary nuclear delivery system is by aircraft. However they also posses a strong missile capability, and they are rapidly advancing naval surface and submarine launch

capability to complete their nuclear triad. India's space program, which has advanced India's missile capability, is also advancing their threat assessment and early warning systems.

India's nuclear strategy and posture must ensure a massive retaliatory punitive strike which would inflict unacceptable punishment. In the context of giving up the first strike option, this means that the command and control must be able to survive and continue functioning after absorbing a first (attempted decapitation) strike. To do so requires mobility, redundancy, dispersal, dummy warheads, frequent moves and relocation of these assets, and the ability to operate from a myriad of locations. All of these yield greater risk of a weapon being captured or misplaced. For example, falsifying the orders for transport and passing it off as a dummy warhead. The capability to be able to launch a nuclear retaliatory strike within a very short time also increases the risk of decisions being made on poor intelligence. Given that India's primary perceived threat is its nuclear neighbour, Pakistan, and the volatile relationship between the two makes the situation more concerning. The close proximity of these states significantly reduces the transit time of an incoming missile, making the rush to react even greater. Further, India's delivery systems can carry both nuclear and conventional warheads. Under heightened circumstances, a traditional missile launch could be mistaken for a nuclear strike. Terrorists may find it easier to launch a traditional missile in hopes of provoking a nuclear response. Online PSYOPS could enhance this ruse. Additionally, India has stated that it will retain the option of using nuclear weapons in response to biological or chemical attacks, thus providing another way for terrorists to provoke a nuclear response (Norris and Kristensen 2005, Boyd 2003).

The Nuclear Command Authority (NCA) of India is the nodal agency for all command, control and operational decisions regarding India's nuclear weapon stockpile. The Cabinet Committee on Security (CCS) is composed of the Political Council and the Executive Council of the NCA. The Executive Council, chaired by the National Security Advisor (NSA), gives the inputs to the Political Council, which can authorise a nuclear attack when deemed necessary. The Political Council is chaired by the Prime Minister, and advised by the Executive Council, chaired by the NSA. Their directives are to be operationalised by a new Strategic Forces Command under the control of a Commander-in-Chief of the rank of Air Marshal (or its equivalent) in charge of the management and administration of the tactical and strategic nuclear forces. India uses various stages of readiness. During peacetime nuclear cores are kept in secure and concealed storage facilities managed by the Atomic Energy Commission. If the army goes on full alert, then some of the nuclear cores are mated to the warhead and strike plans are reviewed. As the alert levels increase, the warhead is mated to the missile and the army begins to lay out operational plans for moving it into launch positions. In the final stages, missiles may be moved to launch positions, targets are decided upon and a launch clearance is awaited for the encrypted code that would give the order from the Prime Minister to fire. India also maintains arrangements for alternate chains of command in the event a critical decision maker is incapacitated (Squassoni 2005).

Pakistan

Pakistan has approximately 30 to 50 nuclear weapons, with its prime intent at deterring aggression from India. These can be delivered by F-16s and short and long range ballistic missiles. Pakistan has rejected the doctrine of no-first-use. This would suggest Pakistan may at times store nuclear weapons mated with missiles and ready for launch. The US has provided assistance and aid to improve safeguarding of Pakistan's nuclear arsenal. This included helicopters, night vision goggles, and nuclear detection equipment, as well as electronic sensors, closed circuit TV cameras, fencing, and electronic sensors at nuclear facilities. Since 2004, Pakistan has employed the US PAL system for securing its nuclear arsenal. (Berry 2008)

Pakistan's nuclear arsenal is overseen by the National Command Authority (NCA) headed by the President and with the Prime Minister as its vice chairman. Key cabinet ministers and the heads of the army, navy and air force are also members of the NCA, which controls all aspects of the country's nuclear program, including deployment and, if ever necessary, the use of the weapons. However, the military manages and controls the nuclear weapons on behalf of the NCA. While all decision-making on nuclear issues rests with the NCA, an affiliated body, the Strategic Plans Division, manages and controls the nuclear weapons on behalf of the NCA. Transfers of power, multiple acts of terrorism, coups, increased Islamic fundamentalist unrest, assassination attempts on Prime Ministers and the assassination of Benazir Bhutto raise concerns over the security of nuclear weapons in such a volatile environment. Pakistan's nuclear command and control may also be lacking in advanced early warning/threat assessment, secure communications channels, and rigorous screening of nuclear personnel (Jones 2000). Despite the uneasy relationship between Pakistan and India, there are a number of communication channels that have been established, including hotlines between army commanders and prime ministers, and agreements to provide prior notification of troop movements and ballistic missile tests (Haider 2008).

North Korea

Little is known about North Korea's nuclear command and control in open source material. Presumably the order to launch a nuclear weapon would come directly from Chairman of the National Defense Commission, Kim Jong-il. The primary delivery method would be via missile, and major targets would be South Korea, Japan, and the US military presence in the region. Sale of these weapons to terrorist operations is a primary concern. North Korea has demonstrated opportunistic and erratic tendencies in the face of strong international criticism. Allegations of state-sponsored drug smuggling, money laundering, and wide-scale counterfeiting, further this notion. The unpredictable nature of North Korea could provide cover for a spoofed nuclear launch by cyber terrorists. Some politicians in Japan have expressed a desire to change Article 9 of the Japanese Constitution, at least in part, influenced by the threat posed by a nuclear North Korea. In the event of government collapse, concerns over the security of these weapons would be magnified (Samore and Schmemann 2006).

3. Paths of Destruction

Having explored how cyber terrorists can operate and the how the nuclear command and control systems are organised, how might a cyber terrorist penetrate these systems? Four main pathways exist for cyber terrorist to detonate a nuclear weapon:

direct control of a launch, provoking a nuclear state to launch a nuclear strike on its own, obtaining a nuclear weapon from a nuclear state, or acquiring the means to build a nuclear or dirty bomb themselves.

Direct control of launch

The US uses the two-man rule to achieve a higher level of security in nuclear affairs. Under this rule two authorized personnel must be present and in agreement during critical stages of nuclear command and control. The President must jointly issue a launch order with the Secretary of Defense; Minuteman missile operators must agree that the launch order is valid; and on a submarine, both the commanding officer and executive officer must agree that the order to launch is valid. In the US, in order to execute a nuclear launch, an Emergency Action Message (EAM) is needed. This is a preformatted message that directs nuclear forces to execute a specific attack. The contents of an EAM change daily and consist of a complex code read by a human voice. Regular monitoring by shortwave listeners and videos posted to YouTube provide insight into how these work. These are issued from the NMCC, or in the event of destruction, from the designated hierarchy of command and control centres. Once a command centre has confirmed the EAM, using the two-man rule, the Permissive Action Link (PAL) codes are entered to arm the weapons and the message is sent out. These messages are sent in digital format via the secure Automatic Digital Network and then relayed to aircraft via single-sideband radio transmitters of the High Frequency Global Communications System, and, at least in the past, sent to nuclear capable submarines via Very Low Frequency (Greenemeier 2008, Hardisty 1985).

The technical details of VLF submarine communication methods can be found online, including PC-based VLF reception. Some reports have noted a Pentagon review, which showed a potential "electronic back door into the US Navy's system for broadcasting nuclear launch orders to Trident submarines" (Peterson 2004). The investigation showed that cyber terrorists could potentially infiltrate this network and insert false orders for launch. The investigation led to "elaborate new instructions for validating launch orders" (Blair 2003). Adding further to the concern of cyber terrorists seizing control over submarine launched nuclear missiles; The Royal Navy announced in 2008 that it would be installing a Microsoft Windows operating system on its nuclear submarines (Page 2008). The choice of operating system, apparently based on Windows XP, is not as alarming as the advertising of such a system is. This may attract hackers and narrow the necessary reconnaissance to learning its details and potential exploits. It is unlikely that the operating system would play a direct role in the signal to launch, although this is far from certain. Knowledge of the operating system may lead to the insertion of malicious code, which could be used to gain accelerating privileges, tracking, valuable information, and deception that could subsequently be used to initiate a launch. Remember from Chapter 2 that the UK's nuclear submarines have the authority to launch if they believe the central command has been destroyed.

Attempts by cyber terrorists to create the illusion of a decapitating strike could also be used to engage fail-deadly systems. Open source knowledge is scarce as to whether Russia continues to operate such a system. However evidence suggests that they have in the past. Perimetr, also known as Dead Hand, was an automated system set to

launch a mass scale nuclear attack in the event of a decapitation strike against Soviet leadership and military.

> In a crisis, military officials would send a coded message to the bunkers, switching on the dead hand. If nearby ground-level sensors detected a nuclear attack on Moscow, and if a break was detected in communications links with top military commanders, the system would send low-frequency signals over underground antennas to special rockets. Flying high over missile fields and other military sites, these rockets in turn would broadcast attack orders to missiles, bombers and, via radio relays, submarines at sea. Contrary to some Western beliefs, Dr. Blair says, many of Russia's nuclear-armed missiles in underground silos and on mobile launchers can be fired automatically. (Broad 1993)

Assuming such a system is still active, cyber terrorists would need to create a crisis situation in order to activate Perimetr, and then fool it into believing a decapitating strike had taken place. While this is not an easy task, the information age makes it easier. Cyber reconnaissance could help locate the machine and learn its inner workings. This could be done by targeting the computers high of level official's—anyone who has reportedly worked on such a project, or individuals involved in military operations at underground facilities, such as those reported to be located at Yamantau and Kosvinksy mountains in the central southern Urals (Rosenbaum 2007, Blair 2008)

Indirect Control of Launch

Cyber terrorists could cause incorrect information to be transmitted, received, or displayed at nuclear command and control centres, or shut down these centres' computer networks completely. In 1995, a Norwegian scientific sounding rocket was mistaken by Russian early warning systems as a nuclear missile launched from a US submarine. A radar operator used Krokus to notify a general on duty who decided to alert the highest levels. Kavkaz was implemented, all three chegets activated, and the countdown for a nuclear decision began. It took eight minutes before the missile was properly identified—a considerable amount of time considering the speed with which a nuclear response must be decided upon (Aftergood 2000).

Creating a false signal in these early warning systems would be relatively easy using computer network operations. The real difficulty would be gaining access to these systems as they are most likely on a closed network. However, if they are transmitting wirelessly, that may provide an entry point, and information gained through the internet may reveal the details, such as passwords and software, for gaining entrance to the closed network. If access was obtained, a false alarm could be followed by something like a DDoS attack, so the operators believe an attack may be imminent, yet they can no longer verify it. This could add pressure to the decision making process, and if coordinated precisely, could appear as a first round EMP burst. Terrorist groups could also attempt to launch a non-nuclear missile, such as the one used by Norway, in an attempt to fool the system. The number of states who possess such technology is far greater than the number of states who possess nuclear weapons. Obtaining them would be considerably easier, especially when enhancing operations through computer network operations. Combining traditional terrorist methods with cyber techniques opens opportunities neither could accomplish on their own. For

example, radar stations might be more vulnerable to a computer attack, while satellites are more vulnerable to jamming from a laser beam, thus together they deny dual phenomenology. Mapping communications networks through cyber reconnaissance may expose weaknesses, and automated scanning devices created by more experienced hackers can be readily found on the internet.

Intercepting or spoofing communications is a highly complex science. These systems are designed to protect against the world's most powerful and well funded militaries. Yet, there are recurring gaffes, and the very nature of asymmetric warfare is to bypass complexities by finding simple loopholes. For example, commercially available software for voice-morphing could be used to capture voice commands within the command and control structure, cut these sound bytes into phonemes, and splice it back together in order to issue false voice commands (Andersen 2001, Chapter 16). Spoofing could also be used to escalate a volatile situation in the hopes of starting a nuclear war. "In June 1998, a group of international hackers calling themselves Milw0rm hacked the web site of India's Bhabha Atomic Research Center (BARC) and put up a spoofed web page showing a mushroom cloud and the text "If a nuclear war does start, you will be the first to scream" (Denning 1999). Hacker web-page defacements like these are often derided by critics of cyber terrorism as simply being a nuisance which causes no significant harm. However, web-page defacements are becoming more common, and they point towards alarming possibilities in subversion. During the 2007 cyber attacks against Estonia, a counterfeit letter of apology from Prime Minister Andrus Ansip was planted on his political party website (Grant 2007). This took place amid the confusion of mass DDoS attacks, real world protests, and accusations between governments.

The 2008 terrorist attacks in Mumbai illustrate several points. First, terrorists are using computer technology to enhance their capabilities. To navigate to Mumbai by sea and to aid in reconnaissance of targets, they used the Global Positioning System (GPS) satellite system and Google Earth (Bedi 2008, Kahn and Worth 2008). They also used mobile phone SIM cards, purchased in foreign countries, VoIP phone calls, and online money transfers (Part of 26/11 plot hatched on our soil, admits Pakistan 2009). Falsified identification and stolen credit cards may have also been aided by online capabilities. Second, a false claim of responsibility was issued through an e-mail to media outlets. Initial tracking of the IP address showed the e-mail to have been sent from a computer in Russia. It was later revealed that the e-mail was sent from Pakistan and routed through Russia (Shashthi 2008). Voice-recognition software was used to allow "dictated text to be typed in the Devnagari font" (Swami 2008). Lastly, the Mumbai attacks showed an increasing reliance on information technology by the intended victims of terrorism. This included Twitter messages, Flickr photos, a map of attack locations on Google Maps, and live text and video coverage of the attacks (Beaumont 2008). Terrorists could insert disinformation into these systems in order to enhance destruction, evade capture, or increase hostility between groups. Terrorist could even clandestinely enlist the aid of their enemy to enhance destruction. For example, at the height of a terror attack they could claim to have exclusive video footage of the attack, which requires a codec to be downloaded in order to be viewed. This codec could contain a Trojan which uses the now infected computer to silently launch DDoS attacks against their desired targets, such as communications networks. Building an infidel botnet prior to an attack could take on

a wide range of symbolism, from a pdf file about anti-terrorism to an unreleased Hollywood film.

Acquiring a Nuke

The previous chapters of this paper have already illustrated concerns over terrorists directly acquiring a nuclear weapon. These concerns include a possible lack of security measures at nuclear facilities in Russia and Pakistan. All of the nuclear armed states have placed an importance on mobility in order to survive a first strike, which raises the concern of increased opportunity for capture or misplacement of these weapons. Dummy warheads, such as those used by India, could further enhance this risk, by providing a cover for the transport of real nuclear weapons. Computer network reconnaissance could gather information on transport schedules. In 2007, the US Air Force mistakenly transported six nuclear missiles on a B-52 bomber from Minot Air Force Base in North Dakota to Barksdale Air Force Base in Louisiana. The nuclear warheads in the missiles were supposed to have been removed before taking the missiles from their storage bunker. These warheads were not reported missing and remained mounted to the aircraft without special guard for 36 hours. Ironically, an investigation concluded the reason for the error was that the current electronic scheduling system was substituted by an outdated paper schedule system which contained incorrect information. But upgrading these systems to electronic means will open the possibility of tampering by remote computer exploitation (Liolios 2008, Baker 2007).

If terrorists did acquire a nuclear weapon, there is no guarantee they could detonate it. The majority of nuclear states, including the US and Russia, utilize Permissive Action Link (PAL) safety devices. A nuclear weapon utilizing a PAL cannot be armed unless a code is correctly entered. Anti-tamper systems can cause the weapon to self-destruct without explosion. These mechanisms vary between weapon types, but can include "gas bottles to deform the pit and hydride the plutonium in it; shaped charges to destroy components, such as neutron generators and the tritium boost; and asymmetric detonation that results in plutonium dispersal rather than yield ... other mechanisms used to prevent accidental detonation include the deliberate weakening of critical parts of the detonator system, so that they will fail if exposed to certain abnormal environments" (Andersen 2001). Tactical nuclear weapons whose nature precludes the use of PALs may be stored in similar tamper-sensing containers called Prescribed Action Protective Systems (PAPS). It is unclear how pervasive the use of PAPS and similar devices is among nuclear states, with multiple reports suggesting that many are protected by nothing more than simple padlocks (Peterson 2004). Information on PAL codes would be a high value target for cyber terrorists.

Building a Nuke

Acquiring the material for building a nuclear bomb or dirty bomb is another option for cyber terrorists. There are more than 50 tons of highly enriched uranium (HEU) in civilian use alone (Glaser and Von Hippel 2006). Civilian infrastructure is significantly less guarded than military installations and is more prone to computer network operations. They may not operate on closed networks or have the funding to implement cyber defences and training. Difficulties in nuclear forensics may make it difficult for a nuclear explosion to be traced back to a HEU source, thereby reducing a

sense of responsibility for keeping sources secure (Allison 2009). If terrorists acquired HEU they would still need to build a gun-type detonating device. Open source information in the information age provides many clues as to how to build such a device. However it remains far from simple. Numerous states, with resources well beyond that of terrorists, have tried and failed to develop nuclear weapons.

One alternative for terrorists would be to acquire a dirty bomb. Dirty bombs combine radioactive material with a conventional explosive. The radioactive material required for these type bombs are much more accessible. There are millions of sources worldwide for medical purposes and academic research. Dirty bombs are designed to disperse radioactive material over a large area. However the death toll caused by this would be minimal. The explosive device itself may cause more death than that caused by subsequent radiation exposure. The resulting financial loss from decontamination, lost business and tourism, and lost confidence and public fear caused by such a device, are what make them an attractive option for terrorists. As of May 2009, no dirty bomb has ever been used, although a few have been found. In 1995, a group of Chechen separatists buried a caesium-137 source wrapped in explosives at the Izmaylovsky Park in Moscow. A Chechen rebel leader alerted the media, and the bomb was never activated. In 1998, a second attempt was announced by the Chechen Security Service, who discovered a container filled with radioactive materials attached to an explosive mine near a railway line. The unsecure nature of radioactive contaminants can be seen in a number of incidents. From the ease in which they can be obtained, demonstrated by two metal scavengers in Brazil who broke into a radiotherapy clinic, accidentally contaminating 249 people, to the undetected transport of polonium-210 used to kill Alexander Litvinenko (Krock and Deusser 2003).

4. Conclusion

This research has shown that nuclear command and control structures are vulnerable to cyber terrorism. Cyber terrorism provides the asymmetric benefits of low cost, high speed, anonymity, and the removal of geographic distance. Inherent flaws in current nuclear postures provide increasing opportunities for computer exploitation. Despite claims that nuclear launch orders can only come from the highest authorities, numerous examples point towards an ability to sidestep the chain of command and insert orders at lower levels. Cyber terrorists could also provoke a nuclear launch by spoofing early warning and identification systems or by degrading communication networks. These systems are placed at a higher degree of exploitation due to the need for rapid decisions under high pressure with limited intelligence. The desire of nuclear states to have multiple launch platforms, mobility, and redundancy, open the opportunity for misplaced or misdirected warheads. Lastly, if a nuclear device were detonated, its destructive powern can now be magnified by computer network operations, such as misinformation or shutting down key infrastructure.

References

Aftergood, Steven. (2000). Strategic Command And Control. Retrieved on April 9, 2009, from http://www.fas.org/nuke/guide/russia/c3i/index.html.

Allison, Graham. (2009). How to Keep the Bomb From Terrorists. Retrieved on April 28, 2009, from http://www.newsweek.com/id/189260/page/1.

Andersen, Ross. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. Chapter 11: Nuclear Command and Control. Retrieved on April 3, 2009, from http://www.cl.cam.ac.uk/~rja14/Papers/SE-11.pdf.

Andersen, Ross. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. Chapter 16: Electronic and Information Warfare. Retrieved on April 3, 2009, from http://www.cl.cam.ac.uk/~rja14/Papers/SE-16.pdf.

Baker, Fred W. (2007). Air Force Relieves Commanders Involved in Nuclear Weapons Incident. Retrieved on May 1, 2009, from http://www.globalsecurity.org/military/library/news/2007/10/mil-071019-afps07.htm.

Beaumont, Claudine. (2008). Mumbai attacks: Twitter and Flickr used to break news. Retrieved on May 1, 2009, from http://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

Bedi, Rahul. (2008). Mumbai attacks: Indian suit against Google Earth over image use by terrorists. Retrieved on May 1, 2009, from http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html.

Berry, Ken. (2008). The Security of Pakistan's Nuclear Facilities. Retrieved on April 8, 2009, from http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ord516=OrgaGrp&ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=90545.

Berry, Ken. (2007). Preventing Nuclear Terrorism. Retrieved on April 2, 2009, from http://www.ewi.info/pdf/TerrorNukesFeb7.pdf.

Blair, Bruce G. (2008). Achieving the Vision of a World Free of Nuclear Weapons: Increasing Warning and Decision Time ('De-Alerting'). Retrieved on April 2, 2009, from http://disarmament.nrpa.no/wp-content/uploads/2008/02/Paper_Blair.pdf.

Blair, Bruce G. (2003). Rouge States: Nuclear Red-Herrings. Retrieved on April 4, 2009, from http://www.cdi.org/blair/russia-targeting.cfm.

Boyd, Kerry. (2003). India Establishes Formal Nuclear Command Structure. Retrieved on April 27, 2009, from http://www.armscontrol.org/act/2003_01-02/india_janfeb03.

Broad, William J. (1993). Russia has Doomsday Machine, US Expert Says. Retrieved on April 7, 2009,

from http://www.nytimes.com/1993/10/08/world/russia-has-doomsday-machine-us-expert-says.html.
Carfano, James. (2008). Combating Enemies Online: State-Sponsored and Terrorist Use of the internet. Retrieved on April 7, 2009, from http://www.heritage.org/Research/nationalSecurity/upload/bg_2105.pdf.
Cheng, Ta-chen. (2006). Britain's Nuclear Command, Control and Operations. Retrieved on April 22, 2009, from http://210.71.44.174/html/B3/file/fhkaj-8714.pdf.
Critchlow, Robert D. (2006). Nuclear Command and Control: Current Programs and Issues. Retrieved on April 15, 2009, from http://www.fas.org/sgp/crs/nuke/RL33408.pdf.
Critical Infrastructure Threats and Terrorism. (2006). Retrieved on April 14, 2009, from http://www.fas.org/irp/threat/terrorism/sup2.pdf.
Cyber Operations and Cyber Terrorism. (2005). Retrieved on April 7, 2009, from http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439217&Location=U2&doc=GetTRDoc.pdf.
Denning, Dorothy E. (2000). Cyberterrorism. Retrieved on April 2, 2009, from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.
Denning, Dorothy E. (1999). Activism, Hacktivism, and Cyberterrorism: The internet As A Tool For Influencing Foreign Policy. Retrieved on April 3, 2009, from http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.
Diaz, Nils J. (2006). Briefing on Nuclear Security and Incident Repsone (NSIR) Programs, Performance, and Plans. Retrieved on March 1, 2009, from http://www.nrc.gov/reading-rm/doc-collections/commission/tr/2006/20060315.pdf.
Flaherty, Ted. (2002). Nuclear Weapons Database: French Nuclear Delivery Systems. Retrieved on April 23, 2009, from http://www.cdi.org/issues/nukef&f/database/frnukes.html.
France would use nuclear arms. (2006). Retrieved on April 18, 2009, from http://news.bbc.co.uk/2/hi/europe/4627862.stm.
Glaser, Alexander and Von Hippel, Frank N. (2006). Thwarting Nuclear Terrorism. Retrieved on May 2, 2009, from http://www.bnl.gov/nns/News/SciAm0206Fishbone.pdf.
Grant, Rebecca. (2007). Victory in Cyberspace. Retrieved on April 1, 2009, from http://www.afa.org/media/reports/victorycyberspace.pdf.
Greenemeier, Larry. (2008). Navy Mulls New Way to Enhance, Hide Submarine Communications. Retrieved on April 12, 2009, from http://www.scientificamerican.com/article.cfm?id=navy-satellite-deep-siren.
Gregory, Shaun. (2001). A Formidable Challenge: Nuclear Command and Control in South Asia. Retrieved on April 15, 2009, from http://www.acronym.org.uk/dd/dd54/54greg.htm.
Haider, Zeeshan. (2008). Pakistan's nuclear command stays unchanged: official. Retrieved on April 20, 2009, from http://www.reuters.com/article/topNews/idUSISL28991220080408.
Hardisty, H. (1985). Emergency Action Procedures of the Joint Chiefs of Staff: Nuclear Control

Orders. Retrieved on May 2, 2009, from http://www.dod.mil/pubs/foi/reading_room/320.pdf.

Jones, Rodney W. (2000). Nuclear Command and Control Issues in Pakistan. Retrieved on April 3, 2009, from http://www.policyarchitects.org/pdf/Nc4i_pakrev.pdf.

Kahn, Jeremy and Worth, Robert F. (2008). Mumbai Attackers Called Part of Larger Band of Recruits. Retrieved on May 1, 2009, from http://www.nytimes.com/2008/12/10/world/asia/10mumbai.html?_r=1.

Kristensen, Hans M.; Norris, Robert S.; and McKinzie, Matthew G. (2006). Chinese Nuclear Forces and U.S. Nuclear War Planning. Retrieved on April 20, 2009, from http://www.nukestrat.com/china/Book-127-172.pdf.

Krock, Lexi and Deusser, Rebecca.(2003). Dirty Bomb: Chronology of Events. Retrieved on May 2, 2009, from http://www.pbs.org/wgbh/nova/dirtybomb/chrono.html.

Lewis, James A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Retrieved on April 10, 2009, from http://www.csis.org/media/csis/pubs/021101_risks_of_cyberterror.pdf.

Liolios, Teodore E. (2008). Broken Arrows: Radiological hazards from nuclear warhead accidents. Retrieved on May 1, 2009, from http://www.armscontrol.info/reports/authors/liolios/Broken%20arrows%20occasional%20paper.pdf.

Lourdeau, Keith. (2004). Virtual Threat, Real Terror: Cyberterrorism in the 21st Century. Retrieved on April 10, 2009, from http://www.globalsecurity.org/security/library/congress/2004_h/040224-lourdeau.htm.

Norris, Robert S. and Kristensen, Hans M. (2005). India's Nuclear Forces. Retrieved on May 2, 2009, from http://thebulletin.metapress.com/content/147052n7g76v4733/fulltext.pdf.

Page, Lewis. (2008). Royal Navy completes Windows for Submarines rollout. Retrieved on April 20, 2009, from http://www.theregister.co.uk/2008/12/16/windows_for_submarines_rollout/.

Part of 26/11 plot hatched on our soil, admits Pakistan. (2009). Retrieved on May 1, 2009, from http://www.ndtv.com/convergence/ndtv/mumbaiterrorstrike/Story.aspx?ID=NEWEN20090083331&type=News.

Peterson, Scott. (2004). Old weapons, new terror worries. Retrieved on April 20, 2009, from http://www.csmonitor.com/2004/0415/p06s02-woeu.html.

Philips, Alan F. (1998). 20 Mishaps That Might Have Started Accidental Nuclear War. Retrieved on May 1, 2009 from http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/issues/accidents/20-mishaps-maybe-caused-nuclear-war.htm.

Pike, John. (2006). The Football. Retrieved on April 4, 2009, from http://www.globalsecurity.org/wmd/systems/nuclear-football.htm.

Plesch, Dan. (2006). The Future Of Britain's WMD. Retrieved on April 17, 2009, from
http://www.globalsecurity.org/wmd/library/news/uk/uk-0603-uk-wmd-future.htm.
Poulsen, Kevin. (2004). South Pole 'cyberterrorist' hack wasn't the first. Retrieved on April 23, 2009,
from http://www.securityfocus.com/news/9356.
Rahman, Maseeh. (2008). Mubai terror attacks: Who could be behind them? Retrieved on May 1, 2009, from
http://www.guardian.co.uk/world/2008/nov/27/mumbai-terror-attacks-india8.
Rosenbaum, Ron. (2007). The Return of the Doomsday Machine? Retrieved on March 28, 2009, from http://www.slate.com/id/2173108/pagenum/all/.
Samore, Gary and Schmemann, Anya. (2006). North Korea's Nuclear Program. Retrieved on April 27, 2009, from
http://www.cfr.org/publication/12535/north_koreas_nuclear_program_rush_transcript_federal_news_service.html.
Schumer, Charles. (2000). Technological Change and American Security. Retrieved on April 10, 2009,
from http://www.brookings.edu/events/2000/0615defense.aspx.
Shashthi, Margashirsha Krushna. (2008). Mumbai terror attack e-mails sent from Pakistan. Retrieved
on May 1, 2009, from http://www.hindujagruti.org/news/5981.html.
Sherriff, Lucy. (2004). US Navy cuts ELF radio transmissions. Retrieved on April 20, 2009, from
http://www.theregister.co.uk/2004/09/30/elf_us_navy/.
Smith, Tony. (2001). Hacker jailed for revenge sewage attacks. Retrieved on April 22, 2009, from
http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.
Swami, Praveen. (2008). E-mail came from Pakistan. Retrieved on May 1, 2009, from
http://www.hindu.com/2008/11/30/stories/2008113060790100.htm.
Squassoni, Sharon. (2005). Indian and Pakistani Nuclear Weapons. Retrieved on April 10, 2009, from
http://www.ndu.edu/library/docs/crs/crs_rs21237_17feb05.pdf.
Tsypkin, Mikhail. (2004). Adventures of the "Nuclear Briefcase": A Russian Document Analysis.
Retrieved on April 20, 2009, from
http://www.ccc.nps.navy.mil/si/2004/sep/tsypkinSept04.asp.
Weimann, Gabriel. (2004). Cyberterrorism: How Real Is the Threat? Retrieved on April 3, 2009, from
http://www.usip.org/pubs/specialreports/sr119.html.
Wilson, Clay. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for
Congress. Retrieved on April 10, 2009, from
http://fas.org/sgp/crs/terror/RL32114.pdf.
Wilson, Clay. (2003). Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for
Congress. Retrieved on April 10, 2009, from
http://www.fas.org/irp/crs/RL32114.pdf.
Wortzel, Larry M. (2007). China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, And Campaign Planning. Retrieved on April, 15, 2009, from http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=776.

Woolf, Amy F. (2002). Nuclear Weapons in Russia: Saftey, Security, and Control Issues. Retrieved on
April 11, 2009, from http://www.fpc.state.gov/documents/organization/9580.pdf.
Zetter, Kim. (2009). Botnets Took Control of 12 Million New IPs this Year. Retrieved on May 6, 2009,
from http://www.wired.com/threatlevel/2009/05/botnets-took-control-of-12-million-new-ips-this-year/.