CHAPTER 12

TO WHAT EXTENT CAN PRECISION CONVENTIONAL TECHNOLOGIES SUBSTITUTE FOR NUCLEAR WEAPONS?

Stephen J. Lukasik

Nuclear weapons technology and its related systems, doctrines, and strategies are based on what was the newest discovery of science in the 1930s. Although nuclear weapons were developed too late to have much of an impact in World War II, they did play an important role in national security during the following decades. In the intervening 70 years, new technologies have been applied to the protection of states and their populations. The proposition examined here is that these new technologies, and the demonstrated capabilities of systems and doctrines based on them, can in some cases substitute for those currently provided by nuclear weapons. The technologies seen as potentially offering these capabilities are those involving the precise and discriminate application of far smaller amounts of force to achieve militarily desirable effects than those delivered by even the lowest-yield nuclear weapons.

The replacement of nuclear weapons with more effective ways of achieving military objectives has been underway for a number of years. During the period of nuclear arms limitation negotiations between the United States and Russia, conventional military capabilities have benefited from developments in radar, stealth, precision navigation, unmanned vehicles, guidance, propulsion, computation, and networked communications linking target-acquisition sensors to

national-level commanders as well as to theater forces and down to quite low organizational levels. The commonly held view is that if one can find a target and identify it, it can be dealt with quickly and effectively. With such capabilities, consideration of the potential for the substitutability of conventional for nuclear weapons is natural.

Substitutability implies trade-offs, since nuclear and discriminate conventional technologies have quite different characteristics, each having both desirable and undesirable characteristics. There are at least four relevant issues:

1. As the United States and Russia reduce their stockpiles equally and in concert to a level of roughly 1,000 warheads, they enter the range in which their stockpiles are numerically comparable to those of other nuclear states. But the downward movement in numbers of the United States and Russia is opposite to the upward trends in at least four nuclear nations. Warhead numbers do not tell the whole story, however. Strategic balance calculations on which U.S. and Soviet net assessments were made included a number of other metrics: yield, range, accuracy, vulnerability, reliability, readiness, etc. None of these are addressed adequately by the simple matter of warhead numbers.

2. As national goals evolve over time, and as national security needs to change correspondingly, new technologies such as those noted above become important in assessing the ability of a nation to enforce its will on another. However, these substitution options are not equally accessible to all nations, because they depend on sustained long-term investments in research and development (R&D), target acquisition, delivery systems, training, employment doctrines, and conventional warhead type and design. Not all states

are equally endowed with the necessary economic, technological, and production capabilities to deploy and maintain weapons based on these advances.

3. The new discriminate technologies have practical limits not shared by the nuclear weapons they could be seen as replacing. Nuclear weapons have such large areas of destruction that small errors in delivery accuracy, target identification, target vulnerability, and uncertainties in weather and visibility are unimportant, but these are central for the effectiveness of conventional discriminate technologies. Thus, nuclear weapons, however costly, could provide more effective and reliable options for the delivery of military force for some countries.

4. Understanding the equivalence between nuclear and discriminate conventional weapons depends on complex calculations related to a nation's perceived adversaries, the nuclear and conventional capabilities of each, how the lower collateral damage of conventional weapons is valued by each, the number of aim points needed to achieve a desired effect, and the fact that the discriminate technologies must be costed on the basis of actual continued use—while nuclear deterrent forces are never to be "used" beyond being in existence and having imputed capabilities that are generally not precisely known by opposing sides. Nuclear weapons are judged on the basis of their presumed first-strike destructiveness. Conventional weapons are judged by their post-conflict outcomes. Thus, the two classes of weapons are not directly commensurate.

NUCLEAR WEAPONS IN PRACTICE

Beyond their potential military uses, nuclear weapons have some perverse characteristics not shared by discriminate conventional technologies—the most serious being accidental or unintended nuclear war. The textbook case is Cuba (1962). While a good deal of the "fog of war" is unavoidable, nuclear capabilities used will result in a large force expended in a relatively short time that does not allow any margin for error. The beginning is the end. In 1969, the Soviets went down the same path with the People's Republic of China (PRC) over several long-running border disputes, with further implications of threats to their nuclear facilities. Soviet nuclear adventurism was repeated a third time, in Afghanistan in 1982, when SCUD missiles were secretly deployed to the Wakhan Corridor to threaten PRC and Pakistani nuclear facilities.

These situations highlight the danger of the unwise deployment of nuclear weapons. Whatever weapons are available will be deployed, however low the stakes. The scale of destruction between 200 pounds (lb.) of chemical explosives and 20,000,000 lb. (20 kilotons [KT]) or 20,000,000,000 lbs. (20 megatons [MT] of trinitrotoluene [TNT] is not easily grasped.) Measuring nuclear capabilities in kilotons and megatons reduces the apparent differences to misleadingly small numbers. Putting weapons or people into situations in which such large differences in scale must be accurately understood is to invite errors in judgment.

Another difficulty is that nuclear weapons interfere with the conduct of more frequent non-nuclear military operations. In 1967 and 1968, only nuclear-armed aircraft were available to go to the aid of the

USS *Liberty* and USS *Pueblo*, and they could not be used under the circumstances. The Union of Soviet Socialist Republics (USSR) found itself in a similar circumstance during the 1979 Soviet invasion of Afghanistan. Secret concentrations of forces in preparation for the invasion were made to appear as normal troop movements, so they had to take their Free Rocket Over Ground (FROG, a North Atlantic Treaty Organization [NATO] designation) mobile nuclear-capable missiles with them. The United Kingdom (UK) was forced into a similar situation in 1982, when it dispatched nuclear-armed naval forces to the Falkland Islands. The need for speed precluded offloading the UK's naval nuclear weapons before departure or en route. While no nuclear consequences resulted in these last two cases, owning nuclear weapons imbues all military operations with nuclear-use implications.

Other potential disasters follow from the accidents attending nuclear weapon deployment. It is difficult to handle nuclear weapons without something going awry, a state of affairs well known to those dealing with reliability theory.[1] The issue in reliability is not the fact of unreliability *per se* but the consequences of reliability failures. These depend on details of weapon design that will not be generally known to all involved: the quality and stability of the chemical explosive components, the number of detonation points required for fission yield, the design of handling equipment, the training of operational and maintenance personnel, the details of the arming and firing circuitry, etc.

Incidents at sea are another source of accidents, given that such international space is often where short-range confrontations between nuclear-armed adversaries occur.

Another emergent characteristic of nuclear arsenals is that of hoaxes, rumors, exaggeration, and fear. These are driven by perceptions—some created by a state wishing to inflate its capability to deter; others, from self-deception. Brian Jenkins makes the case, in his provocativelytitled book, *Will Terrorists Go Nuclear?* that al Qaeda *is* a nuclear power, not because it possesses nuclear weapons, but because we are as frightened of them now as we would be if they did possess them.[2] An earlier observation by Secretary of State Dean Acheson in 1951 with regard to nuclear weapon use in Korea was similar:

> The threat represented by our stockpile of atomic bombs was not a political advantage or asset, but, rather a political liability. The threat of its use by us would frighten our allies to death but not worry our enemies.[3]

Recognizing that beliefs and fear are the essence of the matter, note must be taken of the opportunities and instabilities of contemporary personal communication channels to propagate hoaxes and rumors, and thus, the fear they engender. These rumors and hoaxes supplement the mass media, especially with their 24 hours a day/7 days a week need to fill airtime with talk, images, and speculation, regardless of substance.

In view of the disadvantages of too much force for rational needs, difficult-to-arrest slides down slippery slopes to unintended conflict, accidents in handling and deployment, and the unbounded fear or anger that they generate make assessment of the value of their substitutability difficult.

EFFICIENT APPLICATION OF MINIMUM FORCE

Sun Tzu said, "Generally in war the best policy is to take a state intact; to ruin it is inferior to this." He further notes, "For to win 100 victories in 100 battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."[4] The excessive magnitude of nuclear force in even the smallest such weapon and the attendant uncertainties in the outcomes of its use makes industrial war—the application of a state's total power toward the use of force against an adversary—no longer feasible as an instrument of national policy.[5] Industrial war spawned the creation of nuclear force, which by its nature renders such conflicts too dangerous to undertake. Multiple nuclear states with multiple competing interests, global relationships across a range of economic and political domains, and the rise of both sub-state organizations and transnational institutions now channel confrontation into more local, limited, and specific directions.

Since resources are limited in practice, prudence suggests using minimal resources in the light of future needs and uncertain outcomes. Nor is there any point expending resources to destroy something of no military or economic value. Destruction must eventually be repaired, and costs and consequences are shared. An attack is a beginning, not an end. Hence, in unleashing force, one is setting sequences of unpredictable events in motion.

In this discussion, we ask if the goals of the use of nuclear force can be as satisfactorily achieved with post-nuclear technology that centers on maximum efficiency and discrimination in the delivery of minimum amounts of force. Sometimes referred to as "surgical," in practice such strikes carry the same costs as those in the medical analogy.

There are a number of technologies that can be combined to protect a nation's security that were not on the horizon when the decision to develop nuclear weapons was made. These are not matters of theory. They represent capabilities that are available today and have been integrated into force structures since the mid-1980s to achieve some efficiency and discrimination in the delivery of force. While not yet perfected, they promise alternatives to the unconstrained use of nuclear force.

Target Attacks with "Dumb" Weapons: The Issue of Collateral Damage.

The first "precision" air attack took place 8 years after the first Wright brothers' flight. On November 1, 1911, Lieutenant Guilio Gavotti, commander of the Italian air fleet, directed his *Bleriot X.1* fighter over a Turkish camp near Ain Zara as part of a campaign for control of Libya and Crete. He leaned over the cockpit and dropped four modified 4 lb. Swedish hand grenades. The attack set a second record when the Turks complained that the bombs hit a field hospital, thus establishing the first mention of collateral damage.[6]

Air attacks were developed by Germany in World War I and in the Spanish Civil War by the German Condor legion. The force commander made the German policy clear when he posted a "Golden Rule" for his pilots: "If for any reason, the original target cannot be attacked . . . the bombs are to be dropped blind anywhere over enemy territory, again without regard for the civilian population."[7]

Air attack was a major tactic in World War II and continued to reflect the debate over precision attacks on military targets vs. indiscriminate attacks on cit-

ies and civilian populations. Air attacks were of three types: air-to-ground tactical support for the Allied forces, for which collateral damage was not a factor; precision attacks on military and industrial targets intended to minimize collateral damage; and outright terror attacks on civilians. Precision bombardment was aided by the famous Norden bombsight, which increased accuracy by being able to compensate for the speed of the aircraft. What it could not do, and which led to circular error probable (CEPs) of several miles, was to compensate for the winds throughout the bomb's trajectory. These were exacerbated by the need to fly at high altitude to avoid anti-aircraft artillery (AAA) fire. By 1942, all reservations about collateral damage were ignored.

In Operation ROLLING THUNDER in Vietnam in 1965, the primary objective was the North Vietnamese logistics system. U.S. policy was mindful of minimizing civilian casualties, so targets and mission details were decided in Washington. Unexpended ordnance could only be jettisoned at sea, and enemy aircraft had to be visually identified before being engaged. Two bridges, the Tanh Hoa heavy-masonry bridge over the Song Ma River and the Paul Doumer Railroad Bridge near Hanoi, were repeatedly attacked with "dumb" bombs between June 1965 and January 1968 without success, pointing to the need for greater bombing effectiveness.

Discriminate Technologies.

Radar hardly seems new, since it had far more effect on the outcome of World War II than did nuclear weapons. It can locate and track moving targets at long range, work through obscuration, filter signals

to match target characteristics, and use Identification, Friend or Foe (IFF) to reduce targeting errors. Newer technology enables radar to work underground, through walls, and operate with a low probability of detection. Its competing technology is low radar cross-section platforms that can penetrate areas with less risk and thus provide better accuracy for weapons delivery and, when manned, add human judgment to the process.

Satellite-based navigation (GPS) enables platforms to know where they are and, with GPS coordinates of targets, enables weapons to be delivered with significant accuracy. Local GPS enhancements can fill in possible reception gaps and increase accuracy further. Satellite-based reconnaissance enables the location of fixed targets. Unmanned air platforms can do the same thing, with more immediacy and specificity. They can, for example, provide virtually continuous surveillance of areas at less risk than can manned aircraft or ground observers. Such platforms can have reduced observables and be configured to deliver warheads to targets. *Cruise missiles*, aided by GPS, *inertial,* or *terrain matching guidance* technology, constitute another type of unmanned platform with a longer range and larger payloads.

A variety of *autonomous homing or manually guided warheads* enable relatively small warheads to engage selected targets with effectiveness when directed to their points of greatest vulnerability. These include home-on-emitter and home-on-jammer warheads as well as those employing visual or infrared (IR) image correlation.

Ballistic missile defense is probably the most highly precise and discriminate technology available and has no downside in collateral damage.

Other precision technologies include *cyber weapons,* which enable networked platforms and facilities to be selectively attacked.

Special forces provide the ultimate in accurately delivering warheads or other devices, to targets with the flexibility provided by human minds, eyes, and hands.

Networks supporting software-enabled functionality provide new capabilities for information collection, collaborative analysis, distribution of information to forces for immediate use, as well as rapid and flexible command and control. Their competing technology is portable, relatively short-range emitters of high-powered focused microwave energy that can couple to electronic circuits to disable or destroy them—with little collateral damage.

While there are a number of technologies that support the precise application of force, one must ask two questions. First, how well have they met their potential capabilities? The second is whether these technologies, employed by trained forces operating under developed and tested operational doctrine, can achieve the same national objectives for security attributed to nuclear weapons.

Precise Delivery of Force to a Selected Point.

The obvious characteristic, and the one technologists and military people enthuse about, is the precision delivery part. This is a matter of design, fabrication, testing, training, mission planning, and mission execution. All these facets of the problem are understood in principle, but they change in significant detail when technologies change and have to be thought out anew in each case.

The second, frequently overlooked, part of the task is to know *what point to select*. This is in part technical: the matter of identifying the most vulnerable points in a selected target that, when struck appropriately, will disable or destroy it. But finding the target, knowing it is the most important target at the time of attack, and doing this in the face of camouflage; deception; target mobility; and under conditions that often result in lack of information, direction, visibility, and other circumstances, is challenging. The latter are matters for the collection, analysis, and distribution of intelligence, both strategic and tactical. Without correct and timely intelligence, precision delivery is worthless. Knowledge acquisition and distribution comes before precise delivery. Precisely killing what you do not want to kill is collateral damage—a large negative on the scoreboard, especially under the conditions of 21st-century conflict among the people and public scorekeeping.

Furthermore, when directing force at a target, the target is typically not passive. It reacts to an attack by defending itself. In so doing, it degrades the performance of the attacker, sometimes successfully evading damage and sometimes causing collateral damage itself.

By 1972, electro-optical guided bombs (EOGB) and laser-guided bombs (LGB) were in the inventory, and available for another go at the two bridges that had defied serious damage 4 years earlier. On the first raid against the Tanh Hoa Bridge, weather precluded the use of the LCBs, but 12 F–4s, each carrying two 2,000-lb. weapons, severely damaged the bridge. A second strike by 8 F–4s resulted in 12 direct hits and 4 probable hits with EOGBs. A third strike by three aircraft carrying 3,000-lb. LGBs dropped the rest of the spans.

The 1981 Israeli air strike against the Iraqi Osirik reactor provides an interesting contrast to the U.S. technology. Israel opted out of using EOGBs in its inventory. Instead, Israel used carefully selected, weighed, and balanced 2,000-lb. Mk 84 gravity bombs delivered in a dive maneuver by eight F–16s at a 3,000-ft altitude. Of the 16 bombs delivered, 15 hit the reactor dome. The attack was timed for a Sunday so that no workers would be on-site; it was at the last possible time before the reactor was in operation and would have released radioactivity when destroyed.

Operation DESERT STORM in 1991 found the U.S. Department of Defense (DoD) better prepared to use its new technology. Again, the F–117A was chosen for its weapon delivery capability. Twenty arrived over Baghdad, Iraq, but collateral damage constraints had the effect that 20 percent of the first strike aircraft had to return with their weapons because they could not positively identify their targets. Because there were so many targets and some covered such large areas, there were many separate aim points. Because there was such a dense air defense environment, cruise missiles were employed also, but their low altitude at relatively low speeds resulted in several being shot down by ground fire.

The results were quite impressive. The 25–30 ft CEPs achieved on test and training ranges were largely achieved by the F–117As, the 104 Tomahawk land-attack missile (TLAM), and 35 air-launched cruise missiles (ALCM). The most famous was the picture of a smokestack in the crosshairs of an F–117A. The LGB went down the stack and destroyed several floors of the building. But a command and control facility in the basement was undamaged. After the war, the DoD estimated that 800 targets were attacked, and only about 50 (6 percent) were misidentified by pilots.

Precision weapons continued to be important in Iraq, with several cases of particular interest. The Amiriya bunker, a large, hardened underground structure 40 ft underground with a 10-ft reinforced concrete roof, was believed to be a part of the Iraqi command and control system. An F–117A released two LGBs simultaneously. Both homed on the same illuminated spot (which was 20 ft off from the intended ventilation shaft target.) The first weapon cratered the building roof but did not penetrate it. The second weapon easily penetrated the crater that the first weapons created and then penetrated the roof. Unfortunately, the bunker was being used as an air raid shelter. Between 300 and 400 civilians were killed, and 28 survived.

Bridges critical to supplying Iraqi forces in Kuwait continued to be important targets. Between January 16 and February 1991, of the 50 bridges in Iraq and Kuwait, 42 were attacked and 27 destroyed. Typically, there was one sortie carrying two LGBs per bridge. Collateral damage was generally light, but on one mission an LGB veered away from the target and hit a market area, killing 130 people.

Air attacks continued for the next several years to try to bring Iraq into compliance with prior agreements. As air attacks in Iraq were phasing down, the national focus shifted to events in the former Yugoslavia. Operation ALLIED FORCE was directed to stabilize the chaos following the dissolution of the communist government in 1990 and the unleashing of long-standing hatreds, underlined by the religious differences in this high-water mark of the Muslim advance into Europe in the 13th century. Ethnic cleansing in Bosnia and Kosovo of all non-Serbs ensued.

The rules of engagement to minimize collateral damage and the nature of coalition warfare proved

difficult to implement to achieve the desired political objectives effectively. The air resources employed were substantial, and, at the same time, described NATO as wanting "half a war." Cruise missiles from B–52s, surface ships, and U.S. and UK submarines attacked air defenses as a preliminary to deeper strikes. Serbian air defenses, a holdover from the USSR, were substantial: *Mig*–21 and -29 fighters, SAM SA–2,–3,and–6s, and AAA.

An F–1117A was lost through an effective use of radars in a bi-static mode. Substantial military damage was inflicted with minimal NATO losses, but post-conflict searches on the ground confirmed only 6 percent of the "confirmed" kills. Apparently many of the kills were against decoys or the result of pilots and photoanalysts who gave these reports the benefit of the doubt. While the precision of weapons delivery was good, some damage, such as to runways, was quickly repaired. Collateral damage was not insignificant, especially when amplified by the news media and on-the-spot reporting.

The most politically embarrassing failure was mistaking the Chinese Embassy for the Yugoslav Federal Directorate of Supply and Procurement. The error was the result of outdated maps that failed to report the new location of the embassy correctly. A lengthy investigation identified seven Central Intelligence Agency (CIA) employees responsible for the intelligence failure. The CIA Director claimed the problem was "systemic," with blame shared by the CIA and the National Imagery and Mapping Agency, but then shifted it to private contractors to whom the government's work had been outsourced.

In all, these air campaigns, however impressive in terms of previous dumb-weapon capabilities, did not

clearly establish confidence in precision low-collateral damage technology. This was due to a combination of genuine technical problems in planning and executing raids in dense urban areas, failures of intelligence, and initial overoptimistic reporting of results that gave decisionmakers reason to continue. On the other hand, the Joint Direct Attack Munition (JDAM), the 5,000-lb. hard-target penetrating munition, was quite effective.

What does not come out of such sound bites as "one-shot-per-kill" is the large amount of effort involved in delivering a small number of precision weapons to targets. Omitted are the additional aircraft for refueling, defense suppression, fighter escorts, carrier protection, air defense, and the like. Also ignored in tallies of accuracy is that defensive actions damage some precision munitions and countermeasures degrade accuracy. When collateral damage is a single metric, it is not entirely under the control of the attacker.

In terms of the utility of conventional weapons delivered with precision and with regard to the minimization of collateral damage, we can conclude:

1. The technology can deliver sufficiently high accuracy such that relatively small amounts of destructive power can effectively destroy many targets if some degree of maturity in technology and doctrine has been achieved.

2. The promise of control of collateral damage is less clear, though significantly less than with nuclear weapons. Intelligence agencies and military planners devote far more time to the study of targets than they do to the comparable understanding and characterization of non-targets.

3. The delivery of conventional force for strategic purposes involves large numbers of supporting capa-

bilities, including intelligence collection and analysis, delivery systems, mission planning technology, command and control, damage assessment, media communication, and "systems" for post-attack exploitation of the results of such operations.

4. However much one might wish the problem away, applying force under circumstances in which targets and non-targets are in intimate contact is not simple. There are realistic limits to what can be done to control collateral damage. These circumstances diminish the utility of discriminate weapons in some situations, especially when the use of civilian populations as a shield is adopted as a deterrent strategy.

Cyber Weapons in a Strategic Role.

Strategic response cyber attacks may not have the immediacy of nuclear attacks, since they can consist of instructions for events to happen at any time in the future, or under specified circumstances. Their effectiveness will depend on the degree to which a target nation is wired with digital networks that penetrate as many aspects of its military and civilian economy as possible.[8] They are precise, because networks can only function when every person, place, or device has a network address. Thus, for a wired nation, all aspects of its activity are in the hands of whoever has the "phone book," and the possibilities open to them depend on the extent of the information technology (IT) penetration and the cleverness of the attacker. Classes of targets that can be selectively attacked or attacked as groups include:

1. *Government*. Governments are laying the foundations for e-governments, whose information networks provide the major interface between clients and

service providers. By disrupting these, the essential functions of government can be interfered with on a continuing basis, reducing the trust in government that is necessary for the maintenance of order and economic functioning. Thus, strategic cyber attacks can start with massive identity manipulation to steal the identities of real people but also to create synthetic people. Trust attacks will be used to confuse records to the extent that health records, credit card records, land transfer records, stock transfer records, and the like are sufficiently distorted to the point that instead of current tolerable error rates of, perhaps 10^{-5}, they might be increased to 10^{-3}–10^{-2} or more.

2. *Infrastructure*. Cyber attacks on cities and energy infrastructures would focus on penetrating operational control centers, such as those of electric power generation, transmission and distribution; gas and oil pipelines; and rail and air systems. Trains provide an attractive kinetic energy weapon if they can be caused to derail, especially in a tunnel or in a way that destroys a bridge, or to release toxic or inflammable cargo. The essence of all infrastructure attacks is not to disrupt operations temporarily but to do so in a way that causes physical devices to operate beyond their intended parameter ranges and destroy themselves—as by destroying bearings in generators, high-voltage transformers in transmission systems, or circuit boards in computers and switches.

3. *Military systems*. Surveillance, intelligence, communication, weapons systems, and command and control facilities all depend, in an age of net-centric warfare, on computation and software for their functionality.

4. *Physical objects*. For reasons such as inventory control, transportation tracking, and prevention of theft, physical objects can be tagged with a transmit-

ter/receiver having its own Internet Protocol (IP) address such as with an Radio Frequency Identification (RFID) device. These can communicate with each other to self-organize into micro-nets to issue an alert in the event of behavior outside specified limits.

5. *Buildings*. Increasingly, buildings are internally networked to integrate occupant communications, heating, ventilation, and air conditioning (HVAC), physical access to areas, energy efficiency, fire protection, etc. As such nets become increasingly intelligent, both through pre-programmed limits and learning occupant activity patterns, they can be made more effective and contribute to environmental protection as well. The target implication is that buildings can be rendered unusable through the denial of communication, heat, water, power, and physical access.

6. *People*. Badges, biometrics, cell phones, and location tracking will enable people to be tracked for normal or emergency communications. They provide electronic identities that can be taken over at any time.

7. *Residences*. The same functions that are useful for military, commercial, and industrial buildings will be useful in residences. In addition, tasks such as ordering and cooking food; providing entertainment; and controlling the thermal, acoustic, and visual environment will add to the quality of life of its occupants. Here the implications are the same as for military, commercial, and institutional buildings. If someone takes over the command and control functions of residences, they can be rendered unusable.

8. *Vehicles*. Tracking vehicles increases the safety of the vehicle and its occupants, increases the efficiency of commercial uses, and provides for downloading vehicle software updates or uploading mechanical status information for maintenance and diagnostics.

GPS already plays this role for some vehicles, and cellular tracking via Bluetooth technology can also be utilized. Control of even a small part of a vehicle fleet will enable attacks on cities by disrupting urban and intercity traffic.

9. *Robots*. Industrial production now makes heavy use of robotic devices, networked within a facility. Higher levels of manufacturing integration will see these networked more broadly. Facilities are currently networked to suppliers and shippers to support just-in-time manufacturing and custom-specified products. Similarly, manufacturing integration will be extended to the retail level for the same reasons. There is, in addition, increasing use of robots at the retail consumer level for such tasks as the delivery of meals in institutions and home cleaning. When robots can be issued arbitrary instructions, they can come under external control and be turned from helpers to saboteurs.

When nations come to depend heavily on cyber technologies, their essential functioning can be disrupted or destroyed by operating their internal controls "in reverse," instructing mechanical devices to work in ways that are beyond the operating or logic limits designed into them. Even if manual backup systems are available, having to resort to them reduces the efficiency level at which an economy operates. Moreover, such attacks are inexpensive, can be repeated until they succeed, and do not expose the attacker to harm or even identification.

The degree to which the above cyber speculations can be substantiated is not nearly as great as when we speak about the performance of nuclear or precision weapons. The Internet as a public access digital communication network did not come into effective exis-

tence until web browsers were developed in the early 1990s. In effect, cyber attack tools today are in about the same relative state of development in achieving their future effectiveness as precision weapons were in the early 1970s, with the first EOGBs and LGBs.

Nevertheless, one does see numerous well-documented cases of cyber attacks. Identity theft, spam, phishing, burglary, fraud, stalking, viruses and worms, distributed denial of service attacks, botnets, and state-sanctioned cyber attack groups worldwide are sufficiently documented in the literature that the general outlines of the capability of such weapons are becoming clear. There have been organized cyber attacks on states that occurred as isolated incidents—as against Estonia in 2007, or, in coordination with military actions, as with the Russian invasion of Georgia in 2008. State actions that are visible to date include intelligence collection that has some degree of legitimacy. Cyber attacks defeat both law enforcement and counterintelligence agencies because cyber attacks use communication facilities in numerous jurisdictions, are performed in complete anonymity, and can be repeated as often as the attacker desires, since there is no penalty imposed on an attacker for attempting an unsuccessful penetration.

Cyber attacks fall into a gray area of international law. They are not seen as "armed attacks" for which one set of remedies is available under the United Nations (UN) Charter, but jurisdiction and anonymity severely hamper domestic law enforcement.

We lack fundamental defensive capabilities such as early warning networks, situation awareness, and order of battle information, while our options for response are limited. Intrusion detectors, anti-virus software, spam filters, and encryption technology pro-

vide some defensive capabilities, but what the human mind can create, another human mind can circumvent. Informed insiders also provide attackers with a significant edge over defenders. One can expect that matters will not always be this way, but at this point rights and responsibilities for those in the global cyber commons are undefined. What is more troubling is the lack of user or market interest in network security and user protection. As a result, consumers and business organizations worldwide are busy attaching more devices to a fundamentally insecure network, all of which create new vulnerabilities and access paths for attackers.

PATHS TO THE FUTURE

The United States and Russia, having been reducing their nuclear stockpiles since the 1990s while at the same time developing a wide range of conventional capabilities, are driven to precision for the obvious reasons of greater efficiency and effectiveness. The two countries may be precursors to substitution by a larger number of countries. Other national stockpiles are still less than 1,000, but some nations are newer to the business and are still in the phase of developing capabilities that have been part of their national agenda since the 1960s. It is unlikely that having striven to achieve their nuclear capability, these nations would change directions so soon.

The newer nuclear nations are drawn to nuclear weapons for the power they unleash, and they have not embraced the idea of limiting damage to their enemies. An announced intention to destroy their enemies, and to benefit from the fear that intent produces is what they are about. So substitution is still a bit too

avant garde. If new nuclear nations, with a more modest set of enemies, do not become mired down constructing huge stockpiles, they may be quite satisfied with a simple deterrent capability without regard to the fine points of strategic theory.

The original five nuclear states will continue to see themselves in a modified but still polarized Cold War relationship, requiring nuclear deterrence *vis-à-vis* each other. In this light, these five states would see missile defense as destabilizing that mutual balance. But deploying ballistic missile defenses (BMD) to protect themselves against threats from the new nuclear states makes much more sense. Anti-Ballistic Missile (ABM) deployments, designed to protect a finite number of self-identified target states from the latter states, are being designed and implemented. They could be separate systems separately administered, based on defense agreements among a limited set of states concerned with particular threats.

Such systems could be boost-phase systems—either sea-based or based in territory of the parties to the separate treaties—or they could be air attacks on soft "R&D" launch facilities during launch preparations. Such ballistic missile defense systems could be viewed as enforcing a quarantine on space launches from threatening states. Pre-launch payload inspections could ensure that peaceful access to space would not suffer interference.

A global missile defense architecture consisting of separate systems to protect group A from threat nation X, another to protect group B from Y, etc., clearly does not scale. But when the number of threat states is small and is growing slowly, one can forgo the efficiency principle in favor of limited solutions tailored to a few particular circumstances. Procurement effi-

ciency will not be totally forgone, since there will, in such a future situation, be a growing market for missile defense systems, and it is not unreasonable to believe that, even with a small number of such systems and some commonalities among the threatened states, they can be networked to some extent.

Some of these ideas in precision conventional weapons, cyber attack and defense capabilities, and missile defense are ongoing and not revolutionary. They all depend on networked arrangements for early warning, strategic reconnaissance, and navigation—front-end systems whose output can be shared among states that feel they need defense capabilities—but do not wish to enter into binding international agreements. The Internet, Google Earth, and GPS are starts in that direction.

The technologies involved in the precise delivery of force, first introduced in this discussion in terms of offensive needs, blur the separation of offense and defense. They reflect the observation of Albert Wohlstetter in discussing deterrence and missile defense, that offense had become defense and defense had become offense.

The new nuclear weapons states are much less homogeneous than were the first five, divided as they were over Communism. The new nuclear nations are a commoditization of nuclear weapons to support the needs of regional interests. To speak of "proliferation" is to lump separate problems into one-size-fits-all prescriptions. Israel–"Palestine," Pakistan–India, Iran–Iraq, North Korea–South Korea, and possibly others to arise from new sources of tension and varied sets of constraints. It is possible that precision in physical targeting may also provide fruitful approaches to precision in political targeting as well.

ENDNOTES - CHAPTER 12

1. Charles Perrow, *Normal Accidents: Living With High-Risk Technologies*, New York: Basic Books, 1984. An alternate body of thought in the same community holds that any desired level of reliability can be achieved—the issue being the amount of care and attention given to achieving reliability. Since investment in reliability is, of necessity, limited, given other needs, the difference between the two viewpoints is quantitative, not qualitative. Thus, the approach taken here is to examine data rather than rely on theory.

2. Brian Michael Jenkins, *Will Terrorists Go Nuclear?* Amherst, New York: Prometheus Books, 2008.

3. William C. Yengst, Stephen J. Lukasik, and Mark A. Jensen, "Nuclear Weapons that Went to War (NWTWTW)," DNA-TR-96-25, draft final report sponsored by U.S. Defense Special Weapons Agency and Science Applications International Corp., October 1996, unclassified, available from *www.npolicy.org/article.php?aid=80&rt=&key=nwtwtw&sec=article&author=*.

4. Sun Tzu, *The Art of War*, Chap. 3, "Offensive Strategy," Samuel B. Griffith, trans., Oxford, UK: Oxford University Press, 1963.

5. Rupert Smith, *The Utility of Force: The Art of War in the Modern World*, New York: Random House/Vintage Books, 2007.

6. This and the following cases are taken from unpublished manuscripts prepared in the 1996–1998 period by William C. Yengst, as part of a preliminary study of precision weapons and their effectiveness.

7. *Ibid*.

8. The common view among cyber technologists is that interfering with computers and the processes they support is the greatest harm that can occur. In suggesting that cyber attacks are an effective application of "force," far-more-serious end results are envisaged here. Societies depend on infrastructure to deliver essential goods and services: electric power, communications, in-

formation, natural gas, crude and refined fossil fuel through pipelines, transportation of raw material, goods and people, water and waste purification and disposal, etc. These depend on rotating machinery, pumps, pipes, circuit boards, and other devices. They are all managed by computers, so they do function as intended by their designers. Cyber attackers can "get into" their computer-based command and control systems and instruct those systems to operate beyond their design limits, causing them to destroy themselves. Such physical destruction is far more serious than causing computers to stop, because the time to repair the damage depends on repair crews, the availability of spares, and the control and repair of associated damage caused when large amounts of the kinetic, electrical, and hydraulic energy involved in their operation are released in an uncontrolled manner. Such attacks are discussed in Stephen J. Lukasik, "Mass–Effect Network Attacks: A Safe and Efficient Terrorist Strategy," SAIC report to the Defense Threat Reduction Agency (DTRA), January 2007.