

This research paper has been commissioned by the International Commission on Nuclear Non-proliferation and Disarmament, but reflects the views of the author and should not be construed as necessarily reflecting the views of the Commission.

NEW WEAPONS TECHNOLOGY

Compiled by Ken Berry, Research Coordinator ICNND.¹

EXECUTIVE SUMMARY

A wide range of new weaponry or weapons technology with links to nuclear weapons already exists or is being developed. Perhaps the most significant is a whole new approach to warfare using computers and the internet: cyberwarfare which has the potential to become a force equaliser *par excellence*. A large number of states are developing sophisticated capacities in this regard. Military and defence establishments around the world are these days routinely penetrated by foreign hackers, sometimes on a massive scale. Events in Estonia and Georgia in recent years have demonstrated how essential public services and utilities can easily be brought down. Even more serious is the potential for military command and control facilities, including those of nuclear-armed states, to be taken over. Currently, however, it is not possible to trace a cyberattack to its source.

Deriving directly from nuclear explosions are electromagnetic pulse (EMP) weapons which can destroy all electrical systems over a wide area. A range of non-nuclear EMP weapons has now been developed by a number of countries which have a similar range to nuclear weapons, but without the latter's destructive capacity and radioactive fallout.

The United States and Russia have developed a number of conventional weapons whose effects have been likened to those of smaller tactical nuclear weapons. These include fuel-air explosives or thermobaric bombs which use finely powdered particles and atmospheric oxygen to greatly enhance the blast effects of conventional explosives. The US has also developed a Massive Ordnance Air Blast bomb (MOAB) (colloquially known as the Mother Of All Bombs) using new types of high energy explosives, and designed primarily to destroy deeply buried or hardened targets. The Russians responded with a 'Father of All Bombs' which they claim to be more powerful than the MOAB.

The United States is also developing an appropriately named 'Future Combat Systems (FCS) which is in effect a combination of advanced robotics systems, including unmanned ground vehicles, unmanned combat aerial vehicles (UCAVs), non-line of sight launch systems and directed energy weapons (DEWs or attack lasers). Because of the speed involved in engagements with such weapons, however, human reaction times and coordination skills are swiftly becoming insufficient. There is consequently a need for smarter—and smaller—autonomous systems to control such weapons.

These are very much in development, using nanotechnology—itsself a product of nuclear laboratories. Prototypes of autonomous surveillance vehicles the size of insects already exist, and research is underway into combing nanotechnology with the emerging science of nuclear fusion for the production of very small nuclear weapons.

¹ This paper is derived from a variety of existing articles, all of which are footnoted.

Introduction

While a number of the NPT nuclear weapons states (NWS) have at various times in the past decade indicated a desire to update their current nuclear arsenals (and some at least are believed to be doing so), a number of them have been working on new classes of weaponry—indeed, of warfare—some of which have implications for nuclear non-proliferation and disarmament.

It does well to recall that military weaponry and concepts are developing and advancing so quickly that they are often confused with—and dismissed as—science fiction. In this regard, the integration of mobile phones and the internet today would resemble science fiction to someone in the 1980s. Current militarily-applicable science and technology, under development or already in use, includes: augmented reality²; biotechnology; genetics; giving soldiers internal/biologic infrared, night vision, radar, and sonar capability³; GPS; force fields⁴; invisibility cloaks⁵; microwave guns⁶; nanotechnology; neuroscience; positron bombs⁷; robotic exoskeletons⁸; space-based weapons such as ANGELS⁹ and Rods from God¹⁰; telepathy¹¹; thought control of internet surfing and electronic devices¹²; unmanned ground combat vehicles¹³; and unmanned combat aerial vehicles¹⁴ (Pike 2008). Indeed, the US military is understood to be planning to build robot soldiers that would not be able to commit war crimes since the Geneva Conventions would in effect be embedded in their software.¹⁵

² Bonsor, Kevin. “How Augmented Reality Will Work”. 2008, <http://www.howstuffworks.com/augmented-reality.htm> .

³ Block, Ryan. “The Brain Port, Neural Tongue Interface Of The Future.” 2006.

<http://www.engadget.com/2006/04/25/the-brain-port-neural-tongueinterface-of-the-future/>

⁴ Hershkovitch, Ady. “Plasma Window Technology for Propagating Particle Beams and Radiation from Vacuum to Atmosphere.” 1998. <http://www.techbriefs.com/content/view/1834/32/1/0/> .

⁵ Mark, David. “Scientists one step closer to invisibility cloak.” Australian Broadcasting Commission news item 11 August 2008. <http://www.abc.net.au/news/stories/2008/08/11/2330897.htm> . See also Winkler, Tim.

“Dragonflies Prove Clever Predators.” 2003. Australian National University Media Release 5 June 2003. http://info.anu.edu.au/ovc/media/Media_Releases/_2003/_030605Dragonflies.asp .

⁶ “Beam It Right There Scotty.” 2005. <http://www.wired.com/science/discoveries/news/2005/07/68152> .

⁷ Davidson, Keay. “Air Force Pursuing Antimatter Weapons.” 4 October 2004, <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/10/04/MNGM393GPK1.DTL> .

⁸ “Berkeley Bionics Human Exoskeleton.” 2007. <http://www.youtube.com/watch?v=EdK2y3lphmE> . See also

Yeates, Ed. 2007. “Exoskeleton Turns Humans Into Terminators.” 2007, from

<http://www.youtube.com/watch?v=h2jIRKswnQ> .

⁹ Lewis, Jeffrey. “Autonomous Nanosatellite Guardian For Evaluating Local Space (ANGELS).” 2005. <http://www.defensetech.org/archives/001996.html> .

¹⁰ Adams, Eric. “Rods From God.” 2004. from <http://www.popsoci.com/scitech/article/2004-06/rods-god> .

¹¹ Braukus, Michael. “NASA Develops System To Computerize Silent Subvocal Speech.” 2004.

http://www.nasa.gov/home/hqnews/2004/mar/HQ_04093_subvocal_speech.html . See also “Put Your Mobile

Where Your Mouth Is.” 2002. <http://news.bbc.co.uk/2/hi/science/nature/2055654.stm> .

¹² “New Technology Can Be Operated By Thought.” 2007.

<http://www.sciencedaily.com/releases/2007/11/071107210708.htm> .

¹³ Bloom, James. “Robots ready to support soldiers on the battlefield.” 2008.

<http://www.guardian.co.uk/technology/2008/jun/26/robots.weaponstechnology> .

¹⁴ Pike, John. “X-45 Unmanned Combat Air Vehicle (UCAV).” 2008. <http://www.fas.org/man/dod-101/sys/ac/ucav.htm> .

¹⁵ “Robot soldiers to get a kinder software side”, *Sydney Morning Herald*, 2 December 2008.

CYBERWARFARE

The area with perhaps the greatest significance for the future of nuclear weapons is cyberwarfare—that is to say, the use of computers and the internet in carrying out operations normally associated with different levels of conventional warfare. Cyberwarfare can be both offensive and defensive.¹⁶ For the most part, the battlefields are virtual as they are located in cyberspace. However, in some cases, there could be very tangible outcomes on real battlefields.

In January 2007 China caused widespread concern by shooting down one of its old weather satellites with a ballistic missile. The United States, which is developing a space-based weapons systems, was particularly concerned. One of China's aims in doing so may have been to emphasise the point it has been unsuccessfully making in the Conference on Disarmament in Geneva that it is time to negotiate a treaty on the peaceful uses of outer space. And in fact, neither China nor any other country has any real need to resort to a kinetic kill weapon such as a missile to destroy future space-based weapons. It can instead achieve the same goal with far less cost and far more deniability by using cyberwarfare techniques.

Although there had been some isolated cases of viruses being introduced into early computer systems running public utilities in the United States, the first serious attack with national security implications is usually identified as having occurred in March 1994. The United States Air Force laboratory in New York was attacked, apparently via an internet service provider (ISP) in New York, though this was then traced on to Seattle, Washington, at which point, the trace was lost. Subsequent attacks on the laboratory occurred—over 150 from 100 apparently different points of origin. Investigators eventually learned of a hacker in the UK who had boasted of having successfully penetrated several US military offices. Scotland Yard was brought into the case and discovered the hacker was “phreaking”¹⁷ through Colombia and Chile to New York. The UK hacker was later observed targeting other sites such as NATO headquarters, Goddard Space Flight Center and Wright-Patterson Air Force Base, both in the United States, and the South Korean Atomic Research Institution. To the non-US targets, it appeared as though they were being penetrated from US military sites. An arrest warrant was issued, and the perpetrator arrested. He was a 16 year old schoolboy, assisted by a 22 year old Israeli technician. Since that time, this type of attack has multiplied exponentially. In 2005, for example, the Pentagon logged more than 79,000 attempted intrusions into its computer systems, of which it says 1300 were successful.¹⁸

One author has described cyberwarfare as the new ‘Cold War’.¹⁹ Another has wittily, but pointedly, described the various elements of cyberwarfare as ‘weapons of mass disruption’²⁰

¹⁶ Congressional Research Service. “Cyberwarfare”, Report for US Congress, 19 June 2001. <http://www.au.af.mil/au/awc/awcgate/crs/rl30735.pdf>

¹⁷ Closely related to hacking, it means using a computer or other device to trick a phone system.

¹⁸ Reid, Tim. “China’s cyber army is preparing to march on America, says Pentagon”, *The Times Online*, 8 September 2007. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece

¹⁹ Nucci, Antonio. “Cyber Security: Protection Against Cyberwarfare”, *Converge Network Digest*, 10 October 2008. Author is Chief Technology Officer, Narus Corporation, a major international cyber protection firm with headquarters in California. <http://www.convergedigest.com/bp/bp1.asp?ID=548&ctgy=>

as this is one of the main objectives of cyberwarfare, though certainly not the only one. In its 2007 annual report, the major multinational internet security company McAfee noted that at least 120 countries have been actively developing cyberwarfare capabilities, with financial markets, industrial corporations, government computer systems and public utilities as their principal targets. Countries such as Russia, China, India, and Cuba openly acknowledge they are developing cyberwarfare programs, and North Korea, Libya, Iran, and Syria are also thought to have developed significant capabilities in this regard.²¹ Equally, of course, countries such as the United States, the UK, France, Germany, a number of other NATO members, and Japan are also advanced in the field, and largely share a similar outlook on the subject.²²

Levels of Cyberwarfare

Some cyberwarfare operations closely mirror more traditional military or related activities, while others are new. They include, in increasing order of severity:

- Propaganda, and even disinformation, which can be easily spread amongst a target population or group via the internet.
- Web vandalism that defaces or changes the content of web pages. This is usually quickly detected and neutralised.
 - ‘Denial of Service’ (DoS) attacks might be included here. These involve deluging a target agency or website with an avalanche of messages or requests that the target system is unable to deal with, to the point that it crashes. Again, such attacks are usually quickly dealt with, though in some cases this might mean closing down the network for a period.
- Compromised hardware involving the embedding of malicious or overtly destructive software in computer systems.
- ‘Cyber Espionage’ involving use of computers and the internet to obtain secrets of whatever kind from governments, military and security agencies, commercial and industrial complexes, NGOs and even individuals. The means adopted vary, though they are usually illegal and often hard or impossible to detect. The objectives will also vary, though basically such operations are aimed at obtaining an advantage—be it political, military, diplomatic or commercial—over a real or potential rival or enemy.
 - As with traditional espionage, there are also ‘cyber counterintelligence’ operations aimed at identifying, penetrating and defeating foreign espionage networks, including cyber espionage operations.
- ‘Distributed Denial-of-Service’ (DDoS) attacks are more overtly hostile and damaging. A ‘botnet’ or network of hundred, indeed sometimes thousands, of computers is used in a concerted, widespread and maintained DoS attack against key systems in a target country. This occurred in Estonia in 2007 and more recently in concert with the Russian military action in Georgia in August 2008.
- System or equipment disruption is similar to DDoS, but relates more to interference with military computer and satellite systems Communication of vital information or

²⁰ Fritz, Jason. “How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness”, *Culture Mandala*, Vol. 8, No. 1, October 2008, pp.28-80. <http://www.international-relations.com/CM8-1/Cyberwar.pdf>

²¹ Office of [US] Naval Intelligence “Navy Names Nations Posing Cyber Threats”, *Defense Week*, 5 September 2000, p. 1.

²² In the view of some observers, however, France may hold somewhat different views about the legitimacy of economic cyberwarfare as a valid weapon. Congressional Research Service, *op. cit.*

orders can be blocked or substituted, with serious consequences for troops on the ground.

- Cyber attacks on critical infrastructure computer systems, including power, water, fuel, communications, financial and transportation.

A Force Equalizer

In the past two decades in particular, much has been written about asymmetric warfare, where one side or the other in a conflict seeks to use different tactics and weapons to compensate for the superiority of their opponents in conventional or other weaponry. When one side has nuclear weapons, this becomes asymmetric warfare *par excellence*.

It has become apparent to many states, as well as to many non-state actors, that cyberwarfare is a significant force equalizer. For an extremely modest outlay on computer equipment and a small number of trained personnel, a state or non-state group can obtain a capacity which is virtually equivalent to that of a traditional army.²³ Using cyberwarfare techniques, they can destroy an enemy's industrial infrastructure or cripple the financial sector and economy more generally. They can also cripple an enemy's military command and control centres, severely undermining or destroying its capacity to respond effectively, if at all, to conventional military attacks by normally inferior forces. Indeed, as the more technically advanced—and largely Western—states develop more and more sophisticated cybernetic systems, and place increasing reliance on them, they are opening themselves up to the ever increasing possibility of hostile cyber attacks. This is *a fortiori* the case if the cyber attacks are directed against another state's nuclear arsenal and control systems.

China in particular regards cyberwarfare as a legitimate form of asymmetrical warfare.²⁴ It is understood to be developing a battalion size unit of highly trained computer experts for this purpose. Several large annual training exercises have already taken place since 1997. China is also active in the debate occurring in the Shanghai Cooperation Organisation²⁵ which is seeking to define a legal framework and possible rules of engagement which would cover cyberwarfare.²⁶

Perhaps not surprisingly, the United States provides an attractive target. Over the past decade or so, the US Armed Forces have been developing a new military doctrine called 'Network-Centric Warfare' (NCW) involving heavy reliance on sophisticated computer-controlled weapons and sensor systems, and ever more complex command and control centres. Today, a bombing mission by the US Air Force can be organised nearly instantaneously, using satellite photos which give accurate coordinates for a target. And this information can be transmitted

²³ "Cyberwarfare" (No author specified.) <http://www.security-gurus.de/papers/cyberwarfare.pdf>

²⁴ Cyberwarfare is seen as a "transformation from the mechanized warfare of the industrial age to ... a war of decisions and control, a war of knowledge, and a war of intellect." Military Strategic Research Center, Beijing, May 1996.

²⁵ An intergovernmental mutual-security organization which was founded in 2001 by the leaders of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.

²⁶ US Department of Defense. Annual Report to Congress: Military Power of the People's Republic of China 2008. <http://www.globalsecurity.org/military/library/report/2008/2008-prc-military-power.htm>

via email to an aircrew already in flight. During the first Gulf War, it could take up to two days to get a photo of the target and plan the mission. Similarly, US ground forces no longer have to rely on maps and radio reports, but can keep track of their troops in real time on computers.²⁷

The US Department of Defense, moreover, is currently advocating the creation of a ‘Global Information Grid’ (GIG) which would be the connecting framework for NCW. All of these advanced weapons platforms, detection and other information-gathering systems and command and control centres, would be linked to the GIG. The aim is to achieve information superiority by making all the data stored on the GIG available on demand to policy-makers, as well as to military and support personnel anywhere in the world.²⁸

But such technical and information superiority comes at a cost. For NCW to be effective, all aspects of the network need to work both continuously and well. This presents the enormous logistical challenge of keeping literally thousands of computer and other IT systems working in unison in the many parts of the world where US forces are in action or through which they must travel. This in turn requires a high degree of control over the land, sea and air space in those areas. As one writer notes, this is an enormous requirement which the United States does not do well in peacetime; and there is no good reason to think the US military can achieve it while fighting a competent enemy.²⁹ The sheer volume of information available also threatens to swamp available analytical capacity. Quantity after all does not necessarily equate with quality. An enemy’s smaller information-gathering network might thus be superior in operational terms.

Moreover, this pursuit of dominance could be categorized as American “hegemony” which is widely—and increasingly—resented by friends and foe alike. In other words, the US drive for information superiority could be creating a dangerous spiral, increasing international tension which only further bolster US military convictions that it needs such superiority.³⁰

Cyber Terrorism

One other aspect of cyberwarfare warrants special mention, and that is cyber terrorism. Many, if not most, of the major terrorist organisations in the world today maintain their own websites which are used mainly for propaganda purposes. In some cases, the websites are also used for fundraising and to maintain communication links between clandestine groups in other countries. It does not require a particularly large leap of the imagination to conjecture that terrorist groups could also be planning cyber attacks on significant public utilities in selected target countries such as the computer systems underpinning telecommunications, banking and finance, and transportation. Opening the floodgates of dams could kill thousands; switching off or destroying the control systems of power stations could bring

²⁷ Fritz, *op. cit.*

²⁸ *Ibid.*

²⁹ Gentry, John A. “Doomed to Fail: America’s Blind Faith in Military Technology”, *Parameters*, Winter 2002–03, US Army War College, Carlisle. <http://www.carlisle.army.mil/usawc/parameters/02winter/gentry.pdf>

³⁰ *Ibid.*

industry to its knees; destroying banking or share market records could cause economic havoc. However, while it is not possible to be absolutely definitive about this in the realm of cyberwarfare, it does not appear as though any such attacks have yet occurred. Certainly no terrorist groups have yet claimed responsibility for any of the tens of thousands of cyber attacks which have occurred around the world.

It would be foolish, however, to write off the possibility altogether. One of the great fears in the nuclear field is of terrorists building or acquiring a nuclear bomb or radiological weapon such as a 'dirty' bomb. In the realm of cyberwarfare, they might not need to go to the trouble. One concern is whether a terrorist group with readily available and cheap computer systems could hack into the computer controls of, say, a nuclear power station and cause its nuclear core to melt down. However, it is international practice to ensure that reactor control systems are isolated from external connections – and in any event safety systems operate automatically, independent of human intervention. Another concern is whether terrorists could hack into the command and control systems of one of the nuclear armed states and create the impression that the country is being attacked by nuclear missiles fired by another nuclear armed state. Even if a retaliatory strike were not launched or was aborted, the effect on international relations, and in the minds of the public around the world, would be serious indeed.

Responses to the Threat

As one writer put it, with cyberwarfare, instead of seeking protection against physical armies using guns and bullets, states and organisations today must guard against virtual armies whose weapons of choice are worms and viruses.³¹ However, while the threat is recognised, the response to date has been mixed. This remained the case even after the concerted and sustained 'Distributed Denial of Service' (DDoS) attack on Estonia in 2007 caused most official websites to be closed down for a lengthy period, with severe disruption of the national economy as a result. Even less international attention was paid to a similar attack on Georgian websites in the early days of the Russian military intervention in that country in August 2008.

Despite the increasing scale of cyber attacks and the acknowledged threat they represent, the response by governments around the world has tended to be *ad hoc*. At best, it is also compartmentalised. Governments tend to see their responsibility for dealing with cyberwarfare as focusing only on identifiable threats to national security such as the hacking of government departments or military systems, and perhaps some types of critical infrastructure. Attacks on industry or financial institutions tends to be regarded as the responsibility of the companies involved, perhaps in cooperation with local police. In Western democracies in particular, this is compounded by a desire not to be seen to grant the armed forces a role in what is regarded as essentially civilian problems.

Ethical Dilemmas

³¹ Nucci, *op. cit.*

There are also some ethical dilemmas that need to be considered when planning responses to cyber attacks. First, there is the major question of whether a cyber attack can in any circumstance justify a counter-attack using conventional weaponry. Russia, for example, has stated clearly in the past that, in relation to cyberwarfare generally, a response not only with conventional weapons, but even with weapons of mass destruction, may be justified.³² It is not known to what extent this may still represent Russian thinking. However, depending on the nature or severity of the cyber attack, it is relatively easy to see why a country might assess that it has little alternative to such a response. If the attack, for instance, was aimed at gaining control over a country's military command and control systems, including its nuclear forces where they exist, this could be regarded with some justification as a fundamental threat to the future of that state and thus warranting an extreme response. Whether other countries would see matters in this light if, of course, moot, and this would *a fortiori* be the case if the target was less critical infrastructure or systems.

One of the extreme difficulties in this regard is that, with the current state of cyber technology, it is still not possible to ascertain exactly where a cyber attack has originated. As already noted, in the many such attacks recorded in the past two decades, with relatively few exceptions, the routing of an attack through a large number of computers (known in this case as proxy servers) scattered around the world has effectively hidden the instigator. While the attacked country might harbour suspicions, sometimes probably well-founded, about the attacker's identity, in the end they remain just that: suspicions. Would a counter-attack with conventional weapons, let alone WMD, be justified in those circumstances? Definitely not, especially when there is always the possibility that the real attacker has deliberately caused the victim to believe that the attack originated in a third country, precisely to cause that third country to be attacked by the first, or at the very least to cause it to be criticised by other countries as a cyber-aggressor.

Indeed, it must even be questioned whether a cyber counterattack which destroyed the intermediate computers would even be justified, particularly when the owners of those computers had no knowledge of them being used in this way.

From 2003 to 2006, computer systems in defence or security related agencies and laboratories in the United States and UK were subjected to sustained and repeated attacks which have come to be known collectively as 'Titan Rain'. Considerable amounts of material, though not all of it classified, was copied and sent to an internet address which appeared to be in China. However, this was never firmly established—much less whether the attacks were state-sponsored or the work of private hackers. A similar series of attacks on the Pentagon and defence-related think-tanks and laboratories occurred in 2008, also appearing to originate in China, though again this was never firmly established.³³

³² "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself." V.I. Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'", (Concept of Information Warfare), speech given at the Russian-U.S. conference on "Evolving post Cold War National Security Issues," Moscow 12-14 September 1995 p 7. Cited in Col. Timothy Thomas, "Russian Views on Information-Based Warfare." Paper published in a special issue of *Airpower Journal*, July 1996.

³³ Fritz, *op. cit.*

Indeed, the only way currently to firmly establish the real identity of the cyber attackers would be to send a team of covert investigators out into the field to physically track the source. This is simply not a feasible proposition for any number of reasons.

It is no real surprise, therefore, that a number of countries are devoting increasingly large amounts of money to the development of accurate tracking technologies. In October 2008, for example, the United States Air Force indicated it was developing a program based on an innovative reformulation of the underlying code of the internet itself, in the hope of thus being able to block cyber attacks and accurately trace the attackers.³⁴ Earlier in the year it had called for submissions that would assist it in developing what it called ‘Proactive Botnet Defense Technology’³⁵—the defensive side of a program which would give the USAF “Dominant Cyber Offensive Engagement”. This would include taking “full control of a network for the purposes of information gathering and effects-based operations” and the ability to “deceive, deny, disrupt, degrade, destroy (D⁵)” a targeted computer system.³⁶

ELECTROMAGNETIC PULSE WEAPONS

Another new type of weapon was originally derived from nuclear weaponry. Collectively, they are known as ‘Electromagnetic Pulse’ (EMP) weapons. They already exist and new technological breakthroughs have meant the development of new applications for EMP weapons in both strategic and tactical warfare. The development of ‘conventional’ (i.e. non-nuclear sourced) EMP devices also allows their use in non-nuclear confrontations.³⁷

Nuclear EMP Weapons

In the immediate aftermath of a high altitude nuclear test in the South Pacific in 1962, it was noted that some electronic systems as far away as Hawaii no longer functioned. It was theorized that the nuclear explosion had generated a broadband, high-intensity, short-duration burst of electromagnetic energy which had caused a large voltage surge which destroyed electrical systems. In further experimentation, it was found that during a nuclear EMP, the magnetic flux lines of the Earth alter the dispersion of energy so that it radiates very little to the North, but spreads out East, West, and South of the blast. The signal is divided into several time components, and can result in thousands of volts per metre of electromagnetic energy ranging from extreme negative to extreme positive polarities. This energy can travel long distances on power lines and through the air.³⁸ It was also noted that EMP did not seem to affect electronic devices using vacuum tubes, although it certainly destroys both transistors

³⁴ Schactman, Noah. “Air Force Aims to ‘Rewrite Laws of Cyberspace’”, *Danger Room – What’s Next in National Security*, Wired Blog Network, 3 November 2008. <http://blog.wired.com/defense/2008/11/air-force-aims.html>

³⁵ Matthews, William. “Cyberwarfare Wish List: U.S. Air Force Calls for Help in Beefing Up Specific Capabilities”, *Defense News*, 26 May 2008. <http://www.defensenews.com/story.php?i=3553238>

³⁶ *Ibid.*

³⁷ Kopp, Carlo. “The Electromagnetic Bomb – a Weapon of Electrical Mass Destruction”, GlobalSecurity Report, 1996. <http://www.globalsecurity.org/military/library/report/1996/apjemp.htm>

³⁸ Wikipedia. “Electromagnetic bomb”. http://en.wikipedia.org/wiki/Electromagnetic_bomb

and electronic silicon and integrated chips. For this reason, many long range Soviet bombers, and indeed MiG fighters, during the Cold War only used hardened vacuum tube technology.³⁹

An aggressor state deploying such weapons could destroy the vast majority of a target country's electronics, including computers, cars, phones, and the power grid. All nuclear armed states have the capacity to achieve this, and it has been estimated that as little as three high altitude nuclear explosions could blanket an area the size of continental US,⁴⁰ Western Europe, Australia, or Brazil. Open source material has indicated that the US, China, France, and Russia have all used the tactic of an EMP as a surprise first strike in war games.⁴¹ Chinese military writings have described scenarios where EMP—presumably non-nuclear—is used against U.S. aircraft carriers in a conflict over Taiwan.⁴² A survey of worldwide military and scientific literature found widespread knowledge about EMP and its potential military utility in countries including Taiwan, Israel, Egypt, India, Pakistan, Iran, and North Korea. Moreover, some terrorist organizations have apparently sought information relating to EMP produced by nuclear weapons, as well as on the technology of directed energy weapons. These are small non-nuclear weapons that produce an EMP-like effect, but over a very much more restricted area.⁴³

However, it is unlikely—though unfortunately, not impossible—that any nuclear armed state these days would use EMP generated by nuclear weapons. Using an atmospheric nuclear blast would attract international opprobrium, both for its proliferation implications and also, increasingly important, for its effects on the environment. As has been discussed above, the same widespread effects of shutting down a nation's power grid, production lines, water utilities, chemical plants, financial institutions, telecommunications, and transportation routes could be achieved by cyber attack. Moreover, given the difficulty of tracing the perpetrators of cyberwarfare, responsibility for such an attack would be deniable.⁴⁴

Generally speaking, the shorter pulse wave forms, such as microwaves, are far more effective against electronic equipment and more difficult to devise hardened protection against.⁴⁵ For maximum effect, the electromagnetic burst must be in the upper atmosphere. Thus, such a weapon stationed in space could in theory knock out electrical systems, including computers and communications, across continent-wide distances. With this in mind, the Soviet Union

³⁹ This was, however, to an extent serendipitous since for many years the Soviets did not have access to solid state electronics. Later they realized that vacuum tubes were advantageous, and they decided to retain them.

⁴⁰ Bartlett, Roscoe. "Nuclear Electromagnetic Pulse", US Congressional Record, 9 June 2005.

<http://cryptome.org/bartlett-060905.txt>

⁴¹ Nock, Howard and Lizun, Daniel. "Cyberterrorism and Cybercrime: Are You Prepared", 2007 <http://www.clevelandfed.org/bsr/Conditions/v3n2/v3n2.htm> ; U.S.-China Economic and Security Review Commission. "China's Proliferation Practices, and the Development of Its Cyber and Space Warfare Capabilities", 20 May 2008 http://www.uscc.gov/hearings/2008hearings/hr08_05_20.php ; Qiao, Liang and Wang Xiangsui. 1999. *Unrestricted Warfare*. PLA Literature and Arts Publishing House, Beijing, February 1999. <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>

⁴² Bartlett, *supra*.

⁴³ *Ibid*.

⁴⁴ Fritz, *op. cit*.

⁴⁵ Kopp, Carlo. "High-Power Microwave (HPM)/E-bomb", GlobalSecurity.org.

<http://www.globalsecurity.org/military/systems/munitions/hpm.htm>

developed nuclear weapons designed for detonations in the upper atmosphere. The United States and the United Kingdom also carried out similar research. It is believed that most of the nuclear EMP weapons were disarmed following the Reagan/Gorbachev arms talks in the 1980s.

Non-Nuclear EMP Weapons

EMP weapons have also been developed which have no link at all to nuclear weapons. As a class, they are known as ‘Non-nuclear electromagnetic pulse (NNEMP)’ weapons. The electromagnetic pulse in such weapons can be generated in a number of ways. One is to build up a charge in a bank of capacitors and release it in one short, major burst through either a loop antenna or a microwave generator, taking advantage of the electromagnetic field generated in any electrical circuit. To achieve the frequency characteristics of the pulse needed for optimal coupling into the target, wave-shaping circuits and/or microwave generators are added between the pulse source and the antenna.⁴⁶ Such a device can be used multiple times.

At the other end of the spectrum are devices which use what are known as ‘explosively pumped flux compression generators’ to propagate the electromagnetic pulse. This is in fact a fancy way of saying that the pulse is generated by a massive conventional explosion. It has the advantage that the pulse can be more directionally focused, but it goes without saying that such devices can only be used once. This type of NNEMP generator can be carried not only as part of a conventional bomb, but also by cruise missiles. It is understood that the United States in particular has also done considerable work on the incorporation of a high power microwave weapon into unmanned aerial vehicles (UAVs).⁴⁷ The lack of radioactive fallout removes from this class of weapons the stigma—and political consequences—attaching to nuclear weapons.

According to some reports, the U.S. Navy used experimental EMP bombs of this kind during the early days of the 1991 Gulf War to knock out Iraqi electronic systems.⁴⁸ Their exact effect in that case is not known, however, since other weapons were used to disrupt and destroy Iraqi communications systems, and the power grid was heavily bombed with conventional weapons. CBS News also reported that the U.S. dropped an ‘E-bomb’ on Iraqi TV during the 2003 invasion of Iraq, but this has not been confirmed.⁴⁹

The type of weapon just described, which uses conventional explosives to generate the microwave surge, will cause the usual effects of severe injury or death of humans in the target vicinity. Depending on the damage required of such a weapon, it might be considered more desirable to minimise or dissipate the explosion, thus lowering the collateral damage to

⁴⁶ Wikipedia. “Electro-magnetic pulse”, http://en.wikipedia.org/wiki/Electromagnetic_pulse

⁴⁷ Kopp, *supra*.

⁴⁸ Kopp, *supra*.

⁴⁹ Martin, David. “U.S. Drops ‘E-Bomb’ on Iraqi TV”, CBS News report, 25 March 2003.

<http://www.cbsnews.com/stories/2003/03/25/iraq/main546081.shtml>

humans, and to maximise the electrical damage by bolstering the electromagnetic surge. Microwaves are only dangerous to humans in close proximity.

In most circumstances, modern non-nuclear EMP weapons are categorized as non-lethal because of the minimal collateral damage they create. This also gives military commanders more politically-friendly options to choose from.

Any electronics within range of the E-bomb that have not been adequately protected have a high probability of being damaged or destroyed. The best way to defend against an EMP attack is to destroy the platform or delivery vehicle in which the E-bomb resides before the weapon is detonated. This in turn suggests that good air defence systems are required. Another method of protection is to shield all essential electronics within an enclosure, called a Faraday cage, which diverts the electromagnetic surge around the target devices. The problem with such enclosures is that most vital equipment needs to be in contact with the outside world via power grids or communication lines. Such contact points would allow the electromagnetic pulse to avoid the cage entirely, thus rendering the attempts at protection useless. There are ways to protect against these flaws. Critical electronic systems can have autonomous power systems, but these apparently must be buried surprisingly deep in the earth to avoid the effect of the EMP. And the fact thus remains that the Faraday cage option is a point of vulnerability in protecting against the effects of an EMP weapon.⁵⁰

FUEL-AIR WEAPONS

Fuel-air explosives (FAE or FAX)—also known as fuel-air munitions, heat and pressure weapons, vacuum bombs or thermobaric weapons—unlike conventional explosive weapons use atmospheric oxygen, instead of carrying an oxidizer in their explosives.⁵¹ By doing so, they produce more explosive energy for a given size than do other conventional explosives, but have the disadvantage of being less predictable in their effect as they can be influenced by weather. A fuel-air explosive consists of a container of finely powdered solid fuel of differing particle size mixed with a low percentage of oxidizer and binder. The solid fuel could be an explosive metal powder or reactive organic substance. A high explosive charge is placed in the middle of the mixture. Once the weapon is fired or dropped from a plane, the explosive charge pulverizes the container, dispersing the fuel in a cloud, which is then ignited by the explosion. The heat released then ignites the smaller solid particles mixed with the compressed hot air behind the blast wave. This sustains an environment which allows 100% fuel combustion to be achieved.

The main destructive force of FAE is high pressure. The rapidly expanding wave front due to overpressure literally flattens all objects within close proximity of the epicentre of the aerosol fuel cloud, and produces serious damage well beyond the flattened area. More importantly, the duration of the overpressure gives it an edge over conventional explosives and makes fuel-air explosives useful against hard targets such as minefields, armoured vehicles, aircraft parked in the open, and bunkers.

⁵⁰ *Ibid.*

⁵¹ This section is derived from a *Wikipedia* entry on Thermobaric Weapons.

There are dramatic differences between explosions involving high explosives and FAEs at close distances. For the same amount of energy, the high explosive blast overpressure is much higher and the blast impulse is much lower than that from an FAE explosion. The shock wave from a TNT explosion is of relatively short duration, while the blast wave produced by an explosion of hydrocarbon material displays a comparatively long duration. The duration of the positive phase of a shock wave is an important parameter in the response of structures to a blast.

The effects produced by FAEs (a long-duration high pressure and heat impulse) are often likened to the effects produced by low-yield nuclear weapons, but without the problems of radiation. While this analogy is scientifically inexact, the injury dealt by either category of weapon on a targeted population and/or infrastructure is nonetheless great.

*The 'Mother of All Bombs'*⁵²

The Massive Ordnance Air Blast bomb (MOAB) (colloquially known as the Mother Of All Bombs) is a large-yield conventional bomb developed for the United States armed forces. Development of the MOAB began in 2002, and it was successfully field tested twice in 2003. It was designed to be delivered by a C-130 and originally used the explosive tritonal. The US Air Force Research Laboratory has said a larger version of the MOAB exists, weighing thirteen tons.

Apart from the two initial test weapons, the only known production figure for the MOAB was a run of 15 units produced in 2003 ostensibly in support of the invasion of Iraq that year. Since none of those are known to have been used as of early 2007, the US inventory of the MOAB presumably remains at approximately 15.

The effect of the MOAB has, like the FAE, also been compared to that of a nuclear weapon. Indeed, the US Air Force ran a series of tests, using a video of the 2003 tests as the subjects. Most of those who watched the video compared the explosion (incorrectly) to that of an atomic bomb. However, the MOAB has only about one thousandth the power of the atomic bomb used against Hiroshima. It is equivalent to around 11 tons of TNT, whereas the Hiroshima blast was equivalent to 13,000 tons of TNT. Modern nuclear missiles are far more powerful than that. In reality the MOAB bomb's yield is comparable to the smallest of current tactical nuclear devices.

While the MOAB is primarily intended for deep and hardened targets, it can also be employed against soft to medium surface targets covering extended areas. However, multiple strikes with lower yield ordnance may be more effective and can be delivered by fighter/bombers such as the F-16 with greater stand-off capability than the C-130 and C-17 which would be used for the MOAB. High altitude carpet-bombing with much smaller 2,000 or 1,000 pound bombs delivered via B-52s is also highly effective at covering large areas.

⁵² Wikipedia. The weapon's military designation is GBU-43/B.

Since the original development of the MOAB, Russia has tested its own ‘Father of All Bombs’ which it claims to be four times more powerful than the MOAB. However, doubts remain about the accuracy of this claim.⁵³

FUTURE COMBAT SYSTEMS

One existing US project that is gaining attention is the appropriately named Future Combat Systems (FCS).⁵⁴ FCS is in effect a combination of a number of others systems involving advanced robotics, which include unmanned ground vehicles, unmanned combat aerial vehicles (UCAVs), non-line of sight launch systems, and ‘Unattended Systems’. “This system of systems seeks to make warfare as networked as the internet, as mobile as a mobile phone, and as intuitive as a video game.”⁵⁵ While the US has yet to determine a definitive name for this new type of information based, highly networked, and highly technological warfare, it is clear that the US government has spent a significant amount of time and money seeking to make it a reality.⁵⁶

Another US project which has developed weapons capable of acting at the speed of light are Directed Energy Weapons (DEWs). These include laser, microwave, and charged particle or neutral particle beam devices. All are based on the emission of electromagnetic energy at different frequencies, usually in focused beams. They can be vastly more accurate than conventional weapons because they follow line-of-sight rather than ballistic trajectories, thus eliminating all the problems of ballistics.⁵⁷ The first operational light-speed weapon, the US Air Force's Yal-1a Attack Laser (also known as ABL or Airborne Laser), was first test flown in 2004, though is still said to be in its development stage.⁵⁸

One advantage of such weapons is that missing the target is less important, since the system will be able to cycle quickly and fire off another speed-of-light burst, this time having corrected its aim. With DEWs, active countermeasures (dodging, throwing chaff, deploying decoys, returning fire) become enormously more difficult and in many cases impossible. Because of the speed involved in engagements with such weapons, however, human reaction times and coordination skills are swiftly becoming insufficient. There is consequently a need for smarter—and smaller—autonomous systems to control such weapons.

⁵³ *Ibid.*

⁵⁴ The following is derived from Fritz, *supra*.

⁵⁵ *Ibid.*

⁵⁶ FCS Watch 2008 http://www.defensetech.org/archives/cat_fcs_watch.html . See also “Future Combat Systems” 2008 <http://www.globalsecurity.org/military/systems/ground/fcs.htm>; Baard, Mark. “Sentient World: War Games on the Grandest Scale.” 2007, http://www.theregister.co.uk/2007/06/23/sentient_worlds/ ; Klein, Alec. 2007. “The Army’s \$200 Billion Makeover.” 2007, <http://www.washingtonpost.com/wp-dyn/content/story/2007/12/06/ST2007120602927.html> .

⁵⁷ Hillaby, Bill. "Directed Energy Weapons Development and Potential," *National Network News*, July, 1997, published by The Defense Associations National Network, Ottawa, Canada, http://www.sfu.ca/~dann/nn4-3_12.htm

⁵⁸ “YAL-1A”. Fact Sheet 2008. http://www.deagel.com/Long-Range-Attack-Aircraft/YAL-1A_a000512001.aspx

NANO-TECHNOLOGY

Automated and semi-automated conventional weapons systems already exist and are becoming steadily more sophisticated. Cruise missiles are just one such system, able to autonomously execute missions formerly requiring manned systems. However, as computer science has progressed exponentially in recent years, with chips becoming ever smaller yet and their computational power increasing enormously, the many benefits of downsizing—some of which still sound like science fiction—have become more practicable.⁵⁹ Over the years, some systems have become even more independent, such as the US Navy's Phalanx air defence weapon, which is "capable of autonomously performing its own search, detect, evaluation, track, engage, and kill assessment functions."⁶⁰ Thanks to advanced sensors and information processing, target recognition and identification methods are being developed to permit truly autonomous guided munitions. This includes munitions capable of autonomously engaging fixed and mobile ground targets, as well as targets in air and space.⁶¹ As one author has stated, warfare has begun to leave "human space."⁶²

More in the category of 'work in progress' are efforts to harness the still relatively nascent science of nanotechnology—in effect the use of extremely miniaturized robots—to develop new classes of weapons. Nanotechnology is itself the product of nuclear weapons laboratories. In 1998, scientists at the Los Alamos National Laboratory in New Mexico announced that they had been able to consistently manipulate subatomic particles. The most obvious application at the time was seen to be development of computers and communications systems many times smaller and faster than those which are still the norm today.⁶³ The following year, researchers at UCLA and Hewlett-Packard succeeded in constructing microscopic integrated circuits using single molecules as building blocks. The project leader speculated that a molecular computer could be developed which would have the processing power of 100 conventional personal computers but be the size of a grain of salt.

This development is extremely important in the context of weapons design. Extremely small computers will have a huge variety of applications across the board. However, as the computing power and memory capacity of these miniaturised devices approaches those of current supercomputers, the prospect of developing autonomous—in other words, self-controlled—mobile weapons systems is likely to reach practical realisation.

⁵⁹ This section is derived largely from Adams, Thomas K. "Future Warfare and the Decline of Human Decisionmaking", US Army War College Parameters, Winter 2001-02, pp. 57-71.

<http://www.carlisle.army.mil/usawc/parameters/01winter/adams.htm>

⁶⁰ US Navy, Phalanx CIWS (Close-In Weapon System) information sheet,

<http://www.chinfo.navy.mil/navpalib/factfile/weapons/wep-phal.html>

⁶¹ "Our Mission," Public Affairs Office, Advanced Guidance Division of the Air Force Research Laboratory, Wright Patterson AFB, Ohio, March 2000.

⁶² Adams, *supra*.

⁶³ "Breakthrough Made in Subatomic Manipulation," Scripps-Howard newspapers, 8 November 1998,

<http://www.nandotimes.com> .

From a military point of view, small systems are highly desirable as they require less resources to transport and less fuel to operate. They are much more difficult for an enemy to detect and, even if detected, that much harder to target and hit. The viability of such systems was demonstrated in January 1999, when Lockheed Martin, under contract with the US Department of Defense, began flight-testing an aircraft with a wingspan of 15 cm or six inches.⁶⁴ This work has continued, with US military laboratories now apparently working on a flying robot the size of a bee.⁶⁵

Earlier in the 1990s, Sandia National Laboratories in the US also produced a 'Miniature Autonomous Robotic Vehicle' (MARV) 16 cm³ or one cubic inch in size, containing all the necessary power, sensors, computers, and controls to operate independently. Although the original MARV was in fact limited in what it could do, developmental work has continued, with new generations of autonomous microsystems having been developed which are much smaller, smarter and capable of cooperating with other similar microsystems. Sandia is also developing technologies which, include the automated assembly of parts down to 100 microns in size.⁶⁶ In parallel, researchers at the Massachusetts Institute of Technology (MIT) have developed robots the size of ants which display some as yet limited aspects of intelligence and specialization, such as avoiding shadows and staying away from each other. They are apparently cheap to produce and easy to reprogram.

These developments are expected to launch a revolution in military thinking. According to researchers: "Thirty-five years from now, analogous small, lethal, sensing, emitting, flying, crawling, exploding, and thinking objects may make the battlefield highly lethal."⁶⁷ With such systems, military commanders will have tiny but very smart machines which could, for example, carry out reconnaissance missions and collect target and damage assessment information without direct human involvement and a low probability of being discovered. And it is even possible to envisage the development of similarly miniature autonomous vehicles to carry out even more complex tasks such as locating and disabling land mines, detecting weapons of mass destruction, including nuclear weapons, and verifying treaties. It has, moreover, been estimated that much of the foregoing could take place in another decade, or at most two.⁶⁸

Such systems could also be moved at speeds, accelerations, decelerations, and in complex manoeuvres that human bodies could never withstand. It is, for instance, possible to envisage launching enormous numbers of these devices at ballistic missile speeds, and having them in action on the other side of the globe in minutes. In such circumstances, they would need to be effectively autonomous since their sheer numbers would make remote control impractical,

⁶⁴ "Micro Air Vehicles," *UK Defence Forum*, March 1999, <http://www.ukdf.org.uk/ts6.html> , accessed 13 March 2000.

⁶⁵ "Bug sized spies: US develops tiny flying robots", *Sydney Morning Herald*, 22 November 2008.

⁶⁶ Sandia National Laboratories, Intelligent Systems and Robotics Center, Miniature Autonomous Robotic Vehicle (MARV) webpage, http://www.sandia.gov/isrc/Capabilities/Prototyping/Small_Smart_Machines/MARV/marv.html

⁶⁷ Institute for National Strategic Studies (INSS), *Project 2025*. National Defense University, Norfolk, Va. 6 May 1992, p. 36.

⁶⁸ Adams, *op. cit.*

and operating only to preset instructions could be potentially too limiting in battlefield situations. Moreover, future battles between opposing arrays of such autonomous systems are likely to occur with such complexity and at such speed as to make human intervention a practical impossibility.

As already noted, small systems such as these would be extremely difficult to target using conventional projectile weapons or even lasers. One potential countermeasure, particularly when such miniature systems are used in large numbers is probably an electromagnetic pulse weapon such as that described above.

Nano with a nuclear twist

One other aspect of nanotechnology warrants mention, namely the studies that are already underway into the possibility of linking nanotechnology with emerging practical applications of nuclear fusion. Nuclear fusion is in effect the driving force of suns.⁶⁹ In thermonuclear weapons—the hydrogen bomb—a fusion reaction triggered by the initial fission reaction greatly increases the power of the weapon. However, harnessing fusion for the generation of electricity has long eluded scientists. The first successful, controlled nuclear fusion reaction was only achieved a decade or so ago, and then on a small scale. However, fusion reactors for power generation, using new technology, are now in experimental stages at several laboratories in the United States and around the world. And a consortium of countries including the United States, a number of European states and Japan are in the process of building a nuclear fusion reactor in France.⁷⁰ Nevertheless, the general assessment is that no commercial fusion reactor can be expected to come on-line before 2050⁷¹—although there are some more optimistic views on this.

Three of the great attractions of nuclear fusion are the abundance of the required fuel (hydrogen), the low amounts of radioactivity generated, and the comparatively small amount of waste produced. It might be noted that although fusion power uses nuclear technology—and fusion is used in thermonuclear bombs—the overlap between commercial research into, and applications of, nuclear fusion with nuclear weapons technology is small. The neutrons produced in a fusion reactor could be used to breed plutonium for an atomic bomb, but not without extensive redesign of the reactor. Plutonium production would thus be difficult to conceal. Moreover, the theoretical and computational tools needed for hydrogen bomb design have very little in common with the type of fusion which has been most scientifically developed up to the present, namely magnetic confinement fusion.⁷²

Nevertheless, given the fact that mastery of nuclear fusion for civilian purposes has been demonstrated on a small-scale, and given also the minimal radioactivity generated by those reactions, the attraction of combining nuclear fusion with nanotechnology to produce

⁶⁹ Gray, Richard. “Scientists plan to ignite tiny man-made star”, *The Telegraph*, 27 December 2008.

⁷⁰ Freudenrich, Dr. Craig. “How Nuclear Fusion Reactors Work”, *How Stuff Works*. See also “Fusion Power”, Wikipedia entry.

⁷¹ “Fusion Power”, *supra*.

⁷² *Ibid.*

miniaturised and low yield nuclear weapons has become at least a possibility.⁷³ Moreover, it has become the goal of some US nuclear weapons-related laboratories which have been advocating development of precisely such a category of weapon for some time, as well as nuclear ‘bunker busters’ aimed at deeply buried or hardened targets.⁷⁴ However, the era of ‘nano nukes’ is probably still a considerable time in the future.

The concept of such weapons do, however, raise some thought-provoking issues which will need consideration at an appropriate time. They would not, for instance, fit the traditional model of a nuclear weapon which, even with the smaller tactical nuclear weapons, are characterised by the scale of the damage they can cause and their indiscriminate nature. A really small scale nuclear fusion weapon, on the other hand, could be very specifically targeted and would have no radioactive fall-out. The main danger with such weapons would lie in the possibility that they could be significantly scaled up in size.

⁷³ Gsponer, André. “From the Lab to the Battlefield? Nanotechnology and Fourth-Generation Nuclear Weapons”, *Disarmament Diplomacy*, No. 67, November 2002. <http://www.acronym.org.uk/dd/dd67/67op1.htm>

⁷⁴ Drell, Sidney, Goodby, James, Jeanloz, Raymond, and Peurifoy, Robert. “A Strategic Choice: New Bunker Busters or Nonproliferation”, *Arms Control Today*, March 2003. http://www.armscontrol.org/act/2003_03/drelletal_mar03