Defence Research and Development Canada
Recherche et développement pour la défense Canada

The Static Remote Weapon Problem

What will Appear on the Battlefield of Tomorrow?

D. Erickson and S. Monckton
Defence R&D Canada – Suffield

Technical Memorandum
DRDC Suffield TM 2005-084
October 2005

Canada

The Static Remote Weapon Problem

What will Appear on the Battlefield of Tomorrow?

D. Erickson, S. Monckton
Defence R&D Canada – Suffield

Defence R&D Canada – Suffield

Technical Memorandum

DRDC Suffield TM 2005-084

October 2005

Author

D. Erickson, S. Monckton DRDC Suffield

Approved by

D. Hanna
Head/Tactical Vehicle Systems Section

Approved for release by

Paul D'Agostmo
DRP Chairperson

Abstract

This paper describes the use of static remote-controlled weapons as an ambush tool that allows guerrilla/terrorist forces to more accurately inflict casualties and damage with less personal risk than a car bomb. This is possible due to the inexpensive and ubiquitous technology that exists in today's society worldwide. This paper provides a different perspective about what will appear on the battlefield in asymmetrical threat environments and why.

Résumé

Cet article décrit l'utilisation d'armes téléguidées stationnaires comme armes d'embuscade qui permet aux forces de guérilla ou terroristes de causer des victimes et d'infliger des dommages avec plus de précision et en prenant moins de risques que dans une voiture piégée. Ceci à cause de la technologie peu coûteuse et omniprésente qui existe dans la société actuelle et le monde entier. Cet article offre une perspective différente et la cause de ce qui aura lieu sur les champs de bataille, dans un milieu de menace asymétrique.

This page intentionally left blank.

Executive summary

This paper describes the use of static remote-controlled weapons as an ambush tool that allows guerrilla/terrorist forces to more accurately inflict casualties and damage with less personal risk than a car bomb. This is possible due to the inexpensive and ubiquitous technology that exists in today's society worldwide. This paper provides a different perspective about what will appear on the battlefield in asymmetrical threat environments and the importance of static remote weapons as a new threat.

There are six characteristics of static remote weapons systems that make these threats important:

1. Ubiquity- The technologies needed to automate weapons have been around for a long time, but the cost of this automation and the extended way in which cellular and internet networks can separate the attackers from the ambush weapons has never been so readily available, seamless, and cost-effective. These weapons depend on readily available hand weapons and there is no shortage of these parts.

2. Invisibility- The subcomponents of these remote weapons systems can be as simple as commercial- grade technology that will not stand out in check point searches in a conflict zone or overseas customs inspections. These weapons can be slipped through security without detection and then be reassembled at the ambush site.

3. Specificity- The aimed remote weapon increases the discrimination that can be used to target soldiers in a crowd or on the road. This allows groups to cause less local resentment by decreasing collateral damage. This improves on the basic car bomb that requires precise timing to hit the right vehicle or personnel.

4. Range of Lethality- These weapon systems do not need to be conventional weapons. The same technology could be used for nuclear, biological, chemical, electromagnetic, or internet denial of service weapons that span the continuum of conflict intensity.

5. Negligible Risk- These systems would allow groups to confront superior armies without personal risk. Determining who conducted the operation would take exhaustive investigation and reconstruction which means that these opponents may be able to slip out of the danger area undetected.

6. Psychology- Like minefields, the immunity to danger makes these remote weapon systems a psychological threat to friendly soldiers and civilians alike. Remote weapons will not be deterred by shelling or distractions and the operators, knowing they risk nothing personally, can await unsuspecting friendly troops until the last possible moment which increases their effectiveness and the shock factor of the attack.

The use of static remote weapons for defense by enemy troops should be considered as a threat for friendly forces in future conflicts in all intensity level conflicts. A complementary research thrust, focusing on the use of static remote weapons would be a useful addition to the research of autonomous robotics since the static remote/autonomous weapon is a less complex subset of the mobile robotics problem. It is important to study the impact and tactics of remote weapons to reveal the solutions that can counter them. Also, some consideration should be given to researching sensor systems, teleoperated vehicles, and electronic countermeasures that can detect and destroy static remote weapon systems prior to ambush.

D. Erickson, S. Monckton. 2005. The Static Remote Weapon Problem. DRDC Suffield TM 2005-084. Defence R&D Canada – Suffield.

Sommaire

Cet article décrit l'utilisation d'armes téléguidées stationnaires comme armes d'embuscade qui permet aux forces de guérilla ou terroristes de causer des victimes et d'infliger des dommages avec plus de précision et en prenant moins de risques que dans une voiture piégée. Ceci à cause de la technologie peu coûteuse et omniprésente qui existe dans la société actuelle du monde entier. Cet article offre une différente perspective de ce qui aura lieu sur les champs de bataille, dans un milieu de menace asymétrique et de l'importance de la nouvelle menace que représentent les armes téléguidées stationnaires.

Ces menaces sont sérieuses à cause des six caractéristiques communes aux systèmes d'armes téléguidées stationnaires :

1. L'omniprésence- Les technologies requises pour automatiser les armes existent depuis longtemps mais le coût de cette automation ainsi que l'étendue de la portée à laquelle les réseaux cellulaires et Internet peuvent séparer les attaquants de leurs armes d'embuscade n'ont jamais été aussi immédiatement réalisables, sans coupures et aussi économiques. Ces armes dépendent des armes de main facilement disponibles et il n'existe pas de pénurie de ces dernières.

2. Invisibilité- Les sous-éléments de ces systèmes d'armes télécommandées peuvent simplement consister en une technologie de classe commerciale qui ne sera pas remarquée durant les perquisitions aux postes de contrôle dans des zones de conflit ou durant les inspections douanières à l'étranger. Ces armes peuvent passer au travers des postes de sécurité sans être détectées puis ré-assemblées sur le site de l'embuscade.

3. Spécificité- Cette arme téléguidée au tir dirigé augmente le niveau de discrimination pour cibler les soldats dans une foule ou sur une route. Ceci permet aux groupes de causer moins de ressentiment localement en diminuant le dommage collatéral. Cette arme améliore aussi l'efficacité d'une voiture piégée requérant un minutage précis pour atteindre le véhicule ou personnel ciblé.

4. La portée de la puissance de destruction- Ces systèmes d'armes ne sont pas toujours des armes classiques. La même technologie pourrait être utilisée avec des armes nucléaires, biologiques, chimiques, électromagnétiques ou Internet refusées de service qui prolongent l'intensité d'un conflit.

5. Risque négligeable- Ces systèmes permettraient à ces groupes de confronter des armées supérieures sans prendre de risques personnels. Il faudrait mener une enquête exhaustive et effectuer une reconstitution pour déterminer qui sont les responsables de la conduite de l'opération ce qui permettrait à ces adversaires de s'éloigner de la zone dangereuse sans être détectés.

6. Psychologie- Comme les champs de mines, l'immunité au danger de ces systèmes d'armes téléguidées représentent une menace psychologique pour les soldats comme pour les civils. Les armes téléguidées ne se laissent pas dissuader par les bombardements ou les distractions ; les opérateurs, sachant qu'ils ne risquent rien personnellement sont en mesure d'attendre, jusqu'au dernier moment, les troupes amies qui ne se méfient pas ce qui augmente l'efficacité et l'effet du choc de l'attaque.

L'utilisation des armes téléguidées stationnaires par des troupes ennemies pour leur défense devrait être considérée comme une menace pour les forces amies dans les conflits futurs et de tous les niveaux d'intensité. Une orientation complémentaire de la recherche qui serait axée sur l'utilisation des armes téléguidées stationnaires serait utile à la recherche sur la robotique autonome puisque l'arme téléguidée autonome est un sous-ensemble moins complexe du problème de la robotique mobile. Il est important d'étudier l'impact des tactiques des armes téléguidées pour révéler les solutions capables de les contrer. De plus, il faudrait aussi considérer étudier les systèmes de détecteurs, les véhicules téléguidés et les contre-mesures électroniques qui peuvent détecter et détruire les systèmes d'armes téléguidées stationnaires antérieurement à l'embuscade.

D. Erickson, S. Monckton. 2005. The Static Remote Weapon Problem. DRDC Suffield TM 2005-084. R & D pour la défense Canada – Suffield.

Table of contents

List of figures

List of tables

1. Introduction

This paper reviews the implications of a conceivable threat on the battlefield of tomorrow derived from the inexpensive technology of today. It is this paper's contention that inexpensive remote-controlled weapons will grow as a potential threat and are no longer a theoretical supposition. Through example, this paper will discuss the impact of real systems that could be made with current unclassified and readily available technology. Some discussion of the counters to these threats are described here.

1.1 Background

The concept of remote controlled weapons is not new. Radio controlled weapons have been used for more than half a century. However, the growth in inexpensive electronics, software, and high bandwidth radio and cell networks has the potential to reduce the cost, size, and, therefore the probability, of remote weapon tactics. Specifically, the technologies behind remote controlled weapons, once limited to short range analog radio, has grown to include a number of consumer technologies, including video cameras, infra-red cameras, linear actuators, micro-controllers, cell and internet network technologies. A military example of such technology, the US Army M93-Hornet Wide Area Munition (WAM) depicted in Figure 1 [1] is a state-of-the-art example of portable remote sensor and control technology.

This munition/anti-tank mine is employed as an area defense weapon by the US Army. The M93's sensors detect the approach of potential vehicle targets, rotates the warhead to intercept these threats and then fires a top-attack projectile at the target. Many M93's are placed together in gauntlets to deny high-speed routes to enemy movement[1]. Since they employ sensors, they are able to cover a wide area of land unlike simple impulse-initiated land mines. Their simple autonomy allows US Army units to employ them to deny and deter enemy advances without needing to remain at the location. This force-multiplies the available Army manpower to defend many locations at the same time. It is this paper's argument that the same sort of capability can be projected by terrorist/guerrilla forces using networked teleoperated remote weapons. The following examples will discuss inexpensive technologies that provide this functionality to such forces.

2. Example 1: Area-Effect Light Remote Weapon

Suppose an army enters a region to achieve a specific objective and that elements in this region oppose this entry. Consider that this region has access to internet/cell networks, schools/universities of technology, access to commercially available video/IR cameras, computers, basic microcontrollers, electric motor and gear sets. Recognizing open high-intensity conflict is not winnable, technically competent combatants will resort to force-multiplied guerrilla tactics to harry and encumber the army. Though less reliable

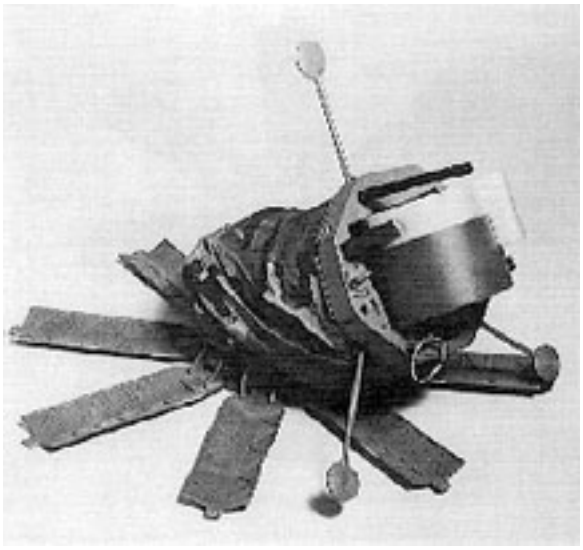

Figure 1: *M93 Hornet Wide Area Munition (WAM); MASS: 15.876kg; TARGET DETECTION RADIUS: 100 meters*

and certainly more primitive than the M93, simple remote-controlled weapons using commercially available sensor and control technology are well within the capability of most nations. Consider a design composed of a basic hand-held weapon cradle permitting weapon rotation and depression, a tripod for stability barrel elevation and azimuth motors, and a trigger solenoid. The motors are controlled by PWM commands from a microcontroller resident on the weapon cradle and powered by a 12 V DC automotive battery. With a land line for command and control, the system would be immune to RF interference and invisible to simple RF sensing. Historically, a remote control weapon of this type would require the operator to remain within visual range of the field of fire. However, current consumer technologies permit inexpensive remote feedback for the system. Combining consumer grade video cameras (many sensitive in the IR) , off-the-shelf image compression/transmission hardware (e.g. NTSC, MPEG2, or simple JPEG) and either cellular or wireless networking hardware, the operator has the means to remotely observe and adjust the elevation and azimuth of the weapon using the transmitted image stream as a guide. Elevation, azimuth, and shoot control could be easily implemented through either keystrokes, joystick motion, or, in slightly more complex systems, mouse click/drag on the displayed image. Further, modest automation could achieve programmatic fire or simple target tracking. Though the camera could be located with the weapon to improve the operator's control and accuracy, it could also be installed away from the weapon to provide greater survivability. Further, multiple cameras could be linked to view the effects and the ambush zone from different angles. Though a number of inexpensive video capture platforms are available (digital video, analog video, and 'webcam'), the discriminating technology of these systems are communication methods. Consumer technology centres around four possible vehicles: digital wireless LAN such as 2.4/5Ghz 802.11a/b/g (data rate: 11-54 Mbps, range: < 50m, boosted up to 16km), 2.4Ghz

analog broadcast to a remote receiver (data rate: 30 fps, range: < 200m), digital cell modem (data rate: 28Kbps, range: < 1000m) internet land line network (data rate: 28Kbps to 1GB/s range: unlimited). Of course, hybrids of the above are likely. Should any of the first three systems receivers be internet connected, the ultimate range becomes unlimited. In the range of general TV, GSM, and 2.4-5Ghz unregulated consumer bands, most wireless methods would be detectable but would not raise suspicion in an urban environment. With a short window of opportunity to respond, ambushed forces could receive fire from various remote weapon locations. Since the attackers are remotely positioned they run a low risk of detection, let alone injury during engagement. Naturally this has implications for the mindset of the attackers; combat will continue until the defenders destruction, retreat, or ammunition exhaustion. The attacker is under no pressure to cease fire or withdraw. Perhaps the most significant feature of this system is the cost (an estimated cost of this remote weapon platform is summarised in Table 1). Equivalent, locally available commercial-off-the-shelf technology, might be still less expensive or obtainable through illicit means. A basic area-effect light remote weapon system might cost less than $US2000 not including an additional $US500 for a computer to program the microcontrollers. An ambush of three weapons would cost no more than $US6500.

3. Example 2: Direct-Fire Heavy Remote Weapon

The remote systems envisaged in example 1 could be expanded to involve heavy weapons such as a heavy machine gun or a rocket launcher (e.g. the RPG-7). This remote weapon would be capable of destroying soft-skinned vehicles or obtaining a mobility kill on armoured vehicles which, in the context of an ambush, would leave the crew at the mercy of the local opponents. The key difference between this and the previous example are the mounting requirements and weapon controllability. A rocket launcher requires a more stable base and a robust weapon cradle to remain on target during motor ignition. Without resorting to more elaborate servo and servo-gear combinations to permit the same control as in example 1, consider that a static, large inertia mount might be just as effective for the given ambush scenario. Like many 4th-generation direct-fire anti-tank land mines, the improvised remote rocket launcher could be simply fixed in a frame with sufficient mass to absorb the initial impulse with minimal motion (e.g. The RPG-7 in a concrete block depicted in Figure 2). Again, the weapon would be controlled by a microcontroller and powered by a 12 V DC automotive battery, needing only a solenoid to depress the trigger. Remote observation and communication equipment would be identical to example 1. The local opponents could line up the direct-fire weapon either directly into the road or at right angles to traffic in an enfilade position producing defilading fire. The operators could use a co-located camera to view when a target vehicle drives into view. The co-located camera would allow them to aim and fire with a high probability to-hit from short distances. Given a co-located camera would be destroyed during the launch, the operator would lose the view of the target without additional cameras. With a point-blank range to target, like a roadside car bomb, it would not matter if the weapon

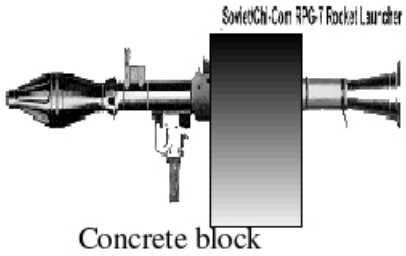

Figure 2: *Remote Weapon with Concrete Base*

Table 2: Direct-Fire Heavy Remote Weapon	Cost Esitmate
RPG-7	$2,000
TTL Logic Chips	$40
Electronics Board	$60
Power Transistors	$55
Solenoid	$50
MCU- PICmicro MCU by Microchip	$10
Wiring	$30
Keyboard	$25
Weapon Cradle	$25
Bullet Visual Camera	$120
Portable TV	$250
TOTAL	$2,665
Additonal Equipment	
500MHz 2 year-old Computer to program Microcontroller	$500

Table 1: *Weapon Cost Breakdown*

and sensor were destroyed since they would have served their purpose.

Figure 2 above is a simplified example of the direct-fire heavy remote weapon that might also be employed against ambushed vehicles. In Table 1 is the rough order of magnitude estimate for the RPG-7 rocket launcher. The price of this direct-fire heavy remote would cost on the order of $US3000 (US$2665) assuming that the RPG-7 cost around $US2000. In many 3rd World countries, an RPG-7 would be much less than this. An ambush based on a single direct-fire heavy remote weapon would destroy most soft-skinned vehicles if they hit the engine compartment. An armoured vehicle would experience typical damage encountered by any Light Anti-Armour Weapon (LAAW) or Heavy Anti-Armour Weapon (HAAW). A mobility kill on an armoured patrol vehicle is likely if many remote weapons are combined in a volley fire.

4. Example 3: Coordinated Ambush

Given the same suppositions as developed in examples 1 and 2, suppose that local opponents built an ambush system combining the weapons made of examples 1 and 2. By establishing network connections to multiple weapons, a coordinated multi-point ambush is possible with a minor investment in infrastructure. With final connection to the internet, the 'operations centre' can be substantially removed from the ambush site. While this would require slightly more expertise, the increasing use of web-enabled products greatly reduces the technical complexity once posed by networked control. In this example, the remote weapons would be pre-positioned as before but with a longer lead time so as to ensure a safe distance prior to operations. Using automotive batteries and low-power electronics, this could be anywhere from 10 minutes to several hours to reliably operate the equipment. Though internet connections could remove combatants completely from the combat region, being 1 km away from the ambush would be sufficient to drastically reduce their risk during the ambush. In this example, local opponents could employ the manual, teleoperated tactics, or a simple preprogrammed command sequence to fire volleys without direct operator control. The introduction of computers would also allow for some simple image processing/ machine vision by the local opponents that could provide rudimentary target tracking and/or suppressing fire by the remote weapons. The exact cost of this option would vary greatly with the age and complexity of the hardware, firmware, and software involved. However, it would be safe to say that it would be approximately an order of magnitude increase over the costs of the weapons from examples 1 and 2. With this increase in complexity, the success of this technique would significantly depend on local technical expertise.

5. Example 4: Large-Scale Static Defense

Assuming the above suppositions from examples 1 through 3, large scale strategic defense is conceivable. Consider that US$1million, including sufficient traditional weapons and ammunition, would produce hundreds of such remote weapon systems. For example, if 400 remote weapons (US$2500 per system) were deployed in fours, then 100 locations could be defended with static remote weapons. For a small force, this would provide improved defense of several small urban areas, or an extremely deep defense of a single city. Alternatively, these weapons might be deployed in 400 separate ambushes where the tactics would be identical to the terrorist/guerrilla scenarios described above. In any case, these weapons would permit a small group of soldiers to harry or damage forces with impunity. This demonstrates the relatively cost-effective nature of remote weapons as an alternative to armoured fighting vehicles. With the cost of a single tank or IFV in the order of $1 million US, remote weapons are both more flexible and more effective than a single land mine as an area effect weapon.

6. Discussion

With limited rounds of ammunition, these weapons are intended to inflict damage and casualties and not for protracted battles. A user would have to accept the loss of the equipment and the weapons. Therefore, this approach is not suitable for combatants of limited means. However, if large numbers of weapons are available and few willing combatants, this method could force-multiply their combat power. If the victim of such equipment is an armoured patrol then the damage potential is low. Conversely, if the victim is a convoy with soft-skinned vehicles like logistics trucks and fuel bowsers, the potential for damage and injury would be equivalent to an ambush by human combatants. Remote controlled directed fire, may offer a number of advantages over the less discriminate remote-controlled Car Bomb, Certainly, remote-controlled weapons would be more selective than a remote car bomb. Large improvised explosive devices are often detected at build time through the tracking of accrued exotic explosives or unusual quantities of chemical constituents. Similarly, explosive sensors/ detection dogs at routine checkpoints may uncover the weapons before deployment. In contrast, the remote weapons components from the examples above could be separated through transit and reassembled at the ambush site. Using mostly commercially available components, the movement of such items would raise little suspicion. Since these weapons would be static, there is no size or mass limit to their design.

As in all combat, the most important components in these remote weapon systems are the human operators. While one might assume that remote weapons would not be as accurate as manually fired weapons, this strategy poses a negligible risk for ambushing forces and, with careful design and training, could greatly increase their effectiveness. None of these systems necessarily needs to employ sophisticated software such as artificial intelligence or machine learning. With a little training, anyone could operate these proposed examples. If the operators are not harmed in the engagement, then they can be redeployed to other locations.

The cost-benefit for hostile opponents is that they can risk engagement of superior units with a limited if not negligible loss of life on their side. Unlike the car bomb that kills indiscriminately, these weapons are directed and can target individual vehicles and personnel. This means less chance of civilian casualties and therefore less local public condemnation of the attacks. If they have a ready supply of weapons, which are the largest costs of the examples above, then all they require is the skill and tools to craft simple improvised electronics to make them remote weapons. This is a realistic asymmetric threat where the local opponents have money to purchase technology and are equally unwilling to suffer casualties in direct conflict with more sophisticated armies. In the current doctrine of Western Armies, the counter to ambush is patrol operations by maneuver units. This means armoured vehicles in the open and dismounted infantry in close spaces must search through suspected areas of resistance, flush out enemies, suppress them, and kill them. Soldiers would be ordered into the areas that could potentially be manned by remote, even fully automated, weapons. Remote weapons would inflict casualties in ambushes on dismounted infantry. Remote

heavy weapons would destroy logistical vehicles and could immobilize armoured vehicles. Casualties always pose a political and strategic problem for theatre commanders, particularly where significant casualties are not acceptable (i.e. international peacemaking/peacekeeping operations). The identification and destruction of remote weapons will pose a number of problems to opposing forces.

Like mines, remote weapons are an area effect weapon, denying access or passage through a prescribed region. Like mines, the complexity of individual weapons can be increased with autonomous software, computing electronics, and additional sensors. They can act/react faster than human opponents. Unlike mines, remote weapons are discriminating and can effectively permit or deny traffic. Unlike mines, remote weapons are not necessarily destroyed during operation and, if conditions permit, can be maintained/replenished in the field. Unlike mines, remote weapons are flexible, operators can change tactics prior and during ambush. Unlike human combatants, remote weapons cannot/need not run from a fight. These features mean that segments of the locally-affected population and opposing forces alike will treat remotely guarded areas like mine fields. Further, attacking/ambushed forces will require heavy defensive armour to withstand attack and precise directed fire to destroy these remote sentinels. As more automation is incorporated into these systems, it is probable that remote weapons tactics will evolve to become a substantial threat to human combatants. Automatic target recognition and tracking could be added to these systems to make the remote weapons detect and engage manned vehicles and dismounted infantry before the friendly forces realize they are in danger. It is crucial to develop counters to these threats that avert personnel/material casualties so that operations in conflict zones meet the political and strategic environments of tomorrow's battlefield. Currently, there are no solutions that counter this specific threat.

There are several obvious solutions that could be used to counter these threats:

- Teleoperated Decoy Vehicles - remote-controlled that are sent out ahead of patrols, for example, to confuse the enemy into attacking the decoy. This would allow the patrol to observe the location and type of ambush weapons before being in the ambush zone;
- Electronic Counter Measures - means such as jamming communication or detecting signal sources in order to alert patrols to the potential threat;
- Autonomous Mobile Robotics - systems sent out ahead of patrols or around defensive installations that are capable of acting independently to sense, identify and at some point engage threats; or
- Advanced Sensor Systems - surveillance sensors manned by human crews capable of detecting threats well in advance of manoeuvre units in order to reduce the probability of moving into ambush kill zones unaware.

Clearly, for friendly forces the employment of static remote weapons to defend friendly installations would force-multiply the local defenders and this would be a cost-effective

alternative to manning the bases with more personnel. Given the countermeasures above, these systems would pose a considerable obstacle to less sophisticated enemy forces.

7. Conclusions

There are six characteristics of static remote weapons systems that make these threats important:

1. Ubiquity- The technologies needed to automate weapons have been around for a long time, but the cost of this automation and the extended way in which cellular and internet networks can separate the attackers from the ambush weapons has never been so readily available, seamless, and cost-effective. These weapons depend on readily available hand weapons and there is no shortage of these parts.
2. Invisibility- The subcomponents of these remote weapons systems can be as simple as commercial- grade technology that will not stand out in check point searches in a conflict zone or overseas customs inspections. These weapons can be slipped through security without detection and then be reassembled at the ambush site.
3. Specificity- The aimed remote weapon increases the discrimination that can be used to target soldiers in a crowd or on the road. This allows groups to cause less local resentment by decreasing collateral damage. This improves on the basic car bomb that requires precise timing to hit the right vehicle or personnel.
4. Range of Lethality- These weapon systems do not need to be conventional weapons. The same technology could be used for nuclear, biological, chemical, electromagnetic, or internet denial of service weapons that span the continuum of conflict intensity.
5. Negligible Risk- These systems would allow groups to confront superior armies without personal risk. Determining who conducted the operation would take exhaustive investigation and reconstruction which means that these opponents may be able to slip out of the danger area undetected.
6. Psychology- Like minefields, the immunity to danger makes these remote weapon systems a psychological threat to friendly soldiers and civilians alike. Remote weapons will not be deterred by shelling or distractions and the operators, knowing they risk nothing personally, can await unsuspecting friendly troops until the last possible moment which increases their effectiveness and the shock factor of the attack.

The use of static remote weapons for defense by enemy troops should be considered as a threat for friendly forces in future conflicts in all intensity level conflicts. A complementary research activity, focusing on the use of static remote weapons would be a useful addition to the research of autonomous robotics since the static

remote/autonomous weapon is a less complex subset of the mobile robotics problem. It is important to study the impact and tactics of remote weapons to reveal the solutions that can counter them. Also, some consideration should be given to researching sensors systems, teleoperated vehicles, and electronic countermeasures that can detect and destroy static remote weapon systems prior to ambush.

References

1. DOD, US Department of the Army (2002), Vol. Field Manual 20-32, Ch. Mine/Countermine Operations. Washington D.C.: Department of the Army.

Annex A
Acronyms

AO Area of Operations

AOR Area of Responsibility

ANSI American National Standards Institute

BIT Built-In Test

C/A Course Acquisition GPS

C4ISR Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

CPU Central Processing Unit

DM Domain Model

DMU Dynamic Measurement Unit

DGPS Differential GPS

ECEF Earth-Centred, Earth-Fixed

FOG Fibre Optic Gyroscope

GPS Global Positioning System

HAAW Heavy Anti-Armour Weapon

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IMU Inertial Measurement Unit

ISO International Standards Organization

JAUS Joint Architecture for Unmanned Systems

JTA Joint Technical Architecture

LAAW Light Anti-Armour Weapon

LAN Local Area Network

MGRS Military Grid Reference System

MMU Memory Management Unit

MSL Mean Sea Level

NBC Nuclear, Biological, Chemical

NIST National Institute of Standards and Technology

NSU Navigational Sensor Unit

NTP Network Time Protocol

OCU Operator Control Unit

OEM Original Equipment Manufacturer

OPI Office of Primary Interest

PID Proportional Integral Differential

POST Power-On Self Test

RA Reference Architecture

RGA Rate Gyro Accelerometer

RMS Root Mean Square

RPG Rocket Propelled Grenade

RPY Roll, Pitch, Yaw

RTK Real Time Kinematic

SAE Society of Automotive Engineers

SI System International

SMA Senior Military Advisor

TNA Thermal Neutron Activation

UAV Unmanned Aerial Vehicle

UGV Unmanned Ground Vehicle

US United States

USA United States of America

USV Unmanned Space Vehicle

UTC Universal Time Coordinated

UTM Universal Trans Mercator

UUV Unmanned Underwater Vehicle

UxV Unmanned (Aerial, Ground, Underwater, Space) Vehicle

WG Working Group

WGS World Geodetic System

Annex B
Distribution List

Internal Distribution

DRDC-Ottawa

DRDC-Valcartier

DRDC-Suffield/AISSSection

Library - 1 electronic copy, 1 hard copy

DRDKIM - 1 electronic copy

External Distribution

NDHQ-J2

NDHQ-DLR

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada - Suffield
PO Box 4000, Medicine Hat, AB, Canada T1A 8K6

2. SECURITY CLASSIFICATION (overall security classification of the document including special warning terms if applicable).

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C,R or U) in parentheses after the title).

The Static Remote Weapon Problem

4. AUTHORS (Last name, first name, middle initial. If military, show rank, e.g. Doe, Maj. John E.)

Monckton, D. Erickson, S.

5. DATE OF PUBLICATION (month and year of publication of document)

October 2005

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc).

24

6b. NO. OF REFS (total cited in document)

1

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered).

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include address).

Defence R&D Canada - Suffield
PO Box 4000, Medicine Hat, AB, Canada T1A 8K6

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Specify whether project or grant).

12ph01

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written).

n/a

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique.)

DRDC Suffield TM 2005-084

10b. OTHER DOCUMENT NOs. (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution beyond the audience specified in (11) is possible, a wider announcement audience may be selected).

Unlimited

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This paper describes the use of static remote-controlled weapons as an ambush tool that allows guerrilla/terrorist forces to more accurately inflict casualties and damage with less personal risk than a car bomb. This is possible due to the inexpensive and ubiquitous technology that exists in today's society worldwide. This paper provides a different perspective about what will appear on the battlefield in asymmetrical threat environments and why.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title).

static remote control weapons ambush terrorist guerilla autonomous mobile robotics sensors