small arms survey

Issue Brief

Number 11 ■ February 2015

MANPADS Proliferation Reduction by Design

On Countermeasures and Kill Switches

Introduction

In the 1980s the United States delivered several hundred missiles for Stinger Man-Portable Air Defence Systems (MANPADS) to Afghan resistance groups, some members of which later formed the Taliban. After Moscow's withdrawal from Afghanistan in 1989, the US government launched a buy-back programme aimed at recovering the missiles. Despite offering rewards of USD 100,000 or more for each missile, only a few dozen were recovered (Fitchett, 2001).

Since then, thousands of MANPADS worldwide have been lost, stolen, or diverted from government arsenals. In 2011, anti-government forces looted the Libyan government's massive stocks of MANPADS. The US State Department official Andrew Shapiro noted that 'Libya had accumulated the largest stockpile of MANPADS of any non-MANPADS-producing country in the world' (Shapiro, 2012, p. 7). Securing these and other weapons in Libya has been costly, as illustrated by US contributions to multilateral threat-mitigation programmes concerning conventional weapons. In 2011, the then Secretary of State Hillary Clinton committed over USD 40 million to these programmes (US AFRICOM, 2011). More recently, armed groups in Syria and Ukraine have acquired dozens of MANPADS, including recent systems (Schroeder, 2014; Binnie, 2014).

With mounting public opposition to human rights violations in Syria and other conflict zones, there is increasing pressure on governments to provide advanced weapons systems to armed

MANPADS are lightweight, surface-to-air missile systems designed to be operated by a single individual or a small crew. The incorporation of technical-use controls could offer some protection against their unauthorized use. © Roger-Viollet/DoD/AFP

resistance groups. Rather than putting troops in harm's way, certain US politicians suggest that the United States should provide allies with the means to defend themselves (Londoño and Miller, 2013). In the long term, however, the provision of MANPADS to non-state actors can be dangerous: after the hostilities end, there is at present little to prevent armed groups and criminals from using these weapons to threaten other governments as well as civilians. As illustrated by events in Afghanistan and Libya, it can be exceedingly difficult to prevent the theft, loss, and illicit retransfer of weapons abroad, including to militants.

Some analysts have called for the development of devices to minimize the risk of non-state actors' unauthorized use of MANPADS. Such devices are often referred to as 'technical-use controls'—technologies that prevent anyone other than those with the legitimate authority from using a weapon. The development and universal deployment of such devices could eventually shut down the black market for MANPADS (Cordesman, 2012).

Members of the Wassenaar Arrangement (WA) and other multilateral forums have already agreed to incorporate 'launch control features' into new MANPADS as these become available. A provision of the Wassenaar Arrangement's policy on MANPADS that is seldom discussed calls on member states to *'implement technical performance and/or launch control features*[1] *for newly designed MANPADS as such technologies become available to them'*. Those responsible for drafting the Arrangement were careful to note that the controls should not compromise the weapon's effectiveness: *'Such features should not adversely affect the operational effectiveness of MANPADS for the legal user'* (WA, 2007, para. 3.4). The Group of Eight (G8) and the Organization for Security and Co-operation in Europe (OSCE) adopted similar language (G8, 2003; OSCE, 2008).[2]

Despite these efforts, it appears that no MANPADS as yet incorporate secure technical-use controls.[3] The apparent lack of progress in developing and installing such controls could be because they are perceived to be not technically feasible. It remains unclear whether MANPADS can be designed or modified to reduce the possibility of diversion to parties other than the intended recipients without impeding operational effectiveness, or to incorporate a 'kill switch' that prevents unauthorized use.

This Issue Brief addresses these questions by examining several use-control technologies and the administrative, engineering, logistical, and strategic issues associated with installing and using them in MANPADS. While much of the discussion is based on an analysis of the US FIM-92 Stinger system, it is assumed that the key issues that apply to Stingers are applicable to most other systems, including where to install the use-control, how it would work, and the operational impact.

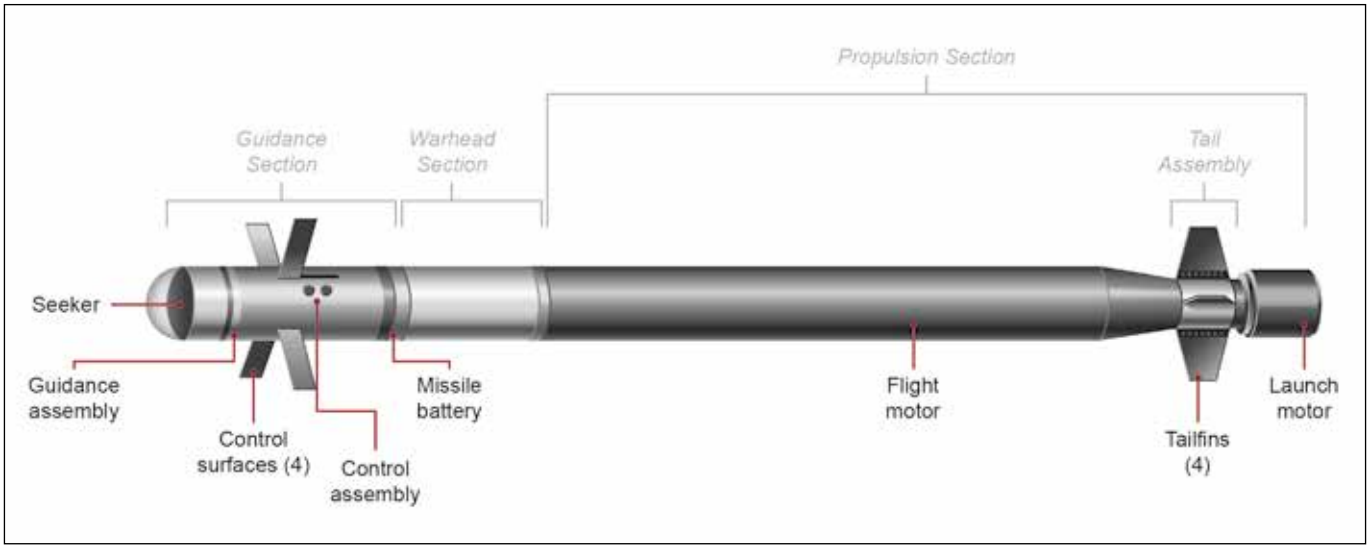
This examination reveals several options for incorporating technical-use controls into current and future MANPADS designs. As the Issue Brief explains, however, developing controls that address the threat to civilian aircraft posed by MANPADS without reducing their viability as air-defence weapons is a complex undertaking, and the administrative, bureaucratic, logistical, and technological barriers to accomplishing this goal are likely to be significant.

Terms and definitions

As defined by the Wassenaar Arrangement, MANPADS are

> *surface-to-air missile systems designed to be man-portable and carried and fired by a single individual; and other*

Figure 1 **Typical components of a MANPADS missile**



surface-to-air missile systems designed to be operated and fired by more than one individual acting as a crew and portable by several individuals.
(WA, 2007, para. 1.1)

While this definition encompasses both man- and crew-portable systems, the vast majority of MANPADS worldwide are shoulder-fired systems, which are the primary focus of this study. A technical-use control (or 'use-control') is defined here as any device designed to prevent or limit a missile launch based on time, location, or the absence of an authorizing device or code.[4]

Man-portable air defence systems: a brief technical overview

Although there are several different MANPADS models, most have certain common elements. Each MANPADS features a missile, the same models of which are often fired from other platforms, including helicopters and ground vehicles. The missile is loaded in a specially designed launch tube, which provides for safe ejection and launch, along with an integrated control with the launching device, often referred to as a gripstock. Each system has a replaceable power supply (a thermal battery or battery-coolant unit (BCU)) and some MANPADS can be equipped with auxiliary features, such as an identification friend or foe (IFF) interrogator antenna or night-vision equipment.

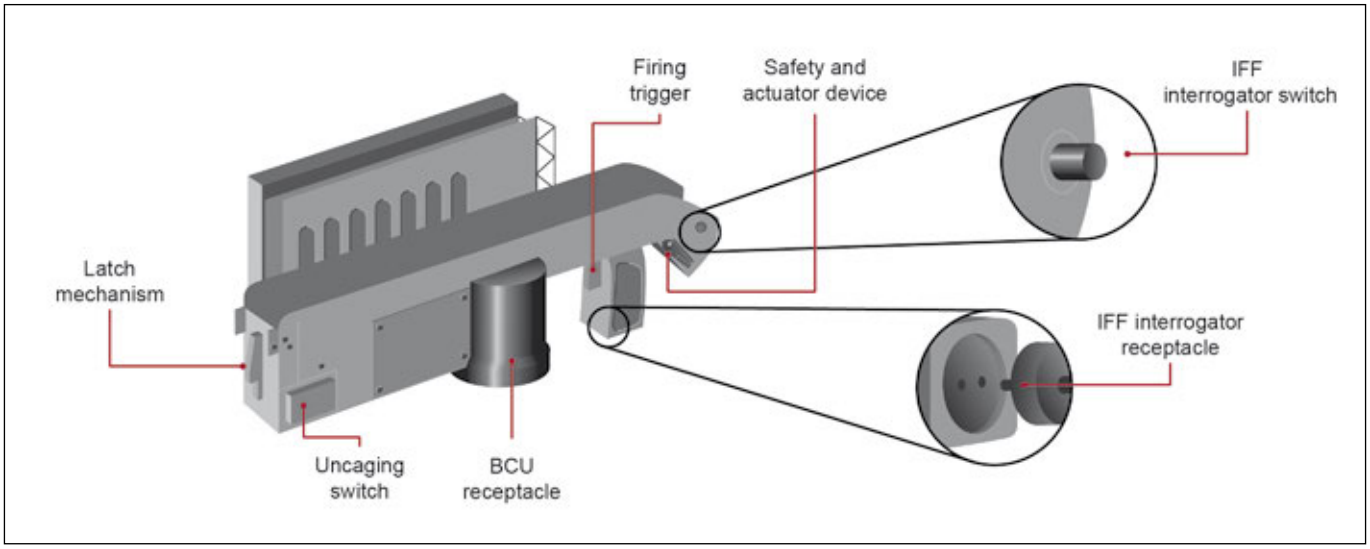
Newer versions of the Stinger MANPADS are equipped with a remotely programmable microprocessor (RMP) that facilitates upgrades and missile modifications. Designers can add new threat profiles, and make other changes to improve performance, without an expensive and costly retrofit (US Army, n.d.; US Marine Corps, 2011; US Marine Corps, n.d.)

The missile round

Most shoulder-fired missiles are 1.5 to 1.8 metres in length and weigh about 15–18 kg. Missiles are often categorized by the type of seeker and guidance system used. These include infrared (or 'heat-seeking') guidance, semi-autonomous command line-of-sight missiles, and laser beam riders. MANPADS are also categorized by generation (i.e. first, second, third or fourth), which reflects when the system was fielded and its technology level (Schroeder, 2013, pp. 5–6; Bolkcom and Feickert, 2004, pp. 1–3; US Army, 2000).

Over time MANPADS have become more deadly and more difficult to evade. The earliest MANPADS, including the Russian SA-7 and the US Redeye, had only the most basic infrared sensors, which lacked the sensitivity of today's seekers. They could be led off course by other heat sources, even the sun (Global Security, n.d.; Schroeder, 2011). Generation Two systems, such as the Soviet SA-14 and early versions of the US Stinger, have nitrogen or argon-cooled detectors that improve the sensitivity of the seekers, making them more reliable and accurate (Bolkom and Feikert, 2004, p. 2). Generation Three systems include Stinger RMP Block 1, the French Mistral and the Russian SA-18, and feature multiple detector elements along with scanning techniques that provide a quasi-image capability and are consequently better at discriminating flares and countermeasures from target aircraft. Generation Four MANPADS will feature a complete infrared imaging capability that increases the range of the missile (Bolkcom and Feickert, 2004, pp. 1–2; IHS Jane's, 2000, p. 3).

Figure 2 **The gripstock assembly, which is attached to the launch tube via the latch mechanism**



The gripstock

The gripstock is the reuseable mechanism designed to initiate the launch of a MANPADS missile. It is attached to and removed from the launch tube by means of a latch. The Stinger gripstock assembly includes a safety switch and an actuator device, which uncages (unlocks, i.e. allows to freely rotate) the gyroscopic mechanism. This action initiates tracking by allowing the seeker to point towards the target, and free rotation of the gyroscopic mechanism allows the missile to correct its trajectory during and after launch. The gripstock also includes a firing trigger, an IFF interrogator switch, an IFF connector,[5] and a BCU receptacle. After the missile is fired, the gripstock can be detached from the empty tube and reused (US Army, 2000).

Major component: thermal batteries or battery-coolant unit

MANPADS are designed to remain in storage for many years. To accommodate this, a special battery is optimized for high power and long storage periods: the thermal battery, sometimes called a liquid or molten-sodium battery (Parthasarathy, 2004). Batteries for later-generation systems also contain coolant for the missile seeker. The seekers of some heat-seeking missiles must be cooled to almost cryogenic temperatures in order to operate properly. These batteries are thus often referred to as battery cooler units, or BCUs (US Army, 1981; Kögler, 2013, p. 29).

To activate the battery, a percussion primer is struck, igniting the mixtures of iron powder and potassium perchlorate pyrotechnics. The heat melts the electrolytes, which activates the electric potential. When the devices are in storage, they can remain ready-to-use for decades, providing full power the instant the primer is struck. The disadvantage of thermal batteries is that they provide a high burst of power for only a short period. The BCU provides only 30–90 seconds of power for pre-flight operations, depending on the type of MANPADS (Kögler, 2013, p. 29). The Stinger battery is limited to 45 seconds of power (US Marine Corps, 2011, paras. 2–6).

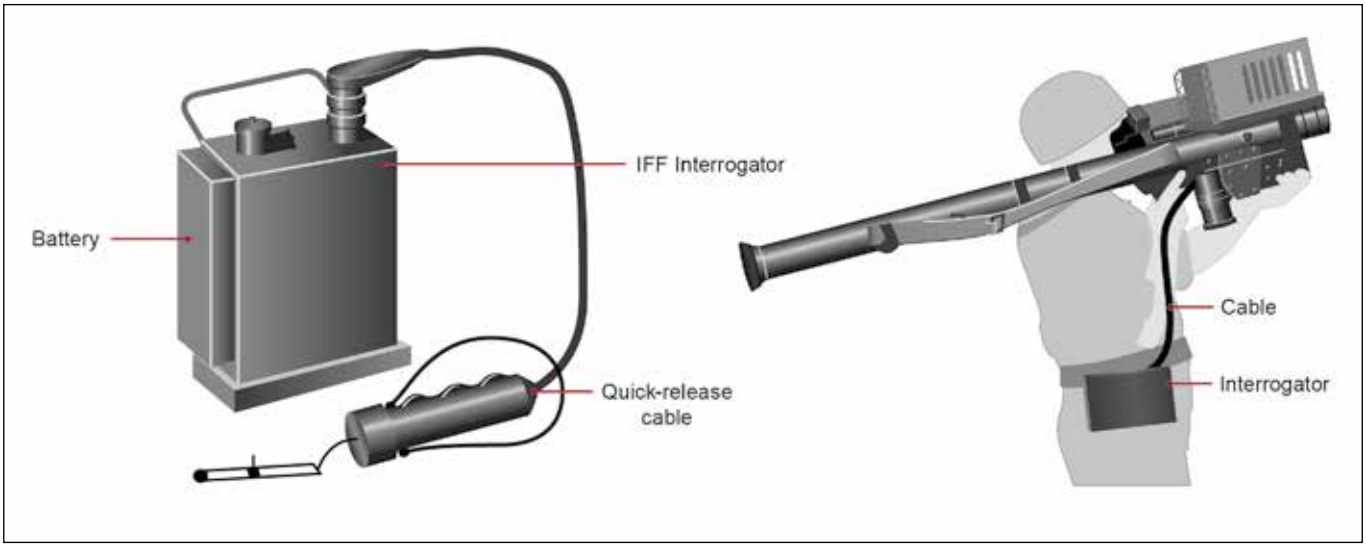
Accessories: identification friend or foe interrogator

The IFF interrogator is a battery-powered unit that is worn on the belt of the MANPADS operator. The device is connected to the gripstock by a quick-release, plug-in cable. The IFF unit is used to interrogate the transponder of military and civil aircraft and to listen for either Mode III (unclassified) or Mode IV (classified) replies.

The complete IFF system consists of two separate components: the interrogator and the programmer. The programmer is a separate piece of equipment that is not carried with the interrogator but tends to be kept at a 'special facility', that is, a place with access to 115 or 220 volt electrical power—typically a unit headquarters (HQ). The interrogator can make about 800 interrogations before it has to be returned to the HQ to recharge the batteries and reload new secure interrogation codes, called combat identification (CID) codes (US Army, 1981, chs. 2–3). The interrogation codes are valid only for a period of a few days. Operational forces use the IFF interrogation CID codes to distinguish between friendly military and civilian aircraft from hostile forces. The codes are classified and periodically changed.

As currently configured, the IFF does not prevent the firing of a MANPADS missile; it emits a tone only when a friendly aircraft is identified.

Figure 3 **The identification friend or foe (IFF) interrogator module**



The operator can choose to ignore this warning and continue with the missile launch (US Army, 2000; US Marine Corps, 2011, chs. 2–5).

Missile operation

To understand the various options for installing technical-use controls on MANPADS, it is necessary to understand how a MANPADS operates. This section provides an overview of the launch process, using the FIM-92 Stinger MANPADS as an example. The basic operation of other types of MANPADS is similar.

A MANPADS is designed for defending fixed points (e.g. military facilities, infrastructure, and airfields) and mobile teams against attacking aircraft. The MANPADS therefore has to be ready to fire in a few seconds. Upon activation, the missile must be fired within 30–90 seconds or the battery is depleted and must be replaced. Stinger missile operators are trained to activate, track, and fire the missile in 10 seconds. Consequently, a MANPADS equipped with a technical-use control must be ready for launching quickly, either by the rapid acquisition of launch authority or by operating in a standby mode (having been activated at some earlier time).

Before launching the missile, the operator centres the target in the sight-range ring, which folds out from the missile tube. There is no electronic sight, although there is an attachment for an optional night-vision device. The operator then determines what type of aircraft is being targeted by pressing the IFF interrogator switch and listening for a response. The IFF interrogator simply assists in identifying the aircraft and does not prevent the missile from being fired (Army, 2000; US Marine Corps, 2011, paras. 2–5).

When the target is within range, the operator initiates the firing sequence. When the seeker identifies the target, it emits a distinct tone. The operator then presses and holds the uncaging switch, which allows the seeker to track the target. If the seeker has locked onto the target and there is still a distinct tone, indicating tracking, the operator squeezes and holds the firing trigger and continues to track the target for three to five seconds, after which the missile's launch motor ignites, propelling it from the launch tube (US Army, 2000). At a safe distance, the flight motor ignites and the missile then guides itself to the target.

Implementing technical-use controls

It may in the future be possible to prevent the unauthorized use of MANPADS by incorporating technical-use controls into new units. Such controls would require the operator to enter special codes, use keys, or otherwise ensure that the she or he is authorized to use the missile before it becomes operational. Producers of future air-defence systems could be required to include such modifications to reduce the possibility of unauthorized use. Anthony Cordesman of the Center for Strategic and International Studies (CSIS) suggests that

> *[A] small chip can be inserted into these weapons that could continuously read their location once activated. If such a chip was tied to a device that disabled the weapon if it moved to the wrong area, it would greatly reduce the risk of its falling into the wrong hands.* (Cordesman, 2012, p. 2)

He goes on to claim: 'Encryption chips can be equally small and cheap and could perform a number of additional functions. They could have a time clock to disable the weapon at a given time, with the option of extending the life if a suitable code was entered' (Cordesman, 2012, p. 2).

The development of technical-use controls for MANPADS may indeed be feasible and would reduce the likelihood of use by unauthorized persons. The usefulness of such devices would be determined by several factors, including their cost, effectiveness, and impact on legitimate use.

There are several possible approaches to introducing technical-use controls in MANPADS, including:

- modifying the characteristics of the missile power system;
- using a Global Positioning System (GPS) geographic lock-out mechanism; or
- using some type of key or code entry. The key could be physical (operating a mechanical switch), manual (such as a keypad), or electronic (using an external device or radio frequency dongle).

In each case, the key or code would enable or activate the missile for a limited period of time. After the set period, the missile system would become inoperable and would need to be returned to a secure maintenance facility, or enabled through the use of special equipment to reset the authorization codes.

The difficulty of applying technical-use controls to MANPADS extends beyond modifying the weapon. Operators would also need the logistical infrastructure and equipment required to ensure that the missile could be activated in ways that minimize the risk of unauthorized access to keys and key codes, and to change the authorization codes as they expire or the MANPADS is moved to other regions.

Another significant challenge is to prevent the removal or circumvention of the control. As noted by Aram Nerguizian of the Center for Strategic & International Sudies, 'people who

get their hands on such weapons could quickly find a way to disable or spoof tracking chips and kill switches' (Reed, 2012). Thus, effective technical-use controls would require anti-tamper components that are sufficiently robust to thwart attempts to remove or circumvent the controls.

Design consideration for technical-use controls

This section examines several possible design changes or system modifications aimed at preventing the unauthorized use of MANPADS, and the potential operational impact of such changes. The section begins with a brief description of Permissive Action Links (PALs)—the closest existing analogue to the technical-use controls assessed in this Issue Brief—and an overview of tamper-proofing, that is, ensuring that components cannot be removed or replaced without compromising the entire missile system. It then considers the logistical requirements for deploying use-controls and concludes with an assessment of GPS-based technologies as use-controls.

Permissive Action Links and tamper-proofing technical-use controls

Given advances in the miniaturization of integrated circuits and experience with nuclear weapons and other types of sensitive equipment, developing the components of a technical-use control should not pose an insurmountable technical challenge. Some of the challenges are similar to those confronting designers of similar devices for nuclear weapons, which, to the best of our knowledge, have never been detonated by unauthorized users.[6] It may be possible to adapt some of these techniques and technologies for use with conventional weapons.

There are several possible approaches to making a device physically tamper-resistant. Common techniques could include:

- packaging that requires special tools to disassemble;
- hardening the electronic enclosure using high-temperature resins;
- ensuring certain components crumble or break apart if they are incorrectly disassembled;
- erasing critical software in the event of inappropriate access.

For tamper-proofing to be reliable, additional features are required to prevent critical firing components from being bypassed or simply replaced. These techniques, as highlighted by Cordesman (2012), suggest the use of an encrypted data stream between the user inputs, or between the launch-activation device and the firing mechanisms. Some of the techniques are commonly used to secure nuclear weapons and might also be viable for MANPADS.

The nuclear counterpart of MANPADS technical-use controls is called a Permissive Action Link (PAL), a term dating back to the early days of nuclear weapons security. It is a device incorporated into a weapon system that is intended to prevent unauthorized firing. Potential unauthorized users range from arms traffickers who have stolen or diverted the weapons to rogue military officers entrusted with them (Bellovin, 2009).

The US Defense Department defines a PAL as:

> *A device included in or attached to a nuclear weapon system to preclude arming and/or launching until the insertion of a prescribed discrete code or combination. It may include equipment and cabling external to the weapon or weapon system to activate components within the weapon or weapon system.* (US DOD, 2001, p. 408)

At the simplest level a PAL comprises two (physically) tamper-proof black boxes. The first, which is buried in the weapon system, decrypts a digital data stream from the second box, which contains complex, encrypted information needed to operate the weapon. The second box also contains the means to receive an activation signal (key), which allows the encrypted information to be transferred to the first box. A key, a code, a time signal, or some other action, is required to pass the critical data to the electronics buried in the weapon. Either box by itself would be useless.

Logistical infrastructure requirement (the authorization chain)

The word 'link' in Permissive Action Link depends on seeking permission from an external source in order to operate the weapon. Creating the link to allow action would require one or more additional logistical steps, regardless of the technique used. These steps include:

- maintenance of a crypto key infrastructure;
- periodic removal of the system to a 'special facility' or maintenance depot for the replacement of time-sensitive components;
- the development of equipment—or the modification of existing equipment—to reset the activation codes;
- the creation and maintenance of some type of communication link to verify that the user is authorized to use the weapon.

The physical act of enabling a MANPADS equipped with a PAL-like technical-use control would not be particularly difficult or complex for the

operator. In theory, the operator would need only to flip open an access panel, insert a key or enter an access code, and the missile would remain active for the period and in the locations permitted by the relevant authority. Conversely, the logistics of putting the infrastructure in place to permit this action is likely to be significant.

The objective of a nuclear PAL is simply to prevent unauthorized firing. For a conventional weapon, a more nuanced approach would be required. Weapons designers and policy-makers would have to answer several potentially difficult questions regarding the length of the authorization period and the system's response to the entry of an incorrect key or authorization code. Such questions would include how long the authorization should last—a week, a month, or a year, for instance—and what the consequences would be of inserting an incorrect key or activation code. For example, the missile could be programmed to blow up in situ if incorrect authorization codes were repeatedly entered or if the operator attempted to bypass or disable anti-tampering devices. If the weapon is not used, preserving the missile and thereby reducing the cost of an error made by authorized operators might potentially give unauthorized users another chance to bypass the security system. Finally, there is the question of whether the system should launch the missile as an unguided munition, risking collateral damage.

Moreover, creating a weapon system that can be used only within a certain period of time or in a specified location might be of concern to legitimate users, particularly governments that import such systems. The issue of international transfers raises difficult questions, including whether the launch-authorizing equipment (i.e. the equipment required to change or extend the operational period or location) would be delivered as part of the weapon system. In short, the policy and doctrine of the authorization chain of technical-use controls would be a critical part of the overall system, and essential to its design. Indeed, this aspect might be more important and difficult to overcome than the technological and logistical challenges. Future research on use-controls should include a full exploration of these challenges.

Global positioning system (GPS) for technical-use control activation

The activation device does not have to be a physical key or keypad entry system. It could just as easily be a separate device that communicates with the weapon via a plug or radio frequency. Such devices are commonly used for computer access to software or networks. They are generally preprogrammed but could be configured to receive an activation code or signal from another data source, such as an overhead satellite or a cell-phone tower. The CSIS has suggested employing a use-control that limits the areas in which a MANPADS can be operated —a GPS-based 'kill switch' (Reed, 2012). The use of such devices would be tricky; under some conditions, GPS-based use-controls[7] could delay launch by as much as 15 minutes (if the GPS device is in a completely uninitialized state). This is the 'time to first fix' (TFF) listed in the manufacturer's specifications (US DOS, 1996, ch. 3.5), although there may be ways around this constraint, as explained below.

While the GPS position determination, or 'fix', is theoretically based on triangulation—using distance measurements to any three of a constellation of satellites—the calculation used by the device is more complicated, and uses a number of mathematical shortcuts. The fix determination requires the loading of a complete catalogue of time-variable system information into the GPS receiver before the fix can be calculated. The position and orbital path of all satellites must be known, along with all the associated individual satellite identification information. This information is repeatedly downloaded or updated to the receiver about every 15 minutes. The position, orbital path, and identification information is called the 'almanac' (US DOS, 1996, ch. 3.5).

When the GPS device is first powered up, it has no global satellite system information. All GPS equipment requires a certain amount of time to 'warm up' by downloading enough information to make the fix calculation. The first fix calculation is called the guaranteed TFF. Depending on the length of time a GPS device has been operating, the TFF can take 15 minutes,[8] 20 seconds, or a millisecond to determine its location. The TFF has three start-up modes:

- **COLD/Factory.** The device has no satellite information. The almanac and all other data must be downloaded before a fix can be computed. Manufacturers usually estimate the download time to be about 15 minutes.
- **WARM/Normal.** If the device is operated every day, the time is known to within 20 seconds, the position is known to within 100 km, and the almanac is loaded, and the device only has to refresh the ephemeris data, which is repeated every 30 seconds. Thus, 30 seconds is the minimum TFF in these conditions.
- **HOT/Standby.** This is the normal operation after the first fix has been determined. Also called 'time to subsequent fix' (TSF), it is almost instantaneous and occurs when the device is operational and con-

tinuously updating (US DOS, 1996, ch. 3.5.1).

The expected scenario for MANPADS 'fresh out of the case' would be cold/factory, so the technical-use controls would require a minimum of 15 minutes to determine the missile's location. Since the thermal battery provides power for less than a minute, a 15-minute delay in readying the missile for launch would be severely limiting.

Delays of more than a few seconds would presumably be too long when a hostile aircraft is approaching the MANPADS operator. Thus, for a GPS-based technical-use control to work, the GPS module would have to be in at least standby mode to activate the missile sufficiently quickly to engage a target. The GPS-based use-controls could be moved to a normal or standby mode if the GPS was turned on some time before it was to be used. Even if authorized military operators were to consider a 30-second delay acceptable (which is unlikely), the device would have to be turned on every few days to keep the GPS active. Consequently, the MANPADS would require some type of low-current power source to keep the GPS in standby mode. Adding a small battery could pose some logistical issues and also reduce reliability. Additional maintenance and inspection would be required to ensure the batteries were fully charged. Furthermore, requiring the system to be electrically active several minutes before use would entail significant modifications to the MANPADS electrical system.

A workaround to an active GPS technical-use control could be relatively simple—such as using only the timestamp data from the GPS. The time signal is available in less than a millisecond. The fix could be performed periodically at a field maintenance facility. Activation could be based on location and could last for a short fixed period of time, but must be periodically renewed. This would mean resetting the activation codes every few days at a special 'in-theatre' facility.

Using GPS for a time reference would make it unnecessary to keep an active timer on the MANPADS system. Since the weapon is powered down in storage, a means to determine the exact time would be necessary as the power comes up from the thermal battery. The use-controls could determine the time within a millisecond, since all GPS satellites use the same time, and the almanac is not required. The use-control mechanism could compare the actual time to a stored 'valid until' time and , if still valid, send an activation signal to the missile. One serious limitation of this workaround is that the missile rounds—designed to require little or no maintenance—could be rendered less reliable by any modification. Nonetheless, it could still be a more practical alternative to employing an active GPS technical-use control.

Another possible approach is to use a cooperative signal intentionally transmitted by the satellite controllers. It might be feasible to reserve a 'special code' or inject a continuously updated signal, which could be interpreted as permission to launch, but only when the satellite is over an authorized area.[9]

Modification of MANPADS components for technical-use controls

The first design consideration would be where to locate the additional hardware, and what subsystems should be inhibited in the case of an authorization failure. For example, the additional equipment could be entirely internal to one or more of the three main components of the MANPADS: the BCU, the gripstock, or the missile round. Alternatively, devices installed in any of the three main components could be used in conjunction with devices installed in auxiliary equipment, such as the IFF interrogator.

As explained above, an effective PAL-like technical-use control would consist of three elements:

(i) An external code or key input device with encrypted operational data.
(ii) A wired or wireless link to pass data between the input device and the internal components.
(iii) Internal components that can decrypt the operational data and activate the missile system.

The external device would provide the encrypted information used to enable the missile, and would probably require its own power source along with a clock or another means of deactivating the weapon. The external device would require periodic rekeying and reauthorization at a special facility, or a field maintenance facility, and communication with those authorized to reset or update the use-control.

As noted above, the activation device or signal would be a digital key, a clock or timer, or a GPS location signal. The device would decrypt a digital message from the external device and load it into the system microprocessor.

Ideally, the message would be necessary in order to operate the missile, rather than relying on a binary launch-authorization code that could be bypassed. Possible options include data on the mapping of the control surfaces that could be fed to the guidance system, parameters for the guidance control gain signal, proximity-fusing algorithms, or any operational characteristic required for the missile to hit its target. Once installed, the internal

device should not require updating or key or code resets because it would simply decrypt the data from the activation signal.

Thanks to the micro miniaturization of contemporary electronics, most integrated circuits and surface-mount components can also be sealed in high-temperature epoxy, which makes the individual components effectively (physically) inaccessible. The next section discusses which of the launch actions can be altered to prevent unauthorized use.

Technical-use controls embedded in the missile round

A GPS antenna could be added to the missile and, thanks to commercial applications, the chip sets are small and inexpensive. The US military has made considerable investment in GPS missile-guidance technology. The Joint Direct Attack Munition (JDAM) and Joint Stand-Off Weapon (JSOW) are two of several missiles that make use of the US GPS for guidance (Federation of American Scientists, n.d.a; n.d.b.). The components are well understood and suited to long-range navigation. Hobbyists have even adapted GPS payloads to model rockets so that they are easier to find when they come down, and to monitor and record their flight paths (Knowles, 2005).

The missile itself is equipped with a reprogrammable microprocessor, which would probably make it slightly easier to interface a GPS sensor with its control system. It is theoretically possible to introduce new software through the gripstock, although interfacing the new hardware to the existing microprocessor could pose a challenge. Nevertheless, the advantage of placing all the technical use-control equipment in the missile round is that it would also be close to the guidance system. Furthermore, it would not be necessary to do anything other than to disrupt one of the many guidance signals internal to the microprocessor. In any case, the missile is designed to self-destruct after a period of time in flight.

That said, adding technical-use controls to the missile would probably not be a weapon designer's first choice. It could reduce reliability or ease of use, and would require more extensive and expensive testing. Since it could interfere with the flight and firing of the missile, adding the additional hardware would be more expensive as it would affect a greater number of flight components. The use-control components would also take up additional space inside the missile, for which there may not be enough room. Even if there were, additional components could affect weight and balance. In some cases, adding use-controls could require significant changes to the design of the missile.

Internal components could be added to deactivate the missile after a specified period of time, but that would require an active power source, a battery, or a trusted external time source.[10] The current battery is inert until activated on launch (to preserve the shelf life). Finally, a strict GPS location-based approach located in the missile is unlikely to be feasible[11] since the time of flight is too short to get a reliable position fix.

An SA-24 Igla-S MANPADS launch tube and missile. © Vitaly V. Kuzmin

Technical-use controls installed in the gripstock

In the case of the FIM-92 Stinger, a better approach might be to put the technical-use controls in the gripstock. The advantage of doing so is that the latest versions of the Stinger are equipped with a module called the remotely programmable microprocessor (RMP),[12] which delivers new software to the guidance microprocessor embedded in the missile (Armada International, 1990). An effective approach might be to programme the system to deliver faulty guidance instructions to the missile microprocessor if authorization fails, which would prevent target locking, cause erratic flight behaviour or simply cause it not to fire.

The authorization could be delivered with a wireless fob or another token, such as a wristband or wristwatch, as proposed by some developers of 'smart gun' technology. The difficulty is that it would introduce yet another piece of hardware to maintain and ensure that it is available when needed. The activation fob would also need to be reset (or reauthorized) periodically and, if not properly protected, the fob could be diverted along with the weapon itself, thereby negating its capacity to prevent unauthorized use.

Technical-use controls and thermal battery redesign

Limiting the operational life of the BCU is an attractive alternative to an electronic PAL-like device. Venting the battery's argon, or the preventing the ignition of the heating materials, would effectively disable the system. It would be a relatively simple engineering task to ensure that the battery or argon supply is guaranteed to fail after a specified period of time, either by an electronic timer or by the progressive degradation of critical components, seals or materials. But ensuring the modifications are tamper-proof would require additional measures.

Furthermore, militants have shown remarkable ingenuity in reviving older MANPADS by using an external power supply instead of the original battery (Binnie, 2013). Preventing the use of an improvised power source may require a technical use-control, such as a mechanical or electronic handshake between the battery and the gripstock. Adding a connector between the BCU and the gripstock would permit electronic handshaking, which would ensure that only a specific set of batteries could be used with a specific gripstock. This would entail additional costs and would require some modifications to the gripstock's electronics but would prevent unauthorized users from using an improvised power supply or procuring unmodified batteries on the black market. Since the BCU is a consumable, there would be no need for extra tools to reset the validity time since it could simply be discarded.

Although the installation of technical-use controls in disposable, short-life batteries is a potential solution, the difficulty is that it may require an excessively long authorization period, given the lead time for battery manufacture and procurement. This raises the issue of what would be an appropriate lifespan for batteries, which could range from between one and five years. Since the clock starts the minute the batteries are manufactured, or set by a factory technician, it might be more convenient to provide for the reset and new 'valid until' dates electronically in the field or at another point in the transfer chain that is closer to operational forces.

Missile activation using the identification friend or foe (IFF) interrogator

The IFF module has logistical features that make it an attractive option for a technical-use control. Since the interrogator's programmer is necessary to transfer security data to the interrogator, it could be modified to allow for loading activation codes and resetting the validity period of the MANPADs. Operationally, the gripstock's microprocessor would contain something like an encrypted reprogrammable memory location for the 'valid until' date, after which the weapon would not fire. When the IFF interrogator is plugged in to the gripstock, it would receive a new 'valid until' date. This of course depends on the gripstock's having access to the correct time. Alternatively, the IFF integrator could provide an activation signal, without considering any 'valid until' date. The main drawback of placing the use-control device in the IFF interrogator is that it would require significant modifications to the gripstock electronics. As currently configured, the IFF is not required to operate the MANPADS. If the use-control device were located in the IFF, it would have to be modified so that the system could not be used without it.

Location of the reauthorization facility or equipment

Regardless of where the technical-use control is installed, special equipment would be necessary to adjust the use-controls for a renewed activation period or a new location. Logically, the equipment would reside in a special facility in the country of origin—at a facility maintained either by the weapon producer or by the government. Where exactly this facility is located would depend on how long the weapon is

scheduled to remain active, national policies on the storage and use of MANPADS, and the nature of the activation and reset security equipment.

Summary: locating the technical-use controls

A GPS approach would require an additional 15 minutes to fix the location, and power to operate the GPS equipment. It could be combined with a short activation period and performed in the days or hours before an expected engagement, using the IFF interrogator or accessory equipment to activate the missile in the field.

Placing the use-control device in the gripstock alone would require a key or code-entry system, anti-tampering devices, or time reference to allow activation in the 45 to 60 seconds that the MANPADS has power. On-board expiry dates would have to be loaded by the manufacturer or an authorized service facility. It would require adding a timer or a clock to the gripstock to ensure the codes have not expired. The addition of a timer would mean the gripstock would have to be electrically active during the authorized period. There is currently no electrical power to operate a timer. The correct time and date might be obtained by the use of a simplified GPS receiver.

Installing a use-control device in the IFF interrogator would allow the weapon to operate at any time during a predetermined activation period. This period would presumably coincide with the existing schedule for re-setting the CID codes[13] (Boyd et al., 2005), which are changed every few days. The authorization codes would be provided to the IFF interrogator only if the device were updated within the permitted geographic region or validity period. As noted above, this approach would be likely to require significant modifications to the system to ensure that the missile could be fired only if the IFF interrogator were attached.

A time-limited BCU would not be a viable approach if an unauthorized user could bypass the unit as has been done in the past.[14] Adding a digital key to the BCU would add security but would also require some modifications to the gripstock.

In summary, technical-use controls could significantly reduce the threat posed by MANPADS that are lost, stolen, or otherwise acquired by unauthorized persons. There are several possible approaches to deploying use-controls on MANPADS, all of which would require at least some modifications to key components and the establishment of a logistics infrastructure to maintain, reset, or transmit activation codes. The financial, administrative, and logistical challenges of doing this may prove to be significant. Furthermore, failure to safeguard codes and other sensitive elements of the infrastructure could render use-controls ineffective. Policy-makers would need to give careful consideration to these issues before adopting programmes to develop technical-use controls.

Other strategies

There are several other modifications to a MANPADS that could help to prevent—or minimize the damage caused by—unauthorized use. One potential option is to reduce the volume of explosives in the missile warhead. A Stinger missile with its 3 kg payload of high explosive has an energy potential of about 18.8 megajoules (MJ), the equivalent of around 20 sticks of dynamite. A 10 kg missile without a warhead travelling at Mach 2 would deliver almost as much punch (16 MJ) as the explosives in the Stinger warhead.[15]

MANPADS can be very effective against single-engine aircraft, and especially helicopters. The charge is seldom sufficient to cause extensive structural damage to wide-bodied, multi-engine planes. When the engines are widely spaced, as is the case with most commercial aircraft, the missile may destroy only one engine.[16] Some attacks against larger multi-engine aircraft have failed, as the missile hit the plane at an altitude that allowed the pilot to recover from the loss of an engine and land safely. Reducing the explosive power of the missile might further reduce the threat to large civilian aircraft. A potential drawback of this approach is its impact on the operational effectiveness of MANPADS that are equipped with proximity fuses. The warheads of many modern MANPADS are designed to detonate —and thereby damage an aircraft— even when the missile does not make a direct hit (i.e. come into physical contact with the target). Reducing the amount of explosive material in the warheads may significantly reduce their effect radius and, consequently, their effectiveness.

Another approach might be to design the missile to discriminate between potential targets based on the size of the aircraft. Some recent missile seekers include full high-resolution imaging systems in place of the scanning single detectors used in earlier generations of missiles (Kögler, 2013, p. 31). Given the miniaturization of modern electronics and small artificial intelligence-based processing systems, it may soon be possible to use image-recognition techniques to identify a potential target as probably being a commercial aircraft and so prevent engagement. More immediately, the guidance system could be modified to prevent firing on large multi-engine aircraft while they are accelerating and climbing during take-off —the flight stage when large or civilian aircraft are typically most vulnerable to

a MANPADS attack. Such an approach might be accommodated by changing the threat profiles stored in the operating system of the reprogrammable microprocessor.[17]

Plane-mounted anti-missile systems

The most high-profile technology-based approach to countering the threat of MANPADS falling into the wrong hands is the installation of anti-missile systems on civilian aircraft. This strategy attracted significant attention from policy-makers and the media, and several companies have developed new systems (or modified existing military systems) for use on commercial aircraft.

Technologies such as flares, flash-lamps, Infrared Countermeasures (IRCM), and Directional Infrared (laser) Countermeasures (DIRCM) can be effective, but equipping even a fraction of commercial wide-body aircraft with these systems would be a costly undertaking. The US Department of Homeland Security (DHS) estimates that installing anti-missile systems on national commercial aircraft alone would cost USD 43 billion over 20 years. This estimate is based on installing, operating and maintaining the defensive systems on more than 3,600 commercial US-registered passenger planes (US DHS, 2010, p. 33). Applying this to all commercial aircraft worldwide would entail enormous costs, which would increase as the commercial fleet grows. The US aircraft company Boeing estimates that, by 2032, there will be more than 40,000 aircraft in service, twice as many as in 2013 (Boeing, 2013, p. 15).

Notably, DHS officials declared the DIRCM technology to be effective: 'The production representative prototypes meet system effectiveness requirements and the design allows for a universal solution across large narrow-body and wide-body commercial aircraft' (US DHS, 2010, p. ii). The DHS report also notes that 'the airlines can integrate these DIRCM systems without significant impacts to daily operations' (US DHS, 2010, p. iv). Where the systems fell short was in reliability and operational factors, such as the level of periodic maintenance required (US DHS, 2010). In other words, they work well when they do work, but may not be sufficiently reliable for use in high-volume, everyday operations. Also, the DHS tested only DIRCM systems, which use a laser rather than pyrotechnic flares, in part because the threat scenario for civil aircraft might require the use of flares near to the ground, where people are living. As noted by the US Congressional Research Service, 'most flares pose a fire hazard to combustibles on the ground, and may be too risky for urban areas' (Bolkcom and Feickert, 2004, p. 13).

Moreover, Aircraft Missile Protection Systems (AMPS) are classified as weapons in the Wassenaar Arrangement Munition List.[18] There is an exception for certain less-advanced systems once they are installed on an aircraft, and certified for civil flight safety by a national aviation authority. But, under current law, the shipment of replacement systems and spare parts would be subject to export restrictions and a cumbersome licensing process (WA, 2013, section ML4.c).[19]

As noted, the devices tested by the DHS were not flare systems, and would not be exempt as civilian items under section ML4.d. The DHS noted in the conclusion of its final report that if counter-MANPADS are deployed on airliners, Congress would have to provide 'export control legislation to specifically address the use of military technologies employed to protect commercial aviation'. Further, it warned that '[c]ompliance with the current International Traffic in Arms Regulation […] requirements […] would cause serious operational, logistical, and financial problems for U.S. air carriers and an unsustainable burden on the U.S. export licensing system' (US DHS, 2010, pp. 56–57).

Finally, it is unclear whether anti-missile systems installed on aircraft today will be effective against MANPADS that may be developed in the future. Each new generation of MANPADS is designed to defeat the countermeasures in use at the time. The technology for anti-missile systems also continues to improve, but the very nature of countermeasure and counter-countermeasure development is that the defensive systems will lag behind the missile technology.

Regardless, the principal obstacles remain. Aircraft-mounted anti-missile systems are expensive and require significant maintenance, logistical support, and special facilities. Modifying the weapon rather than the target may be a more viable strategy.

Conclusion

Whether the use-controls are based on time, location, authorization codes, or some combination of all three, an infrastructure is required to maintain and reset the activation codes. This infrastructure would include, among other things, a key or code-management system, software, and hardware,[20] and could have significant logistical, budgetary, and tactical implications for the armed forces of countries seeking to deploy MANPADS with use-controls.

There are several key procedural and policy questions that must be addressed even before the design phase of any potential use-control. These questions include issues such as the optimum length of the activation period, who is permitted to own the activation-reset equipment, and the export-control regulations that

would apply to MANPADS equipped with use-controls, and for the associated technology. Further questions include whether use-control devices should be incorporated into all missiles produced, or whether it is sufficient to make modifications for special circumstances.

The successful development of use-controls would generate an additional set of questions for policy-makers, such as whether MANPADS equipped with use-controls should be supplied to foreign purchasers and operators. If so, this would raise the issue of where the initial authorization should take place—in the country of origin or in the importing country—and whether the activation or reset equipment would be transferred to the importing country. A further consideration is that of national policies for transferring weapons from a government to a non-governmental entity. Selecting the most effective approach to equipping MANPADS with technical-use controls requires careful consideration of these questions—and the underlying issues they are meant to address—by all the relevant parties.

In addition to policy work at the national level, international action may be required to harmonize national approaches to designing and establishing control standards for technical-use controls. Preliminary efforts to this end took place in 2003, when the WA Plenary agreed to 'implement technical performance and/or launch control features for newly designed MANPADS as such technologies become available to them' (WA, 2007, para. 3.4) as part of an expanded version of the 'Elements for Export Controls of Man-Portable Air Defense Systems (MANPADS)' (WA, 2007).[21]

It may be appropriate for the WA, the OSCE, and the G8 Secretariats, and other multilateral forums to address this issue by facilitating the sharing of information on technological innovations relevant to the development of use-controls and by encouraging member states to report on progress in applying use-controls in newly designed MANPADS.

Finally, it should be noted that use-control devices are not a panacea. It is unlikely that technology can provide solutions for scenarios similar to the Libyan or Syrian civil wars, during which hundreds of older MANPADS were looted from government depots. Addressing the threat posed by these and the thousands of additional MANPADS already in the global inventory that are vulnerable to diversion requires continued efforts to eliminate obsolete or poorly secured stocks of MANPADS and to limit transfers only to those governments with the means and the will to secure

Live-fire testing of an FIM-92 Stinger MANPADS at the US Air Force's Eglin test facility in Florida, 2014. © Samuel King Jr./US Air Force photo

them. These efforts will remain essential, regardless of whether technical-use controls are included in the next generation of MANPADS.

Technology continues to advance, and these advances will reduce or eliminate some of the key technical constraints associated with MANPADS discussed above. New and improved technologies that are relevant to the development and deployment of technical-use controls include faster position determination, improved ground-based or satellite telecommunication links, and onboard biometric (e.g. retina and fingerprint) scanners. But the greatest difficulty with any technological solution will be to ensure that authorized firings do not fail, and that unauthorized firings do not succeed. ■

Abbreviations and acronyms

AMPS	Aircraft Missile Protection Systems
BCU	Battery-coolant unit
CSIS	Center for Strategic and International Studies
CID	Combat identification
DHS	Department of Homeland Security (US)
DIRCM	Directional Infrared (laser) Countermeasures
G8	Group of Eight
GPS	Global Positioning System
HQ	Headquarters
IFF	Identification friend or foe
IRCM	Infrared Countermeasures
ITAR	International Traffic in Arms Regulation
JDAM	Joint Direct Attack Munition
JSOW	Joint Stand-Off Weapon
MANPADS	Man-Portable Air Defence System(s)
MJ	Megajoule
OSCE	Organization for Security and Co-operation in Europe
PAL	Permissive Action Link
RMP	Remotely programmable microprocessor
TFF	Time to first fix
TSF	Time to subsequent fix
WA	Wassenaar Arrangement

Endnotes

1 The WA's Elements for Export Controls on MANPADS do not define 'technical performance and/or launch control features' but it is assumed that the term refers to the types of device described as 'technical-use controls' in this Issue Brief.

2 The relevant provision in the G8 agreement reads 'we agree […] [t]o examine the feasibility of development for new Manpads of specific technical performance or launch control features that preclude their unauthorized use' (G8, 2003, para. 1.6). Paragraph 3.4 of the OSCE's Principles for Export Controls of Man-portable Air Defence Systems is identical to the wording of the relevant provisions in the WA.

3 Most MANPADS-producing countries, including the United States, have not introduced new models since the provision was added to the WA's Elements in 2003, and the available evidence suggests that few, if any, countries have incorporated use-control devices into their MANPADS (Schroeder, 2013, pp. 5, 26–27).

4 While journalists frequently refer to launch-control devices as 'kill switches', the term 'technical-use control' is more representative of the broad array of technological options. See Reed (2012) and Bonomo et al. (2007).

5 The IFF is a separate unit that operators wear on their belt.

6 Other factors, including robust physical security and stockpile management at nuclear weapons sites, also help to explain the absence of documented cases of unauthorized use of US nuclear weapons.

7 GPS refers only to the US navigation systems. Other space-based systems in existence or being developed by other countries are known collectively as Global Navigation Satellite Systems (GNSS). However, as the US system is the most developed, only GPS specifications were used in the technical analysis.

8 This may be counter-intuitive to those who use GPS every day, as a civilian GPS receiver usually has to download the complete data set only on certain occasions, such as when the batteries are removed or the device is moved a great distance while turned off.

9 While theoretically possible, changing the structure of the GPS signal to accommodate a weapons-activation code would pose significant challenges, both political and technical.

10 A non-PAL solution could be based on the timed degradation of the rocket fuel or explosive. But intentionally limiting the shelf-life of a MANPADS system is unlikely to be acceptable to the manufacturer or purchaser.

11 Some existing options are discussed in the section on GPS-based technical-use controls.

12 Also referred to as the RMP ROM module.

13 For a more detailed review of IFF and CID technology see Boyd et al. (2005).

14 See Chivers (2014). To the author's knowledge, armed groups have developed improvised batteries only for SA-7 pattern missiles, which do not contain coolant.

15 Author's calculation.

16 The exception being planes in which the engines are mounted close together at the tail of the aircraft, which makes them more vulnerable to catastrophic MANPADS attacks. Examples include the downing of a Tupolev 154B operated by Transair Georgia on 22 September 1993 and the attack on a Boeing 727-30 operated by Lignes Aeriennes Congolaises on 10 October 1998. See US DOS (2011).

17 There is a wide body of work using artificial neural networks, a branch of artificial intelligence (AI), techniques for image-processing to identify objects, based on thermal imagery. For a review of this topic see Rogers et al. (1990).

18 Also under the US International Traffic in Arms Regulation (ITAR) USML Category XI, as Military Electronic in the United States, although in a slightly more general way. CategoryIV(c) […] Note 2 to paragraph (c): *'Aircraft Missile Protection Systems (AMPS) are controlled in USML Category XI.'* Category XI provides no additional guidance on AMPS (US ITAR, 2014, Title 22, Chapter 1, Subchapter M, Part 121).

19 The United States is starting to recognise foreign civil certification and, in 2011, the Saab Civil Aircraft Missile Protection System (CAMPS) was granted a commodity classification in which the system itself (i.e. not installed in an aircraft) is classified under the US ITAR (see US ITAR (2014), XI(a)(4)(i) and XI(c); US DOC (n.d.), ECCN 9A991.b), but export licences are not required for the international movement of aircraft equipped with the systems. The classification does not apply to spares and other equipment, so a number of logistical issues remain. The relevant entries read, in part: 'ML4. Bombs, torpedoes, rockets, missiles, other explosive devices and charges and related equip-

ment and accessories, as follows, and specially designed components therefor: […] N.B.2. For Aircraft Missile Protection Systems (AMPS), see ML4.c. […] ML4. c. Aircraft Missile Protection Systems (AMPS)' (WA, 2013, p. 170).

20 A nuclear key management called the Code Management System (CMS), developed in about 1995, has simplified the logistics for the operators, and has improved the flexibility and speed in deploying and arming weapons. But the greater security comes at the cost of developing 14 custom tools (nine software and five hardware products) (Kristensen, 2005, pp. 20–21).

21 The WA agreement was revised in 2007 and the OSCE revised its counterpart in 2008. The language specific to 'Launch Controls' remains unchanged.

Bibliography

Anderson, Ross. 2008. 'Nuclear Command and Control.' In *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: Wiley, pp. 415–431.

Armada International. 1990. 'General Dynamics Stinger RMP deployed in Europe (remotely programmable microprocessor).' 1 February.

Bellovin, Steven M. 2009. 'Permissive Action Links.' Department of Computer Science, Columbia University. Updated 2 September. <https://www.cs.columbia.edu/~smb/nsam-160/pal.html>

Binnie, Jeremy. 2013. 'Militants Improvise MANPADS Batteries.' *Jane's Defence Weekly*. 14 May.

—. 2014. 'Grail Quest: MANPADS Proliferation in the Wake of Libya.' *Jane's Defence Weekly*. 12 June.

Boeing. 2013. *Current Market Outlook: 2013–2032*. <http://www.cme-mec.ca/download.php?file=4yoc7eob8.pdf>

Bolkcom, Christopher and Andrew Feickert. 2004. *Homeland Security: Protecting Airliners from Terrorist Missiles*. Congressional Research Service Report for Congress. RL31741. Updated 22 October. <http://fas.org/irp/crs/RL31741.pdf>

Bonomo, James, et al. 2007. *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*. Santa Monica, CA: RAND Corporation. <http://www.rand.org/content/dam/rand/pubs/monographs/ 2007/RAND_MG510.sum.pdf>

Boyd, Cameron S., et al. 2005. 'Characterisation of Combat Identification Technologies.' In TENCON 2005 IEEE Region 10 International Conference. <http://www.concepts.aero/system/files/CID-tencon-2005.pdf>

Chivers, C.J. 2014. 'A Syrian Rebel Advance Off the Battlefield: A Longer-Lasting Battery for Missiles.' *The New York Times*. 25 July. <http://www.nytimes.com/2014/07/26/world/middleeast/a-syrian-rebel-advance-off-the-battlefield-a-longer-lasting-rechargeable-battery-for-the-sa-7b-a-shoulder-fired-missile-system.html>

Cordesman, Anthony H. 2012. 'Syria, U.S. Power Projection, and the Search for an "Equalizer".' The Center for Strategic and International Studies (CSIS). 9 October. <http://csis.org/publication/syria-us-power-projection-and-search-equalizer>

Federation of American Scientists. n.d.a. 'AGM-154A Joint Standoff Weapon [JSOW].' FAS Military Analysis Network. <http://fas.org/man/dod-101/sys/smart/agm-154.htm>

—. n.d.b. 'Joint Direct Attack Munition (JDAM) GBU-29, GBU-30, GBU-31, GBU-32.' FAS Military Analysis Network. <http://fas.org/man/dod-101/sys/smart/jdam.htm>

Fitchett, Joseph. 2001. 'What About the Taliban's Stingers?' *The New York Times*. 26 September. <http://www.nytimes.com/2001/09/26/news/26iht-stinger_ed3_.html>

G8 (Group of Eight). 2003. 'Enhance Transport Security and Control of Man-portable Air Defence Systems (MANPADS): A G8 Action Plan.' Adopted at the June 2003 G8 summit. <http://www.g8.fr/evian/english/navigation/2003_g8_summit/summit_documents/enhance_transport_security_and_control_of_man-portable_air_defence_systems_-_manpads_-_a_g8_action_plan.html>

Global Security. n.d. 'FIM-43 Redeye.' <http://www.globalsecurity.org/military/systems/munitions/redeye.htm>

IHS Jane's. 2000. 'Raytheon Electronic Systems FIM-92 Stinger Low-altitude Surface-to-air Missile System Family.' *Jane's Land-based Air Defence*. 13 October.

Knowles, Vern. 2005. *Anglefire GPS Payload*. <http://www.vernk.com/Construction/AngelfireGpsPayload.htm>

Kögler, Christof. 2013. 'Technical Aspects and Components of MANPADS.' In *MANPADS: A Terrorist Threat to Civilian Aviation?* BICC Brief 47, pp. 26–40. <http://www.bicc.de/uploads/tx_bicctools/BICC_brief_02.pdf>

Kristensen, Hans. 2005. 'U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning.' New York: Natural Resources Defense Council. <http://www.nrdc.org/nuclear/euro/euro.pdf>

Londoño, Ernesto and Greg Miller. 2013. 'CIA Begins Weapons Delivery to Syrian Rebels.' *The Washington Post*. 11 September. <http://www.washingtonpost.com/world/national-security/cia-begins-weapons-delivery-to-syrian-rebels/2013/09/11/9fcf2ed8-1b0c-11e3-a628-7e6dde8f889d_story.html>

OSCE (Organization for Security and Co-operation in Europe). 2008. 'Updating the OSCE Principles for Export Controls of Man-portable Air Defence Systems.' Decision No. 5/08. 26 May. <http://www.osce.org/fsc/32082>

Parthasarathy, Harikrishna. 2004. 'Thermal Batteries — On the Rise?' *Frost & Sullivan*. 19 February. <https://www.frost.com/sublib/display-market-insight.do?id=10370700>.

Reed, John. 2012. 'Tracking Chips and Kill Switches for Manpads.' *Foreign Policy*. 19 October.

Rogers, Steven K., et al. 1990. 'Artificial Neural Networks for Automatic Target Recognition.' *Proc SPIE. 1294, Applications of Artificial Neural Networks*, 2. 1 August.

Schaffer, Marvin B. 1993. 'Concerns About Terrorists With Manportable SAMS.' *RAND Corporation Reports*. Santa Monica, Rand Corporation.

Schroeder, Matt. 2011. 'Man-Portable Air Defence Systems (MANPADS).' Research Note No. 1, 'Weapons and Markets'. Geneva: Small Arms Survey.

—. 2013. *The MANPADS Threat and International Efforts to Address It: Ten Years after Mombasa*. Washington, DC: Federation of American Scientists. <http://www.smallarmssurvey.org/fileadmin/docs/L-External-publications/ 2013/FAS-2013-The-MANPADS-Threat.pdf.pdf>

—. 2014. *Fire and Forget: The Proliferation of Man-portable Air Defence Systems in Syria*. Issue Brief No. 9. Geneva: Small Arms Survey. <http://www.smallarmssurvey.org/fileadmin/docs/G-Issue-briefs/SAS-IB9-MANPADS-and-Syria.pdf>

Shapiro, Andrew. 2012. 'Addressing the Challenge of MANPADS Proliferation.' Address to Stimson Center. 2 February. <http://www.stimson.org/images/uploads/Shapiro_Libya_Remarks.pdf>

US AFRICOM Public Affairs. 2011. 'TRANSCRIPT: Officials Provide Background on Secretary of State Clinton's Visit to Tripoli.' 17 October. <http://www.africom.mil/Newsroom/Transcript/8656/transcript-officials-provide-background-on-secreta>

US Army (Department of the Army). 1981. *Air Defense Artillery Employment Stinger.* Field Manual No. 44–18. 30 September. <http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm44_18.pdf>

—. 2000. 'Short Range Air Defense.' In *Air Defense Artillery Reference Handbook.* Field Manual No. 44-100-2. 31 March. <http://fas.org/spp/starwars/docops/fm44-100-2fd/chapter3.htm>

—. n.d. 'Stinger/Avenger.' Redstone Arsenal Historical Information: Missilery. <http://history.redstone.army.mil/miss-stingeravenger.html>

US Army Air Defense Artillery School. n.d. 'Introduction to MANPAD (16S) Stinger.' Subcourse No. AD 0575. US Army Air Defense Artillery School Fort Bliss, TX. <http://www.globalsecurity.org/military/library/policy/army/accp/ad0575/index.html>

US DHS (Department of Homeland Security). 2010. *Counter-MANPADS Program Results: Fiscal Year 2008 Report to Congress.* 30 March. <http://www.fas.org/programs/ssp/asmp/documents/DHSMANPADSReport.pdf>

US DOC (Department of Commerce). n.d. Commerce Control List. <http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>

US DOD (Department of Defense). 1996. *Navstar GPS User Equipment Introduction.* September. Accessed 8 January 2015. <http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf>

—. 2001. Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. 12 April (Amended 31 August 2005). <http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2805%29.pdf>

US DOS (Department of State). 2011. 'MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems.' 27 July. <http://www.state.gov/t/pm/rls/fs/169139.htm>

—. 2012. *Daily Press Briefing.* 25 October. <http://www.state.gov/r/pa/prs/dpb/2012/10/199742.htm#RUSSIA>

—. 2014. 'Commodity Jurisdiction Final Determinations.' Directorate of Defense Trade Controls. Updated 19 September. <http://www.pmddtc.state.gov/commodity_jurisdiction/determinationAll.html>

US ITAR. 2014. US International Traffic in Arms Regulations: United States Munition List (USML). <http://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5>

US Marine Corps. 2011. *Low Altitude Air Defense (LAAD) Gunner's Handbook,* MCRP 3-25.10A. 9 May. <http://www.marines.mil/Portals/59/Publications/MCRP%203-25-10a.pdf>

—. n.d. 'FIM-92A Stinger Weapons System: RMP & Basic.' *FAS Military Analysis Network.* <http://fas.org/man/dod-101/sys/land/stinger.htm>

WA (Wassenaar Arrangement). 2007. Elements for Export Controls of Man-Portable Air Defence Systems (MANPADS). <http://www.wassenaar.org/publicdocuments/2007/docs/Elements for Export Controls of Manpads.pdf>

—. 2013. Lists of Dual-Use Goods and Technologies. WA-LIST (13) 1. <http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf>

About the Small Arms Survey

The Small Arms Survey serves as the principal international source of public information on all aspects of small arms and armed violence, and as a resource centre for governments, policy-makers, researchers, and civil society. In addition to Issue Briefs, the Survey distributes its findings through Research Notes, Working Papers, Occasional Papers, Special Reports, Handbooks, a Book Series, and its annual flagship publication, the *Small Arms Survey*.

The project has an international staff with expertise in security studies, political science, international public policy, law, economics, development studies, conflict resolution, sociology, and criminology, and works closely with a worldwide network of researchers and partners.

The Small Arms Survey is a project of the Graduate Institute of International and Development Studies, Geneva.

For more information, please visit www.smallarmssurvey.org.

This Issue Brief has been made possible through the support of Germany's Federal Foreign Office.

Author: Gregory L. Tarr

Copy-editor: Deborah Eade

Fact-checking: Salome Lienert

Proofreader: John Linnegar

Illustrations: Daly Design (www.dalydesign.co.uk)

Layout: Frank Benno Junghanns (fbj@raumfisch.de)

Small Arms Survey

Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland

t +41 22 908 5777
f +41 22 732 2738
e info@smallarmssurvey.org

Federal Foreign Office

small arms survey