September **2014**

Remotely Piloted Aircraft Systems in Contested Environments

A Vulnerability Analysis

Joint Air Power Competence Centre

Cover picture [M] © Northrop Grumman Corporation

Disclaimer
This publication is a product of the JAPCC. It does not represent the opinions or policies of the North Atlantic Treaty Organisation (NATO) and is designed to provide an independent overview, analysis, food for thought and recommendations regarding a possible way ahead on the subject.

Author
Major André Haider (DEU A), JAPCC

Release
This document is releasable to the Public. Portions of the document may be quoted without permission, provided a standard source credit is included.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Telephone: +49 (0) 2824 90 2201
Facsimile: +49 (0) 2824 90 2208
E-Mail: contact@japcc.org
Website: www.japcc.org

[M] Denotes images digitally manipulated

FROM:

The Executive Director of the Joint Air Power Competence Centre (JAPCC)

SUBJECT:

Remotely Piloted Aircraft Systems in Contested Environments

DISTRIBUTION:

All NATO Commands, Nations, Ministries of Defence and Relevant Organizations

Over the past two decades, Remotely Piloted Aircraft Systems (RPAS) have been fielded in increasing numbers across many nations and military services. From the first operational deployment of the MQ-1 Predator during Operation Deliberate Force in 1995 to Operation Unified Protector over Libya in 2011, their flight hours have grown exponentially, providing distinctive capabilities with reduced risk and extensive time on station in comparison with manned systems.

In contrast to ground and manned aviation operations, recent RPAS missions have been conducted in a permissive air environment only, where Allied forces did not anticipate vigorous enemy Air Defence assets. Based on the assumption that in the future, NATO will be forced to deal with something other than an inferior or outgunned enemy, adversaries will have the capability and intent to oppose or disrupt NATO air operations and will represent a serious threat to Allied RPAS assets.

Therefore, this study provides a detailed assessment of current RPAS components' limitations and vulnerabilities, addressing operational, technical and legal questions. It outlines a vision of possible future conflict scenarios and compares these predicted threats with current capabilities. The study focuses on Medium Altitude Long Endurance (MALE) and High Altitude Long Endurance (HALE) RPAS. However, the identified risks and threats, as well as the given recommendations, may apply to other classes of RPAS as well.

We welcome your comments on our document or any future issues it identifies.
Please feel free to contact the RPAS section of the Combat Air Branch at the JAPCC staff via email: rpas@japcc.org.

Joachim Wundrak
Lieutenant General, DEU AF
Executive Director, JAPCC

JOINT AIR POWER COMPETENCE CENTRE

Joint Air Power Competence Centre | centre de compétence de la puissance aérienne interarmées
von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar | Germany/Allemagne | Tel +49 (0) 2824 90 2201 | Fax +49 (0) 2824 90 2208 | www.japcc.org
NCN: +234 or 239 2201 | **E-Mail:** contact@japcc.org

TABLE OF CONTENTS

ANNEX A–H

Recommendations by Threat Type

ANNEX I–K

Recommendations by Implementation Timeframe

ANNEX L–N

Recommendations by Application Area

ANNEX O

EXECUTIVE SUMMARY

Purpose of the Study

Over the past two decades, Remotely Piloted Aircraft System(s) (RPAS) have been fielded in increasing numbers across many nations and military services. RPAS provide distinctive capabilities for the Joint Force Commander (JFC) with reduced risk and extensive time on station in comparison to manned systems. In contrast to ground and manned aviation operations, current RPAS missions are conducted in a permissive environment only, where Allied forces do not anticipate a robust enemy Air Defence network. This study provides a detailed assessment of current RPAS limitations and vulnerabilities. It addresses operational and technical, as well as legal questions, outlines a vision of possible future conflict scenarios and compares these predicted threats with current capabilities. The study focuses on Medium Altitude Long Endurance (MALE) and High Altitude Long Endurance (HALE) RPAS. However, the identified risks, threats and recommendations may apply to other classes of RPAS also.

Assumptions

This study is based on the assumption that future North Atlantic Treaty Organization (NATO) operations will be forced to deal with something other than an inferior or outgunned enemy. It is assumed that future adversaries have the capability and intent to oppose or disrupt NATO air operations. It is also assumed that they are on a similar technological level and represent a serious threat to Allied forces.

Methodology

The study provides assessments of possible scenarios for future conflict derived from recent strategic studies. Based on these assessments, individual threats to RPAS were identified and analysed in more detail. As RPAS typically consist of several individual system elements, a matrix was set up to identify which threat affected a given RPAS element. Once this was completed, the vulnerabilities of the individual RPAS elements were outlined in detail with reference to the matrix. To assess the individual RPAS element's vulnerabilities, the 'Survivability-Kill-Chain' methodology was used. This methodology was adopted from Prof. Robert E. Ball's book, 'The Fundamentals of Aircraft Combat Survivability Analysis and Design'. Each identified threat and vulnerability was rated as either 'low', 'moderate' or 'high' and used the common 'traffic lights' colour system. All individual ratings of the identified threats and their respective RPAS element vulnerabilities were correlated and consolidated in a final 'criticality assessment matrix'. Recommendations were outlined following the 'Survivability-Kill-Chain' structure used in the vulnerability analysis chapter. As the study lists more than one hundred detailed recommendations, a quick reference was added as an annex. Finally, the study concludes with a strategic vision for future RPAS operations in NATO.

Background

RPAS have been used in support of NATO operations since 1995-96, when the first unarmed RPAS were deployed in support of Allied operations during the Bosnian War. The real turning point for RPAS came after 9/11 when the United States initiated Operation Enduring Freedom (OEF). Unmanned Intelligence, Surveillance and Reconnaissance (ISR) capabilities became critical in the global fight on terrorism. These operations were almost uniformly characterized by a permissive air environment. It must be noted this permissive air environment may have negatively influenced the most recent developments in RPAS technology. This may have resulted in exploitable vulnerabilities in newly fielded or soon to be fielded RPAS.

Possible Future Conflict Scenarios

It is difficult to predict future security threats. If NATO decides to intervene in interstate conflicts, it can be assumed that state actors are capable of confronting us with similar capabilities. Furthermore, the escalating number of actors gaining access to advanced and

dual-use technologies increases the potential for asymmetric attacks against the Alliance by those who are unable to match Western military technology. It can also be assumed that an adversary will probably avoid NATO's strengths and gravitate towards areas of perceived weaknesses. Therefore, it is likely an adversary will avoid conventional military operations and attack in an irregular or asymmetric manner.

Threat Identification

The identified threat dimensions for RPAS can be subdivided into symmetric, asymmetric and systemic. A symmetric threat is commonly defined as an attack on a comparable military level (i.e. force on force) which abides by the Laws of Armed Conflict (LoAC). The most probable adversary that can deliver a symmetric attack is a state actor. In the NATO Glossary of Terms and Definitions (Allied Administrative Publication 06, AAP-06), an asymmetric threat is defined as a 'threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting their weaknesses to obtain a disproportionate result.' Lastly, there are systemic limitations that may have an impact on future RPAS operations as well, e.g. the public perception of RPAS is influenced by the legal and moral aspects of their use.

Vulnerability Identification

In addition to the aircraft itself, all RPAS consist of several common components, which are the payload, human element, control element, data links and support element. RPAS share many of the same limitations manned aircraft have and have additional unique vulnerabilities. This study analyses the vulnerabilities of each individual RPAS component listed above.

Remotely Piloted Aircraft and Payload

The vulnerabilities of Remotely Piloted Aircraft (RPA) and their attached payload are quite similar to those of manned aircraft. The highest risk to airborne RPA will come from enemy Air Defence (AD) systems and combat aircraft as they are designed to detect and engage aircraft at long ranges. However, even Rocket-Propelled Grenades (RPGs) or sniper rifles could cause catastrophic damage to the airframe and payload if an adversary were within range. Each RPA is one of many nodes in the overall RPAS network, each of which is vulnerable to cyber-attacks and the corruption of microelectronics supply chains.

Human Element and Support Element

Attacking personnel rather than the RPA may be a favourable option for an adversary. Depending on the mission, RPAS personnel may be working at different locations. Within the Area of Operations (AOO), adversaries may engage RPAS personnel with any available weapons, e.g. combat aircraft, artillery or infantry. The vulnerability of RPAS personnel is equal to that of any other military personnel deployed to the AOO. RPAS remote split operations offer different opportunities for an adversary to conduct covert attacks. Special Operations Forces (SOF) assets or other means of asymmetric force can be employed on mission critical RPAS personnel in non-secure (civilian) environments. This study could not identify protective measures currently in place for off-duty and/or non-deployed personnel, but countless references were found revealing the names and identities of RPAS personnel during interviews and other press-related activities, indicating there is ample information to support such attacks.

Control Element

The Control Element consists of physical infrastructure (external hardware), computer systems (internal hardware) and non-physical software. All may be subject to different types of attack. The physical hardware may be attacked by kinetic weapons while the non-physical software may be subject to attack through cyber-warfare. Due to their unique size and shape, the hardware components may be positively identified as RPAS components to an alert adversary. Their persistent radio transmissions may also reveal their location to enemy electronic reconnaissance.

The Control Element's computer systems often include Commercial-off-the-Shelf (COTS) components. Identifying the multiple layers of contractors, subcontractors and suppliers contributing to the design or fabrication of a specific chip is difficult; tracing all of the contributors for a complete integrated circuit is even more difficult. This widely dispersed supply chain may provide an adversary with opportunities to manipulate those components or penetrate the distribution chain with counterfeit products.

The software components necessary to operate an RPAS are not limited to the Ground Control Station (GCS), but also include the aircraft, satellites and ground stations if applicable, as well as support systems for logistics, maintenance or Processing, Exploitation and Dissemination (PED). This variety provides an adversary with a broad spectrum of possible entry points into the RPAS network. Although current protective measures are thought to ensure an adequate level of cyber-security, they cannot guarantee absolute security.

Data Link

Data links connect RPA with the GCS and enable the operators to remotely control the RPA and receive transmissions. Possible Electronic Warfare (EW) targets for the adversary include the GCS, RPA, satellites and satellite ground segments. From the enemy's perspective, the satellite's receiving antenna and the RPA's Global Positioning System (GPS) antenna appear to be the most promising targets for EW engagements. Regarding the exploitation of transmitted RPAS signals, multiple discoveries of pirated RPA video feeds have proven that militant groups have adapted their tactics and have regularly intercepted Full-Motion Video (FMV) feeds. Shortly after these security issues were revealed, encryption of FMV streams was designated as a high priority. However, even today, not all currently fielded RPAS are capable of transmitting encrypted video feeds.

Consolidated Criticality Assessment Matrix

To determine the most critical effects on RPAS operations, the respective ratings of the threat and vulnerability summary are correlated. The individual ratings are displayed according to the standard 'traffic light colour system'. (cf. Table 1) Red indicates a highly critical issue which affects current RPAS operations and should be addressed as a high priority. Yellow indicates a moderately critical issue which is not yet highly critical, but may become so as technology evolves. Green indicates a less critical issue, meaning the RPAS could sustain attacks from threats listed in this category or they are not expected to face these threats.

Recommendations

This study identified more than one hundred individual recommendations throughout the entire scope of RPAS. They include measures in the air, ground and cyber-domains. However, there is no single solution that is suitable for all types of remotely piloted systems currently in use by NATO nations. Some recommendations may be easily and quickly adopted whereas others are expected to take years of development and integration. The annexes provide tables with an overview of all recommendations sorted by RPAS elements, threat types, application areas and expected implementation timeframes. They also provide the reader with a reference to the respective chapter number of the individual recommendation for further details.

Conclusions

Remotely Piloted Aircraft

It is very unlikely there will be a 'one-size-fits-all' solution for RPAS operations in a contested environment. In addition to Reconnaissance RPAS, which are expected to be upgraded and continue the role of current MALE/HALE systems, this study envisions the following categories of future RPAS which are optimized for specific purposes:

Deep Penetration RPAS - designed for full electromagnetic stealth, designated to conduct reconnaissance and air strikes deep inside enemy territory;

Combat RPAS - designed for high G-forces and manoeuvrability, designated to conduct air-to-air and air-

to-ground combat in non-permissive and hostile air environments;

Swarm RPAS - designed for expendability and operating in large numbers, forming a swarm;

Carrier RPAS - designed to carry an immense stock of long-range, precision-guided air-to-air and air-to-ground munitions, designated to project military power like naval aircraft carriers.

Ground-Based RPAS Elements and Personnel

To improve the survivability of deployed RPAS ground components, users should employ established and proven measures such as camouflage and dispersion of equipment, reducing radio transmissions or increasing mobility to facilitate leapfrog operations. However, the best way to protect RPAS ground elements would be to not deploy them at all. Therefore, the range of RPA must be significantly improved so they can be launched and recovered from inside NATO territory.

This study did not identify protective measures currently in place for off-duty personnel. Pre-emptively deterring threats for home-based RPAS infrastructure and personnel must not be considered a military-only task. Military Force Protection Conditions (FPCON) should be complemented with additional protective measures provided by local civilian authorities. Comprehensive and joint civil and military force protection measures should also encompass the domestic environment to include families of RPAS personnel.

Command, Control, Communications and Computers

Improvement of RPAS Command, Control, Communications, and Computer (C4) security must be comprehensive and should encompass the physical components required for RPAS communication, the

Table 1 – Consolidated Criticality Assessment Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft	Highly Critical	Highly Critical	Low Critical	Low Critical	Moderately Critical	Moderately Critical	Moderately Critical	Highly Critical	Moderately Critical
Payload	Highly Critical	Highly Critical	Low Critical	Low Critical	Moderately Critical	Moderately Critical	Moderately Critical	Highly Critical	Moderately Critical
Human Element	Low Critical	Moderately Critical	Low Critical	Low Critical	Moderately Critical	Low Critical	Highly Critical	Low Critical	Highly Critical
Control Element	Low Critical	Highly Critical	Low Critical	Highly Critical	Highly Critical	Low Critical	Low Critical	Highly Critical	Highly Critical
Data Link	Low Critical	Highly Critical	Low Critical	Highly Critical	Highly Critical	Low Critical	Moderately Critical	Highly Critical	Highly Critical
Support Element	Low Critical	Moderately Critical	Low Critical	Low Critical	Moderately Critical	Low Critical	Low Critical	Low Critical	Moderately Critical

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

computer systems (to include their software packages), the electromagnetic spectrum they operate in, and any personnel with access to the RPAS. They may be all subject to different types of attacks and require different levels of protection. Physical components should follow the same principles of camouflage, dispersion and mobility like any other ground-based element aiming to avoid detection. COTS computer hardware should be thoroughly balanced against the inherently superior security of proprietary systems. If COTS systems are preferred, trustworthy supply chains for these hardware components and their sub-components must be ensured. Capable, trustworthy and updated security software suites are essential in defending computer networks. In addition to these defensive measures, offensive and pre-emptive cyber-operations should be conducted to eliminate threats in advance. Future RPAS development should focus on reducing radio communications dependency by introducing new means of data transmissions and increasing RPA automation. To prevent corruption, adversary recruitment or blackmail attempts which may lead to a breach of security, RPAS personnel should receive mandatory training to raise awareness of those issues. Computer system access policies (both for software and hardware) should be as restrictive as necessary to defend against intrusion attempts or exploitation of human carelessness.

Automation and Human Interaction

Achieving higher levels of automation is a prerequisite in enabling many of the recommendations made in this study; however, what is technically possible is not necessarily desirable. The automated release of lethal weapons should be considered very judiciously with respect to legal, moral and ethical questions. This study recommends two fundamental types of lethal weapons release, i.e. deliberate attack and automated defence. For any target that requires approval by the Joint Targeting Process, a deliberate human decision for weapon release must be enforced. Conversely, automated weapon release should be approved for any target that is actively engaging the RPA. The threshold of what is considered an active attack should follow the same principles as for manned combat aircraft. This study refrains from recommending an 'Automated Attack' mode for RPAS. Such an automated attack mode would entail a multitude of legal, moral and ethical questions.


© US Air Force, Lance Cheung

CHAPTER 1

Introduction

Over the past two decades, RPAS have been fielded in increasing numbers across many nations and military services. From the first operational deployment of the MQ-1 Predator[1] during Operation Deliberate Force (ODF) in 1995 to Operation Unified Protector (OUP) over Libya in 2011, their flight hours have grown exponentially and this growth continues today. RPAS provide distinctive capabilities for the JFC with reduced risk. Some of these capabilities include surveillance, reconnaissance, precision targeting and precision strike.[2,3,4]

The enormous increase in RPAS mission flight hours shows how important remote flight has become to the JFC. RPAS in combat and the information they provide have transformed the view of these systems. Once viewed as simply an expendable tool, they have now become an invaluable asset. NATO's military forces are dependent on accurate and timely information and therefore reliant on the capabilities RPAS provide.[5]

The original purpose of RPAS was surveillance, reconnaissance and target acquisition. Their development was driven by Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF). Their primary role today remains unchanged. Therefore, current RPAS are still based on their legacy design and have only been modified to conduct precision strike operations. Unchallenged by enemy Air Defences, RPAS have been able to reach far into insurgent territory, where it would have been difficult to insert ground forces.[6] However, current RPAS have had little or no survivability features incorporated into their designs. New designs incorporate basic stealth technology to help reduce susceptibility, but little attention has been paid to reducing vulnerability.[7]

RPAS designed specifically for attack operations are currently in development but have not yet been fielded. Fielded RPAS architectures were not designed

for operations in higher threat environments, leaving them vulnerable to enemy forces.

Current RPAS doctrine, Tactics, Techniques and Procedures (TTP) were fostered by the absence of a robust enemy AD capability. The current success of RPAS employment is highly dependent on maintaining air superiority over the AOO. If airspace superiority is not possible, depending on RPAS to provide the same capability in future combat operations will be challenging. Regardless, RPAS involvement in future operations is expected to increase and the JFC will be even more dependent on remotely piloted weapons systems than they are today.[8,9,10]

This document focuses on RPAS use in possible future combat environments where the threat is higher than what was seen in recent military operations. It provides concepts for the continuing development and employment of RPAS across all military domains. It also delivers operational and technical recommendations.

1.1 Aim

This document aims to:

- provide a detailed assessment of current RPAS components' limitations and vulnerabilities;
- provide inputs to identify future RPAS requirements;
- provide guidance to facilitate RPAS operations in contested air environments;
- address operational, technical and legal questions;
- outline a vision of possible future conflict scenarios and compare these predicted threats with current capabilities.

1.2 Assumptions

This study assumes that NATO's global interests and responsibilities will endure and threats to those will continue. Furthermore, the study assumes that future military operations will no longer deal with an inferior or outgunned enemy. It is likely the Alliance will face an enemy that is able to project a viable threat to Alliance air assets. More clearly stated, this assumption means an adversary has the capability and the intent to oppose or disrupt friendly air operations.

1.3 Limitations

To keep this publication on an unclassified level, the research and analysis supporting this study used publicly available (unclassified) reports, studies and roadmaps. If classified sources were used, only unclassified information was extracted. Additional information was acquired from various RPAS manufacturers during conferences, exhibitions and personal interviews, but only used if permission for public release was granted.

1. The General Atomics MQ-1 Predator is a class II MALE UA initially conceived in the early 1990s for reconnaissance and forward observation roles. The Predator carries cameras and other sensors but has been modified and upgraded to carry and fire missiles or other munitions.
2. R. C. Owen, Deliberate Force – A Case Study in Effective Air Campaigning, 2000.
3. U.S. Department of Defense, Unmanned Systems Integrated Roadmap FY2011-2036, 2011.
4. Headquarters, United States Air Force, RPA Vector: Vision and Enabling Concept 2013-2038, Feb. 2014.
5. Major Jaysen A. Yochim (US Army), US Army Command and General Staff College, 'The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack', Jan. 2010. [Online]. Available: http://www.fas.org/irp/program/collect/uas-vuln.pdf. [Accessed 16 Apr. 2013].
6. P. C. Nolin, Countering the Afghan Insurgency: Low Tech Threats, High-Tech Solutions, NATO Parliamentary Assembly, 2011.
7. Kevin R. Crosthwaite, 'Unmanned Aerial Vehicle (UAV) Survivability Enhancement Workshop', Aircraft Survivability, pp. 6-9, Fall 2005.
8. National Defense Magazine, 'Efforts Under Way to Harden Unpiloted Aircraft for Contested Airspace', Jul. 2011. [Online]. Available: http://www.nationaldefensemagazine.org/archive/2011/July/Pages/EffortsUnderWaytoHardenUnpilotedAircrafftforContestedAirspace.aspx. [Accessed 12 Apr. 2013].
9. Vice Admiral William Burke, AUVSI Annual Conference, Las Vegas, NV, 2012.
10. A. Carter, United States Deputy Secretary of Defense, Washington, D.C., 2012.

© US Air Force, Airman 1st Class Jonathan Steffen

CHAPTER 11

Definitions

This document uses specific terminology with regards to RPAS and its components, threat levels and types of operations. Not all of this terminology is defined within the NATO Glossary of Terms and Definitions AAP-06. Different organizations may use different terminology for the same concept, even within a single nation. The following chapter introduces terminology and provides definitions as they are used for this study. If applicable, this document uses existing NATO terminology and definitions from the AAP-06.[1]

2.1 Remotely Piloted Aircraft Systems

The idea that Unmanned Aircraft Systems (UAS) are 'unmanned' is a misnomer. While the Unmanned Aircraft (UA) itself is not manned, the system is manned and the aircraft is remotely controlled. Therefore this study prefers to use the term Remotely Piloted Aircraft System (RPAS) and Remotely Piloted Aircraft (RPA) instead of UAS and UA. RPAS can be defined as systems whose components include the RPA, the supporting network and all equipment and personnel necessary to control the RPA.[2] In addition to the aircraft, RPAS consist of several common components. (cf. Fig. 1) These additional components are the payloads, human element, control element, data links and support element. The following sections briefly describe these components.[3]

2.1.1 Remotely Piloted Aircraft

The RPA does not carry a human operator and is capable of flight under remote control or automated programming. It can be a rotary, fixed wing, or lighter-than-air aircraft. It includes integrated equipment such as propulsion, avionics, fuel, navigation, and communication systems.[4]

An RPA is an aircraft which is remotely controlled by a pilot who has been trained and certified to the same

standards as the pilot of a manned aircraft.[5] RPAs are typically operated by the air force.

In contrast to RPA, Remotely Operated Aircraft (ROA) are remotely controlled by an operator who has not been trained nor certified to the same standards as the pilot of a manned aircraft. ROAs are typically operated by services other than the air force. For the purposes of this study, the term RPA will include ROA as well.

2.1.2 Payload

The payload includes sensors, communications equipment, weapons and/or cargo. They are carried either internally or externally by the RPA.[6]

2.1.3 Human Element

The Human Element consists of the aircraft's pilot and the payload operator. RPAS personnel also include maintainers, mission commanders and intelligence analysts.[7]

2.1.4 Control Element

The Control Element handles multiple aspects of the mission, such as Command and Control (C2), mission planning, payload control and communications. It can be ground-based, sea-based or airborne. The portion of the Control Element where the aircraft's pilot and the payload operator are physically located is referred to as the GCS. The physical location of the GCS can vary greatly and depends if Line of Sight (LOS) or Beyond Line of Sight (BLOS) communication is established. If the RPA is controlled via BLOS Satellite Communication (SATCOM), the GCS can be located outside the AOO.[8]

2.1.5 Data Links

Data links include all means of communicating among the RPA, the Control Element and every relay station and network node in-between them. They are used for any means of data transfer. The RPA data links can be transmitted via either LOS or BLOS.[9]

Figure 1 – RPAS Elements.

2.1.6 Support Element

The Support Element includes all of the prerequisite equipment to deploy, transport, maintain, launch and recover the RPA and enable communications. These tasks are typically conducted by Launch and Recovery Units (LRU).[10]

2.2 RPAS Classifications

RPAS function at all levels of operations (tactical, operational, and strategic.) There is a strong correlation between categorization as specified in the NATO RPAS Classification Guide (based on take-off weight and operating altitude) and the level of operation a specific RPAS influences. (cf. Table 2) This document will focus on MALE, HALE and Strike RPAS normally employed at the Strategic and Operational level. The conclusions and recommendations in this document may also be applicable to other classes of RPAS.

2.3 Operational Environments

NATO differentiates between permissive, non-permissive and hostile environments. These terms are defined in the AAP-06 and used in this document as follows:

2.3.1 Permissive Environment

In a permissive environment, friendly forces anticipate no obstructions to, or interference with, operations. A

permissive environment does not necessarily imply absence of threat.[12]

2.3.2 Non-Permissive Environment

In a non-permissive environment, friendly forces anticipate obstructions to, or interference with, operations.[13]

2.3.3 Hostile Environment

In a hostile environment, an adversary has the capability and intent to oppose or disrupt operations of friendly forces.[14]

In contrast to ground and manned aviation operations, RPAS missions have largely been conducted within a permissive environment, where NATO forces do not anticipate enemy AD activity. This document assumes that NATO must expect non-permissive and even hostile environments during air operations in future conflicts.

1. NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-06), 2012.
2. Ibid.
3. JAPCC, Strategic Concept of Employment for Unmanned Aircraft Systems in NATO, 2010.
4. Ibid., p. 3.
5. NATO Joint Capabilities Group Unmanned Aircraft Systems (JCGUAS), 2013.
6. Ibid. 3, p. 4.
7. Ibid. 3.
8. Ibid. 3, p. 4 f.
9. Ibid. 3, p. 5.
10. Ibid. 3, p. 5.
11. NATO Joint Capabilities Group Unmanned Aircraft Systems (JCGUAS), 2009.
12. Ibid. 1.
13. Ibid. 1.
14. Ibid. 1.

Table 2 – NATO RPAS Classification Guide.[11]

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
CLASS I < 150 kg	MICRO <2 kg	Tactical Platoon, Section, Individual (single operator)	Up to 200 ft AGL	5 km (LOS)	Platoon, Section	Black Widow Mikado SpyArrow
	MINI 2-20 kg	Tactical Sub-unit (manual launch)	Up to 3K ft AGL	25 km (LOS)	Company, Squadron	Scan Eagle Skylark Raven
	SMALL >20 kg	Tactical Unit (employs launch system)	Up to 5K ft AGL	50 km (LOS)	Battalion, Regiment, Brigade	Luna Hermes 90 Skylark II
CLASS II 150 kg - 600 kg	TACTICAL	Tactical Formation	Up to 10,000 ft AGL	200 km (LOS)	Brigade	Hermes 450 Seeker 400 Shadow 600
CLASS III > 600 kg	Strike/ Combat	Strategic/National	Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre COM	Predator B Predator C
	HALE	Strategic/National	Up to 65,000 ft MSL	Unlimited (BLOS)	Theatre COM	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF COM	Predator A Heron Hermes 900

CHAPTER III

Operational Environment Background

There has been an immense growth in the development and fielding of acquired RPAS since 9/11. (cf. Fig. 2) RPAS have been very effective in anti-terrorist operations, as these groups were effectively incapable of presenting a viable air threat. As such, RPAS operations were almost uniformly characterized by a permissive air environment. This permissive air environment may have negatively influenced recent RPAS development. For more than a decade, the focus to further improve RPAS was primarily on sensor capability, imagery exploitation and aircraft endurance rather than on survivability. This may have resulted in exploitable vulnerabilities.

3.1 Balkan Operations

RPAS were used in support of NATO operations since 1995-96, when the first unarmed RPAS were deployed in support of Allied operations in the Bosnian War.[3] During Operation Allied Force (OAF) in 1999, six nations operated RPAS over the former Federal Republic of Yugoslavia. RPAS were employed in OAF to detect land mines, conduct damage assessments and gather intelligence on the movement of forces, equipment and refugees.[4] While highly vulnerable to AD, RPAS offered two key advantages: they helped limit collateral damage by improving precision in the identification of targets for air strikes and they reduced allied casualties by providing reconnaissance, which otherwise could only have been delivered by low-flying manned aircraft highly vulnerable to AD.[5]

RPAS were flown as low as 1,000 ft above enemy troop positions gathering real-time video and imagery to enable immediate attacks by manned aircraft. Several RPA were lost when they descended into the lethal envelopes of Serb Anti-Aircraft-Artillery (AAA) or Man-Portable Air Defence Systems (MANPADS). At least four MALE RPA were shot down by Surface-to-Air Missiles (SAM). RPA were eventually restricted to operat-

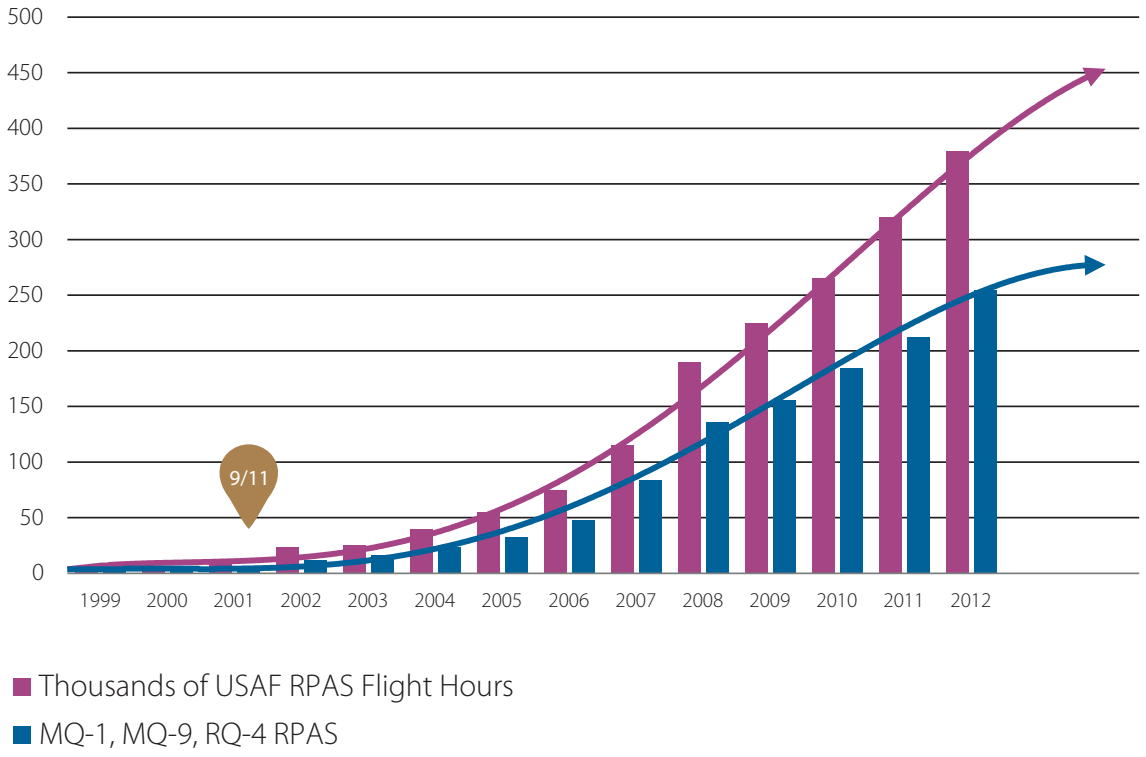


Figure 2 – US Air Force RPAS Flight Hours and MALE/HALE Systems.[1,2]

ing in a designated airspace. This resulted in a predictable pattern that was easily recognized by Serbian forces. This led to additional RPA losses.[6]

3.2 Iraq Operations

During the beginning of operations in Iraq in 2003, aging first-generation RPA were used as decoys to expose Iraqi AD and stir up Iraqi fighters.[7] RPAS were used in joint manned/unmanned missions for the first time. Also, RPAS directly supported US Army Counter Improvised Explosive Device (C-IED) task forces by using Electro-Optical and Infrared (EO/IR) sensors to detect and identify insurgents placing Improvised Explosive Device(s) (IED) under the cover of night.[8]

3.3 Afghanistan Operations

The real turning point for RPAS came after 9/11 when the United States was attacked and initiated OEF. Unmanned ISR capabilities became a critical capability in this global fight against terrorism.[9] On 14 November 2001, the first strike of an armed RPA took place in Afghanistan, when a combined F-15/Predator attack killed key Taliban and al-Qaeda decision makers responsible for the attacks of 11 September 2001. Since then, RPAS have become an integral part of military efforts in Afghanistan.[10]

The most prominent role of RPAS in Afghanistan continues to be ISR, in which their remote sensing capabilities are utilized to the fullest extent. Additionally, armed RPAS were frequently switched from the primary ISR role into a strike asset. Often employed in coordination with troops on the ground, they have eliminated insurgent leaders and destroyed critical enemy infrastructure.[11]

3.4 Libya Operations

The air campaign to enforce a no-fly-zone over Libya was supported by both armed and unarmed RPAS.

They were used primarily to conduct ISR operations similar to those in Afghanistan. Additionally, most of the strike targets by manned aircraft were identified by RPAS. For example, the capture of Colonel Muammar Gaddafi was facilitated by an RPAS. Manned aircraft attacked Gaddafi's convoy as he attempted to flee the city of Sirte on 20 October 2011.[12] Nevertheless because of their high vulnerability and the imminent threat of the Libyan SA-24 missiles, RPAS were not employed until a more favourable situation was achieved.[13] Additionally, the Libyan conflict revealed RPAS capacity shortfalls in most of NATO's European member states. The growing demand for RPAS capability requirements was only filled by the significant contributions of the United States Air Force.[14]

1. U.S. Department of Defense, Unmanned Systems Integrated Roadmap FY2011-2036, 2011.
2. U.S. Department of Defense , Defense Budget Priorities and Choices - Fiscal Year 2014, Apr 2013.
3. P.C. Nolin, Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance, NATO Parliamentary Assembly, 2012.
4. Ibid.
5. Ibid.
6. B. S. Lambeth, NATO's Air War for Kosovo: A Strategic and Operational Assessment, Rand, 2001.
7. National Defense Magazine, 'Efforts Under Way to Harden Unpiloted Aircraft for Contested Airspace', Jul. 2011. [Online]. Available: http://www.nationaldefensemagazine.org/archive/2011/July/Pages/EffortsUnderWaytoHardenUnpilotedAircraftforContestedAirspace.aspx. [Accessed 12 Apr. 2013].
8. P.C. Nolin, Countering the Afghan Insurgency: Low Tech Threats, High-Tech Solutions, NATO Parliamentary Assembly, 2011.
9. Ibid. 3.
10. Ibid. 8.
11. Ibid. 8.
12. Ibid. 3.
13. Ibid. 7.
14. Ibid. 3.

CHAPTER IV

Possible Future Conflict Scenarios – Strategic and Operational Challenges in Future Combat Environments

It is hard to predict future security threats. No matter how thorough we are in our plans or how diligently we prepare, there will always be surprises and the future is not certain. The next threat may be another strategic surprise or 'wildcard' incident. The Japanese attack on Pearl Harbor in 1941 or the al-Qaeda attacks on the World Trade Center in 2001 are examples of this type of event.[1,2]

4.1 Proliferation of Air Defence Technology

The Soviet Union and Warsaw Pact disintegrated more than two decades ago. Together with their Third World satellites and surrogates, they possessed the largest global inventory of SAM systems, SAM war stocks and supporting radars. The economic crisis that ensued after this disintegration resulted in the loss of state funded cash flow for manufacturing and maintenance of military systems. This resulted in a global 'fire sale' of all types of AD equipment and component war stocks. Nations that were previously denied access to top end Soviet equipment suddenly found themselves being offered whatever they could afford, and more.[3]

AD systems and anti-access technologies became more widely available to state and non-state actors through official arms trade or via arms smuggling. While Western Nations remain strongly wedded to Cold War era controls on weapons exports, Russian, Chinese and those of many former Soviet republics industries operate without such constraints. The variety of AD systems ranges from small man-portable systems up to highly advanced stationary or mobile SAM systems. The main challenge is, once these

weapons are outside of governmental control, it is often extremely difficult to track their movement and control who has access to them. This is especially true with small, mobile and man-portable systems.[4]

Western nations have not been confronted by modern, state-of-the-art AD equipment since the early 1970's Vietnam War. Aside from some legacy Russian style Surface-Based Air Defence (SBAD) systems in the 1999 Kosovo war, the air campaign against the Taliban in late 2001 was effectively uncontested, as was the invasion of Iraq in 2003.[5] Sophisticated AD systems could dramatically shift the balance of power in a certain region and may even prevent projection of air power by Allied forces. As a result, NATO may face increasing difficulty in ensuring and maintaining a permissive air environment.

4.2 State and Non-State Actors

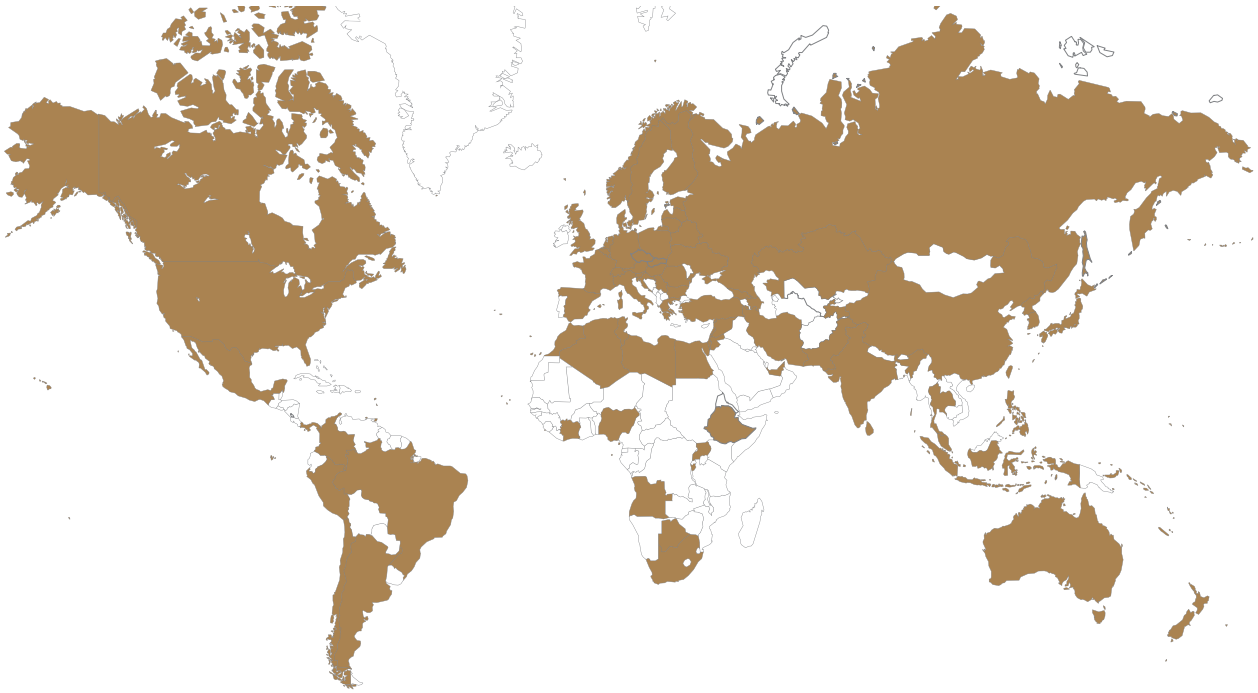
Despite the possibility of strategic surprise, a large-scale conventional confrontation with NATO as a whole is unlikely. There are potential interstate conflicts in the Middle East, the Caucasus, and East and South Asia which may involve NATO air operations.[6] NATO may not only have to deal with rogue states, but also with non-sovereign entities that exercise significant economic, political, or social power and influence at a national or even international level. Although it is more likely NATO will be threatened by instabilities versus a full scale conventional war, the consequences of these regional conflicts may have a significant impact on the security of the Alliance.[7]

Sophisticated adversaries may use asymmetric capabilities, to include electronic and cyber-warfare, ballistic and cruise missiles, advanced AD systems and other methods of warfare. Some proliferation of sophisticated weapons and technology may extend to non-state actors as well.[8]

4.3 Proliferation of Advanced Technology

The availability and proliferation of advanced technology will provide adversaries with high end capabilities like never before. Non-state entities have already used more advanced missile systems to target state adversaries, e.g. Hezbollah against Israel. The proliferation of precision technologies and longer-range delivery platforms puts Allied forces increasingly at risk. Further-

Figure 3 – Proliferation of RPAS.



more, significant advances in technology can cut both ways. It can increase the capabilities of the Alliance while also improving the enemy's ability to attack NATO systems and networks. Therefore, a determined adversary who wants to achieve a strategic surprise may exploit this technology against NATO's interdependent systems and infrastructures. Attacking those information systems may create a 'digital' Pearl Harbor.[9]

4.4 Proliferation of RPAS Technology

'Those worried about drone proliferation must face facts. We are no longer in a world where only the US has the technology, and we are not moving toward a future in which the technology is used only in the same way we use it now.'
Peter Warren Singer
Director of the Center for 21st Century Security and Intelligence at the Brookings Institution

Approximately 80 countries currently possess RPAS, of which fewer than a dozen operate systems that can be armed. This number has increased from approximately 41 countries in 2004 to at least 76 countries in 2012.[10,11] (cf. Fig. 3) This trend is expected to continue. The number of countries running their own RPAS development programs or are actively trying to achieve RPAS technology can only be estimated. It can be assumed this number is higher than those states already using RPAS technology.

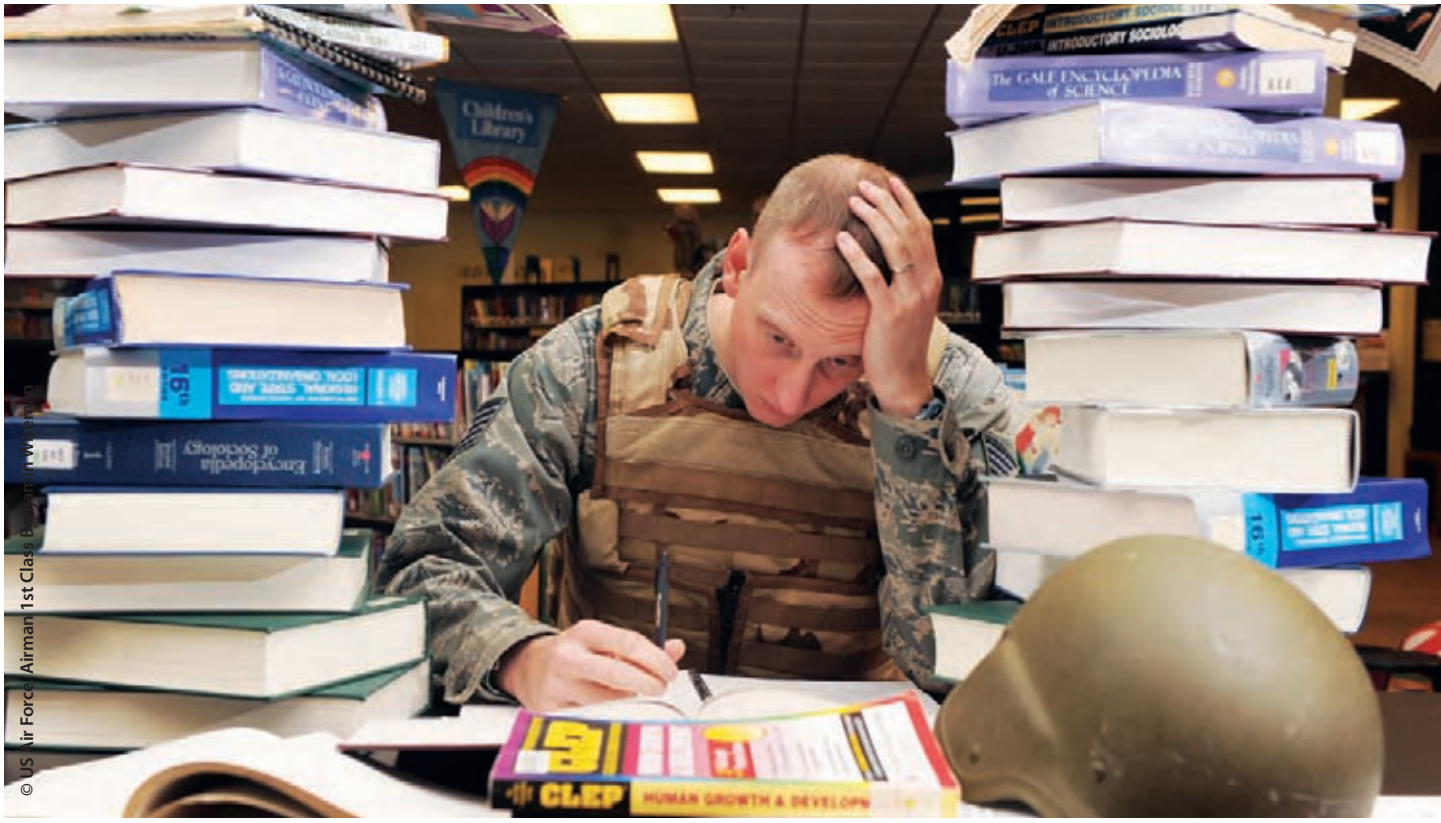
Adversaries may obtain Alliance RPA, reverse engineer the captured aircraft and exploit the information to copy the technology and develop systems or countermeasures. Iran, for example is actively researching shaping methods to reduce the detectability of its RPA.[12] In addition, an insurgent force may score a strategic communications victory by displaying a captured RPA in their propaganda. Therefore, recovery or destruction of lost RPA should be considered a high priority mission due to security and strategic concerns.[13]

4.5 Symmetric vs. Asymmetric Warfare

If NATO decides to intervene in interstate conflicts, it can be assumed that state actors are capable of attacking with nearly symmetric capabilities. These capabilities may include ballistic missiles, manned and remotely piloted aircraft, electronic warfare, cyber-capabilities and even anti-satellite weapons. The implications on the Alliance may be exacerbated by state actors who supply advanced arms to non-state actors and terrorist organizations. The escalating number of actors gaining access to advanced and dual-use technologies increases the potential for asymmetric attacks against the Alliance by those who are unable to match Western military technology.[14]

It can be assumed that an adversary will probably avoid NATO's strengths and gravitate towards areas of perceived weaknesses. Therefore, it is likely an adversary will avoid conventional military operations and will attack in ways we might consider irregular or asymmetric.[15] Some political entities also subscribe to ideologies that welcome martyrdom. This raises many questions about deterrence and force protection.[16]

1. 38th IFPA-Fletcher Conference on National Security Strategy and Policy, 'Air, Space, & Cyberspace Power in the 21st-Century', 2010.
2. NATO, Allied Command Operations, Multiple Futures Project, Navigating towards 2030, Apr. 2009.
3. Dr. Carlo Kopp, 'Proliferation of Advanced Air Defence Systems', Defence today, pp. 24 - 27, Mar. 2010.
4. Ibid.
5. Ibid.
6. A. C. Transformation, 'Strategic Foresight Analysis Report', 2013.
7. Ibid. 2.
8. 'Sustaining U.S. Global Leadership: Priorities for 21st Century Defense', United States Department of Defense, Washington, 2012.
9. Ibid. 1.
10. L. Brooke-Holland, Unmanned Aerial Vehicles (drones): an introduction, U.K. House of Commons, 2013.
11. U.S. Government Accountability Office (GAO), NONPROLIFERATION - Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports, GAO, 2012.
12. Hamid Heidar, Naser Moradisoltani, Omid Alihemati, 'Simulation and reduction of radar cross section the unmanned aerial vehicle in X-band using Shaping technique', Majlesi Journal of Telecommunication Devices, vol. 1, no. 4, pp. 132-137, Dec. 2012.
13. Major Jaysen A. Yochim (US Army), US Army Command and General Staff College, 'The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack', Jan. 2010. [Online]. Available: http://www.fas.org/irp/program/collect/uas-vuln.pdf. [Accessed 16 Apr. 2013].
14. Ibid. 1.
15. Ibid. 2.
16. Ibid. 1.



© US Air Force / Airman 1st Class B...

CHAPTER V

Threat and Vulnerability Identification Methodology

Chapters VI and VII will identify possible threats to and vulnerabilities of RPAS and will conclude with an assessment of the respective threat or vulnerability level, which will be expressed as 'low' (green), 'moderate' (yellow) or 'high' (red).

5.1 Defining the Threat Level

The threat level is expressed as the probability of an attack and is depicted at the end of the respective chapters in a vulnerability matrix. To determine the probability of an attack, there are two factors being considered: 'Availability' and 'Accessibility'. The 'probability of attack' factor does not consider the possibility of success or failure. It merely rates the likelihood that possible future adversaries are in possession of certain weapons and NATO can anticipate their use against Allied RPAS.

5.1.1 Availability

'Availability' describes the probability that an adversary possesses certain weapons, weapon systems or military force which is required to produce a threat to the RPAS.

5.1.2 Accessibility

'Accessibility' describes the probability that an adversary can get into striking distance to cause physical damage, disrupt or interfere with any component of the RPAS.

Table 3 – Threat Levels Examples.

Availability	Accessibility	Probability
High	High	High
High	Moderate	Moderate
Low	High	Low
Low	Low	Low

5.1.3 Probability of Attack

The 'Availability' and 'Accessibility' factors affect each other. For example, if a weapon system is highly available, but the adversary is unable to get access to the RPAS with that weapon system, the overall probability of attack will be assessed as 'low'. Therefore, the probability of attack is derived from the lower rating of either the 'Availability' or 'Accessibility' factor. (cf. Table 3)

5.2 Determining the Vulnerability Level

The 'Survivability Kill Chain' methodology taken from the reference book, 'The Fundamentals of Aircraft Combat Survivability Analysis and Design' by Robert E. Ball, is used as the foundation in determining the vulnerability level for this analysis. The vulnerability level is depicted in the matrix at the end of the respective chapters.

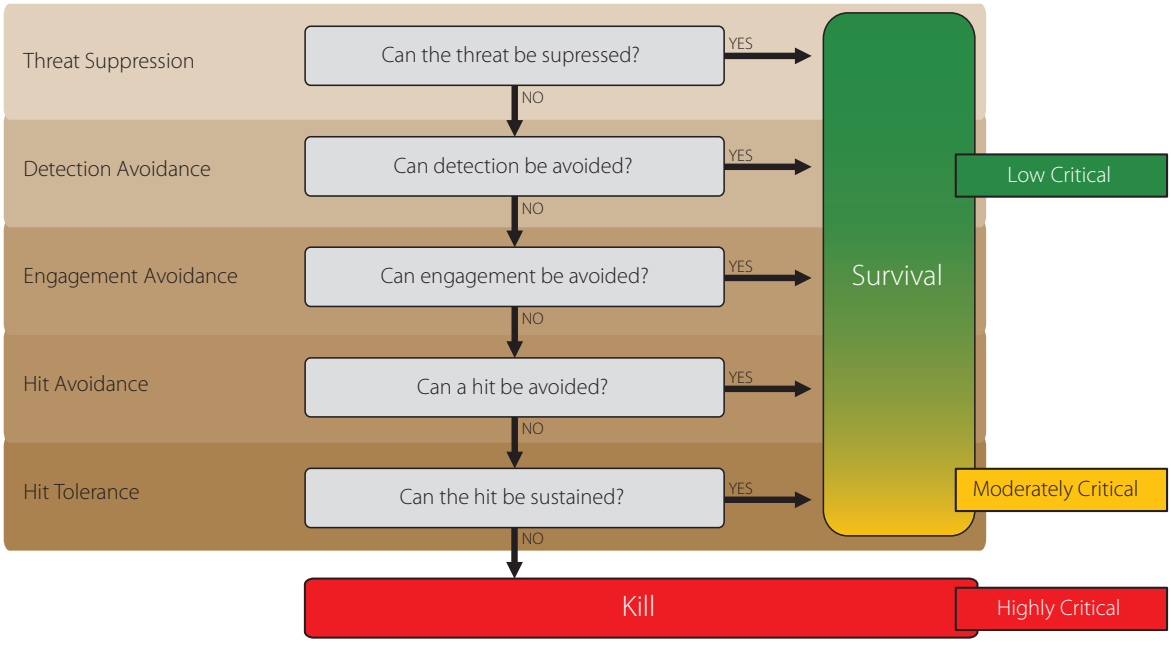
The 'Survivability Kill Chain' defines survival conditions in chronological order, i.e. Threat Suppression, Detection Avoidance, Engagement Avoidance, Hit Avoidance and Hit Tolerance.[1] (cf. Fig. 4)

5.2.1 Survivability Kill Chain Tiers

To assess an RPAS element's vulnerability, the 'Survivability Kill Chain' must run through all five tiers until a survival condition is met. The 'Survivability Kill Chain' tiers are as follows:

5.2.1.1 Threat Suppression. The first tier determines if an active threat is present. If the threat can be suppressed or eliminated in advance, the survival condition is met and the RPAS element survives this tier. Assuming a contested environment typically consists of active threats which cannot be easily suppressed or eliminated, the next tier is always applied for the purpose of this study.

Figure 4 – 'Survivability Kill Chain' by Robert E. Ball (2003).



5.2.1.2 Detection Avoidance. The second tier determines the visibility of the RPAS element to the threat. If the RPAS element can avoid detection, it will survive the engagement. If the RPAS element cannot avoid detection, the next tier is applied.

5.2.1.3 Engagement Avoidance. The third tier determines the possibility that the RPAS element could avoid its engagement in combat activities. If combat can be avoided, the RPAS element will survive the engagement. Otherwise, the next tier is applied.

5.2.1.4 Hit Avoidance. The fourth tier determines the chances that the RPAS element will be affected by the threat (i.e. kinetically, electronically, etc.). If the RPAS element can avoid the threat effects, it survives the engagement. If not, the next tier is applied.

5.2.1.5 Hit Tolerance. The fifth and last tier estimates the magnitude of the attack including effects on other RPAS elements. If the RPAS is able to sustain or absorb the attack, it survives. Otherwise, it's destroyed.

If any of the survival conditions of the first four tiers are met, the vulnerability rating of the respective RPAS element will be 'low' as it is assumed the threat will be completely negated. If the fulfilment of a survival condition is uncertain, the vulnerability rating for that tier is set to 'moderate' and the next tier is applied to identify additional vulnerabilities. If the fifth tier is reached, the vulnerability rating will be defined as 'moderate' if the RPAS is expected to sustain the attack. It is rated as 'high' if the RPAS is expected to be destroyed, rendered inoperable or the mission is expected to fail in any way.

1. Robert E. Ball, Ph.D., The Fundamentals of Aircraft Combat Survivability Analysis and Design, 2nd Edn, Blacksburg, Virginia: Virginia Polytechnic Institute and State University, Oct. 2003.

CHAPTER VI

Threat Identification

'All warfare is based on deception. When confronted with an enemy one should offer the enemy a bait to lure him; feign disorder and strike him. When he concentrates, prepare against him; where he is strong, avoid him.'

Sun Tzu

Deducing the threat dimensions for the RPAS from possible future challenges outlined in chapter IV, they can be subdivided into symmetric, asymmetric and systemic.

A symmetric threat is commonly defined as an attack on a comparable military level (i.e. force on force) which abides by the Laws of Armed Conflict. The most probable adversary that can deliver a symmetric attack is a state actor.

An asymmetric threat is defined in the AAP-06 as a threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting their weaknesses to obtain a disproportionate result.[1]

However, asymmetric attacks are not necessarily less dangerous if aimed at crucial points. Cyber-warfare for example, if directed properly, may have devastating effects to network centric systems. Finally, there are systemic limitations which may have an impact on future RPAS operations as well.

This chapter lists the identified threats to RPAS and outlines which system components will be affected. A successfully conducted attack on one of the system's components usually has an impact on other components as well. The table below illustrates those possible points of attack and their implied effects.

Table 4 – RPAS Threat Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft	■	■				■	■		■
Payload			■	■					
Human Element							■		
Control Element	■	■			■	■	■	■	■
Data Link			■	■			■		
Support Element	■	■	■	■	■	■	■	■	■

■ Targeted Component
■ Secondary Effects

6.1 Surface-Based Air Defence Systems

Surface-Based Air Defence (SBAD) systems are directed against the RPA by physically destroying the airframe, degrading its ability to fly or averting the aircraft from its mission. As a secondary effect, it also degrades the functionality of the carried payload or renders it useless.

6.1.1 General Overview

An SBAD system consists of one or more sensors and a shooting element, e.g. missile launchers or AAA. The sensors usually include wide area coverage by radar and may be reinforced by other active and passive sensors, e.g. Infrared Search and Trackers (IRST) or passive radars for detecting and localizing electronic emissions from aircraft. SAMs are launched toward the area where the target is expected to be. If the SAM is not self-guiding (such as infrared or active radar missiles), the final target data and intercept parameters are sent to the missile via data link during flight. They are further updated before the terminal intercept to respond to evasive manoeuvres and countermeasures dispensed by the target.[2] As outlined in chapter 4.1.1, AD technology has become more widely available to possible future adversaries. This access could be attributed to the exports of Russian and Chinese armament industries or remnants of the Cold War era.

6.1.2 Current SBAD Capabilities

A number of key trends in Russian and Chinese Integrated Air Defence Systems (IADS) that exploit the globalized market for higher technology have been identified. Commercially and strategically driven developmental activity in the Russian and Chinese defence industries have been observed in the previous decade. These are outlined below.[3]

6.1.2.1 High Mobility of all Key Components. Recently developed SAM systems are self-propelled and expected to be capable of changing their firing-positions in less than 5 minutes. Acquisition radars are presumed to be capable of redeploying in less than 15 minutes. Mobility upgrades for legacy systems are also available and exported.[4]

6.1.2.2 Phased Array and Active Array Antenna Technology increasing the effectiveness of SAM en-

gagement radars. Phased arrays are capable of jam resistant, high precision angle tracking and high update rate angle/range tracking of multiple targets.[5]

6.1.2.3 Increased Radar Power and Operation in Lower Frequency Bands to provide counter-stealth capabilities. Operating in lower frequency bands and increasing radar power aids in defeating stealth shaping and coatings optimised for S-band[6] and X-band[7] threats. Most EW self-protection systems jam below the S-band due to antenna size limitations.[8]

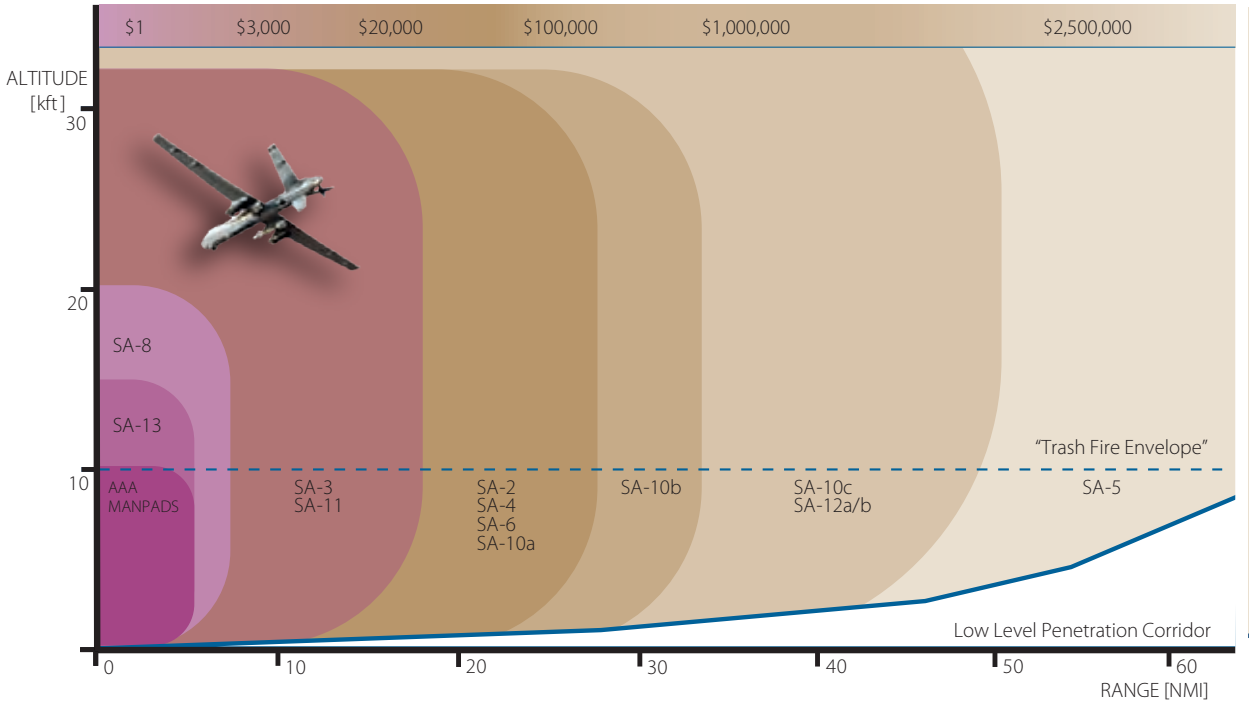
6.1.2.4 Emitter Locating Systems capable of tracking all electromagnetic emissions from the aircraft, including jammers. ISR platforms are especially vulnerable to tracking by such systems due to their extensive radio transmissions while providing imagery and FMV.[9]

In addition, modern SAMs are capable of outmanoeuvring any modern fighter aircraft and can also effectively intercept short- and medium-range ballistic missiles that would be targeting the site. AD sites may be additionally defended by Short-Range Air Defence (SHORAD) which makes the site virtually immune to standoff attack by precision-guided weapons. Modern systems are also designed to operate effectively even when subjected to severe countermeasures and Electronic Attack (EA), which makes them especially difficult to suppress.[11]

6.1.3 Availability of SBAD Systems

Acquisition of sophisticated AD technology and its integration and operation in an IADS require a lot of skill, resources and an infrastructure which can usually only be provided by a state-actor. Therefore, non-state actors and terrorist organizations are very unlikely to acquire AD systems other than MANPADS or perhaps individual non-integrated AD systems. However, in a contested environment, Allied RPAS must be prepared to face a variety of adversary SBAD systems. Due to their widespread proliferation through both legal exports and illegal arms trading, these systems are determined to be highly available to potential future adversaries.

Figure 5 – Air Defence Weapon Envelopes and Estimated Costs per Round.[10]



6.1.4 Accessibility of RPAS by SBAD Systems

Operating in an IADS environment requires a combination of stealth and stand-off capabilities to penetrate adversary SBAD systems or to engage them outside of detection range. To survive in a modern IADS environment, a Radar Cross Section (RCS) in the range from -35 dBsm to -45 dBsm[12] is required as a minimum. This means that only 0.01% to 0.001% of the incoming radar energy will be reflected. Such performance is currently only demonstrated by the F-22A and the B-2A.[13,14,15]

Sophisticated AD systems are highly capable of detecting, tracking and engaging even the most advanced combat aircraft. Therefore, it can be concluded that current MALE and HALE RPAS are no challenge for SBAD systems. Consequently, it is assessed that RPAS are highly accessible to adversary SBAD systems. (cf. Fig. 5)

6.1.5 Threat Assessment

The availability of SBAD systems to possible future adversaries has been assessed as 'high'. The accessibility of Allied RPAS to the threat SBAD systems present has also been assessed as 'high'. Accordingly, the estimated overall threat level for SBAD systems against RPAS and their payload is also 'high'. (cf. Table 5)

1. NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-06), 2012.
2. Defense Update, 'Net Centric Air Defense Systems', 28 Nov. 2004. [Online]. Available: http://defense-update.com/features/du-2-04/SHORAD-netcentric.htm. [Accessed 24 Jun. 2013].
3. Dr. Carlo Kopp, 'Surviving the Modern Integrated Air Defence System', Air Power Australia, 2009. [Online]. Available: http://www.ausairpower.net/APA-2009-02.html. [Accessed 23 Oct. 2013].
4. Ibid.
5. Ibid.
6. The S-band is defined by an IEEE standard for radio waves with frequencies that range from 2 to 4 Gigahertz (GHz). It is used by weather radar, surface ship radar, and some communications satellites.
7. In radar engineering, the X-band frequency range is specified by the IEEE at 8.0 to 12.0 GHz.
8. Ibid. 3.
9. Ibid. 3.
10. Dr. Karlo Kopp, 'GPS Aided Guided Munitions', Air Power Australia, 1996, 2005, 2008. [Online]. Available: http://www.ausairpower.net/TE-GPS-Guided-Weps.html. [Accessed 24 Jun. 2013].
11. Tamir Eshel, 'How Dangerous is the S-300 Syria is About to Receive?', Defense Update, 18 May 2013. [Online]. Available: http://defense-update.com/20130518_how-dangerous-is-the-s-300.html. [Accessed 24 Jun. 2013].
12. dBsm or dB(m2) – decibel relative to one square meter measuring the RCS of a target. The power reflected by the target is proportional to its RCS. Stealth aircraft and insects have negative RCS measured in dBsm, large flat plates or non-stealthy aircraft have positive values.
13. The B-2A, sometimes called the "Stealth Bomber', was designed using sophisticated low-observable technologies that give the aircraft a very low RCS. The B-2A is capable of delivering both conventional and nuclear weapons against heavily defended targets. 'NORTHROP B-2A Fact Sheet', U.S. Air Force, 20 Aug. 2010. [Online]. Available: http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=2757. [Accessed 22 Apr. 2014].
14. The Lockheed Martin F-22A Raptor is the world's first stealthy air dominance fighter. Its radar, weapons control and electronic warfare systems work together as one integrated unit. 'LOCKHEED MARTIN F-22A RAPTOR Fact Sheet', U.S. Air Force, 7 Feb. 2014. [Online]. Available: http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=8389. [Accessed 22 Apr. 2014].
15. Ibid. 3.

Table 5 – SBAD Threat Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

6.2 Combat Aircraft

Combat Aircraft may be directed against all physical components of the RPAS (i.e. the RPA and its payload, the control element and the support element) by delivering kinetic effects to destroy or degrade its functionality. In addition, attacks against the Control or Support Element will most likely result in casualties of friendly RPAS personnel as well. Secondly, combat aircraft may also employ EW capabilities against the RPAS data link to disrupt sensors and communications.

6.2.1 General Overview

Combat aircraft are aircraft designed and used for combat, causing different effects on the enemy through armament or equipment. Combat aircraft include both fixed and rotary wing platforms. Based on the currently available technology, both types of aircraft are capable of posing a credible threat to the air or ground segment of an RPAS if they are properly armed and employ specific TTPs.

6.2.2 Current Combat Aircraft Capabilities

Modern combat aircraft are essentially high performance sensor and weapons platforms, equipped with radar, IRST, Electronic Support Measures including Radar Warning Receivers (ESM/RWR), Electronic Counter Measures (ECM) for signal jamming, Missile Warning System (MWS), Forward Looking Infrared (FLIR) thermal imaging, a laser designator, Air-to-Air and Air-to-Ground Ordnance. Comprehensive sensor suites, the ability to fuse data from multiple sensors and defeat the opponent's sensors, enable modern combat aircraft to engage in 'Beyond Visual Range (BVR)' combat in addition to their established dogfight capabilities.[1]

Threats from combat aircraft to an RPAS arise from the following capabilities:

6.2.2.1 Air-to-Air. Sensors and Weapons enable combat aircraft to detect, track and engage RPA from great distances while being able to generally fly faster and at higher altitudes than current remotely piloted sys-

tems. The RPAS operator's lack of situational awareness compared to the pilot of a manned aircraft makes the combat aircraft superior in air-to-air combat.

6.2.2.2 Air-to-Ground. Combat sensors and weapons enable manned aircraft to engage ground targets from great distances. Adversaries may also be capable of employing Precision-Guided Munitions (PGM) using laser guidance or the GPS unencrypted signals or other global satellite navigation systems like the Russian 'GLONASS' or the Chinese 'BeiDou'[2] to engage RPAS ground components, i.e. the LRU, the GCS and airport or logistic infrastructure hosting the Support Element.

6.2.2.3 Electronic Warfare. ECM equipment may enable manned aircraft to disrupt communication between the RPA and the GCS, rendering the RPA helpless against an impending kinetic attack.

6.2.3 Availability of Combat Aircraft

In 2014, roughly 10,000 combat aircraft and 9,300 combat helicopters are listed in the active duty inventories of air services from more than 120 nations outside the United States and Western Europe. (cf. Fig. 6) Most of th ose countries are equipped with Russian manufactured aircraft. In conclusion, the availability of combat aircraft for possible future adversaries is assessed as 'high'.[3]

6.2.4 Accessibility of RPAS to Combat Aircraft

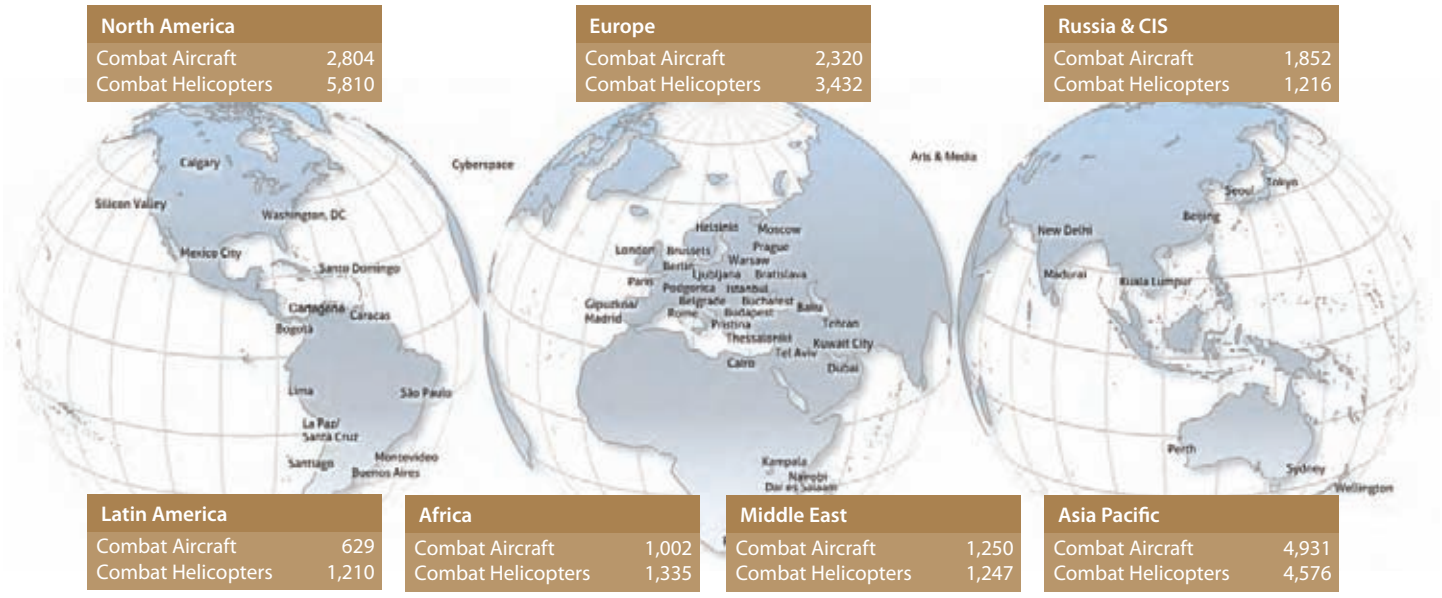
Only nations with strategic air assets have the capability of conducting strategic air strikes. Hence, it is highly unlikely that most potential adversaries will be capable of conducting an attack by combat aircraft on Mission Control Elements (MCE), GCS and communications infrastructure deep inside NATO territory.

Conversely, the RPA, GCS and other supporting equipment deployed to the AOO are highly accessible to enemy aircraft. It can be assumed even legacy combat aircraft with a fairly low level of technology will impose a viable threat to any deployed RPAS due to their capabilities in air-to-air and air-to-ground combat. The accessibility of deployed RPAS elements to adversary combat aircraft is therefore assessed as 'high'.

6.2.5 Threat Assessment

The availability of combat aircraft for possible future adversaries has been assessed as 'high'. The accessi-

Figure 6 – World's Air Forces.[4]



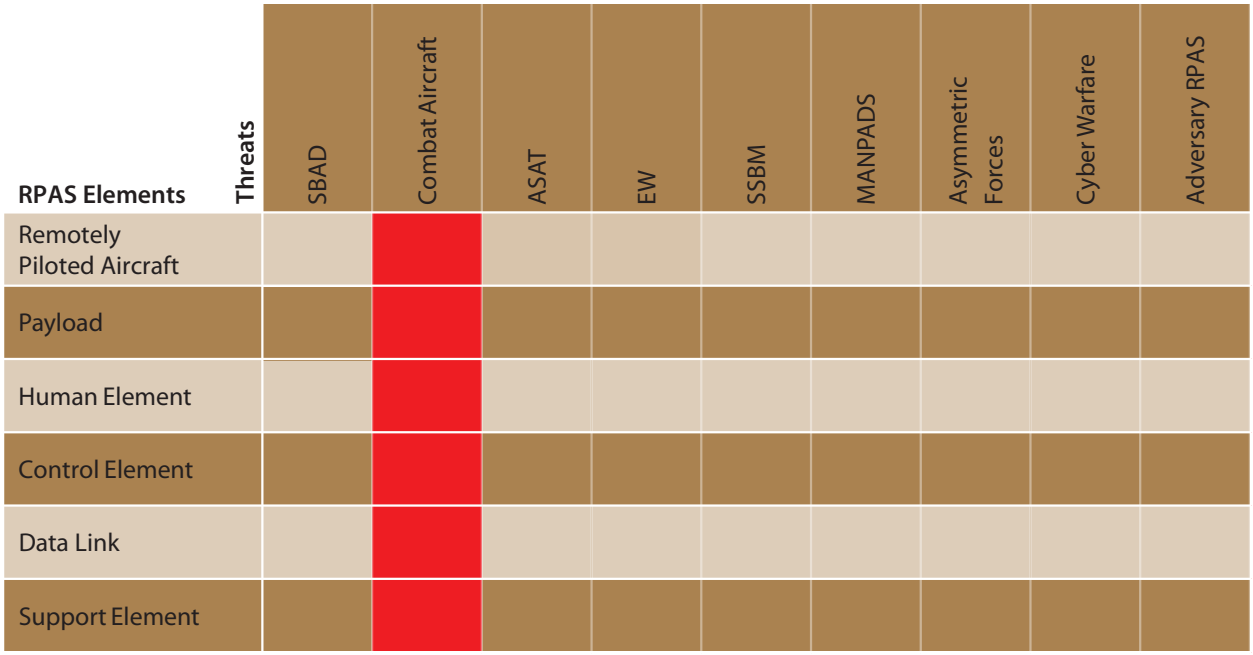


Table 6 – Combat Aircraft Threat Matrix.

bility of home-based RPAS elements to adversary combat aircraft has been assessed as 'low' while it has been assessed as 'high' for the deployed elements. The overall threat assessment takes the higher rating for the deployed RPAS elements into account because the main focus of potential adversaries is estimated to be inside or close to the AOO. Therefore, the overall threat rating for adversary combat aircraft against any element of the RPAS is assessed as 'high'. (cf. Table 6)

1. Dr. Carlo Kopp, 'Measures of Fighter Capability', 1999 - 2005. [Online]. Available: http://www.ausairpower.net/air-superiority-3.html. [Accessed 24 Jun. 2013].
2. .International Committee on Global Navigation Satellite Systems, 'Current and Planned Global and Regional Navigation Satellite Systems and Satellite-based Augmentations Systems', United Nations Office for Outer Space Affairs, New York, 2010.
3. Flightglobal Insight, 'World Air Forces 2014', 2014. [Online]. Available: http://www.flightglobal.com/products/insight/. [Accessed 14 Aug. 2014].
4. Ibid.

6.3 Anti-Satellite Weapons

Current BLOS RPAS operations are entirely dependent on a reliable satellite data link network, provided by either commercial or military satellites. A single Global Hawk, for example, requires 500 Mbps bandwidth, which equates to five times the total bandwidth of the entire U.S. military used during the 1991 Gulf War.[1] This demand cannot be satisfied by military satellites alone. This is why civilian providers have widened their business segment and offer their services for RPAS applications.[2] In 2001, an estimated 60 % of the military's satellite communications during OEF went through commercial satellites.[3] Destroying or disrupting this communications infrastructure would eliminate BLOS RPAS operations. In addition, RPAS navigation also relies on satellite signals, i.e. GPS.

6.3.1 General Overview

Anti-Satellite (ASAT) weapons can be subdivided into Kinetic-Energy Weapons (KEW) or Directed-Energy Weapons (DEW). Both types of ASAT weapons can be ground-, air- or space-based. KEW are usually designed to incapacitate or destroy the satellite while DEW are designed to permanently damage or disrupt the satellite's communications or sensors. ASAT weapons range from direct-ascent and co-orbital interceptors to high-power radio-frequency and high-energy laser emitters. It is also possible to use the Electromagnetic Pulse (EMP) and radiation from a high altitude nuclear detonation to destroy any unshielded satellite in line of sight of the explosion. ASAT attacks can result in a range of damaging effects. For example, they may cause temporary, reversible interference or they may cause permanent destruction. They may target the satellite, the ground station, or any of the links between them.[4] This chapter only discusses the use of KEW and DEW intended to physically degrade or destroy the satellite system or its critical components. The use of non-destructive directed-energy devices is discussed in chapter 6.4 'Electronic Warfare'.

6.3.2 Satellite Orbits

Depending on their purpose, satellites operate in various orbital altitudes, speeds and inclinations. The common

Figure 7 – Orbital Altitudes of Satellites.[18]

orbits are the Low Earth Orbit (LEO), Medium Earth Orbit (MEO) and the Geostationary Orbit (GEO). (cf. Fig. 7)

Satellites in LEO operate at altitudes of between approximately 150 km and 2,000 km.[5] LEO satellites have orbital periods of 90-120 minutes with an orbital speed of up to 7,800 m/s. Due to the relatively low altitude, the satellites field of view is limited and the over flight time is very short. Consequently, a satellite network is required to provide coverage of the entire earth's surface. Therefore this orbit type is most commonly used by satellites which provide observation and not for communication satellites.[6]

Satellites in MEO have altitudes from roughly 2,000 km to 36,000 km. A special type of MEO is the semi synchronous orbit, which has a period of 12 hours, an altitude of roughly 20,000 km and an orbital speed of 3,900 m/s. The United States' GPS, the Russian Glonass navigational satellites and the European Galileo navigation system use this orbit.[7]

Satellites in GEO have an orbital period equal to the Earth's rotation which makes them appear as a fixed point in the sky. The GEO is at roughly 36,000 km with an orbital speed of 3,100 m/s. In GEO three satellites can provide worldwide coverage, excluding the Polar Regions. The area of visibility of the satellite covers about 43% of the Earth's surface. Most SATCOM systems use the GEO, e.g. the U.S. Defense Satellite Communications System (DSCS).[8]

6.3.3 ASAT Capabilities

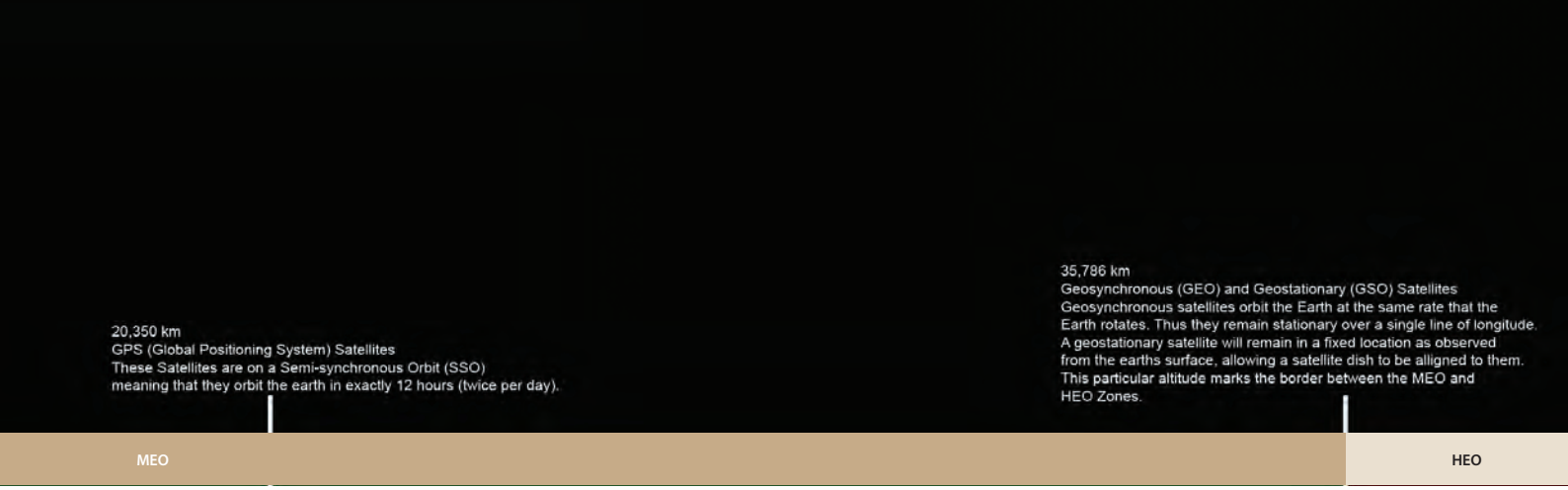
Depending on the satellite's orbit, disruption of satellite communication and navigation signals may be achieved by the following types of attacks.

6.3.3.1 Laser Attacks. High-power lasers can subject satellites in LEO to large amounts of laser energy. The resulting heat can upset the delicate thermal balance of the satellite long enough to damage the satellite's components. If it is sufficiently intense, it can damage a satellite's structure.

6.3.3.2 Ground-Based Kinetic Energy Attacks. Also referred to as Direct-Ascent Attacks, Ballistic missiles can carry a warhead above the atmosphere into LEO and release it in the direction of the target satellite. It is then detonated in the vicinity of the satellite with the objective of creating an inert collision or ejecting a large cloud of pellets into the satellite's path.[9] China (2007) and the US (1980's and 2008) have already demonstrated this capability.

6.3.3.3 Space-Based Kinetic Energy Attacks. Also referred to as 'Space Mines' or 'Kill Vehicles', these types of ASATs are used in all orbits up to GEO and are deployed in space well before they are intended to be used. They are capable of delivering the same effects as Ground-Based Kinetic Energy Attacks, but, by placing them in a crossing orbit, the kinetic energy is much greater.[10] Every enemy satellite in the same orbital regime as the target could potentially be used as a kinetic kill vehicle.

6.3.3.4 High-Altitude Nuclear Explosion. The intense EMP resulting from a nuclear explosion would likely destroy all unshielded satellites in LEO that are in line of sight. In addition, the explosion would generate a persistent radiation environment (months to years) that would slowly damage unshielded satellites.[11]



6.3.4 Availability of ASAT Weapons

ASAT weapons are most likely available to state-actors only. Depending on whether the potential adversary is a space faring or a non-space faring nation, the availability of certain ASATs and the effective employment of those ASATs may differ significantly. As only a handful of nations possess space capabilities, the availability of ASAT weapons to possible future adversaries is assessed as 'low'.

6.3.5 Accessibility of Satellites to ASAT Weapons

Critical military satellite infrastructures such as GPS or the U.S. DSCS use either semi synchronous or geostationary orbits[12] and are well out of range for any ground-based KEW or DEW. Only the LEO satellites are currently in range of these types of weapons. However, it may take a significant number of ASATs to disrupt those networks, as they typically consist of a very large number of satellites, e.g. Iridium (66 satellites) or Globalstar (32 satellites).

Table 7 – ASAT Threat Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

Satellites in LEO are well within range of ballistic missiles and possibly in range of non-space faring nations. Conversely, access to the MEO and GEO, as well as employment of any space-based weapon system, is limited to space-faring nations only, as it requires technology which exceeds that of normal ballistic missiles. Nations currently capable of launching satellites into space are the United States, Russia, China, India, Japan and the European Union.[13,14] However, it is questionable whether space-faring nations which have their own interests in space exploitation are willing to destroy satellites and cause orbital debris which would cause a cascading effect through space.[15] For example, China successfully conducted an ASAT weapon test in 2007 by destroying a Chinese weather satellite on an 850 km orbit. The event created more than 3,000 traceable debris fragments. This cloud of debris (ranging from 200 km up to 4,000 km) endangers other spacecraft orbiting at these altitudes with the potential of catastrophic damage.[16]

Delivering high intensity laser energy to satellites in LEO requires a powerful laser, a large mirror for focusing the beam and adaptive optics to reduce atmospheric effects. Satellites in GEO are protected from structural damage by ground-based lasers due to their extreme altitudes. Analysis of laser attacks reveals that kilowatt-class lasers are required as a minimum to inflict substantial damage on unshielded satellite components in LEO. Developing a laser ASAT system for these types of attacks is difficult and expensive. Thus, such attacks are determined to be restricted to technically sophisticated countries.[17]

The accessibility of satellite systems that support RPAS operations to threats from potential adversaries is assessed as 'low'. This is because these systems typically operate in geostationary orbit outside the range of current ASAT weapons. Satellites operating in lower orbits (e.g. GPS) may be more accessible, but are generally part of a constellation which must be destroyed in its entirety to render it inoperable. Therefore, the overall accessibility rating of the RPAS data link is still assessed as 'low'.

6.3.6 Threat Assessment

The availability of ASAT weapons as well as the accessibility of satellites providing the data link connectivity for RPAS to potential future adversaries have both been assessed as 'low'. Therefore, the estimated overall probability of attack for ASAT weapons against the RPAS is 'low'. (cf. Table 7)

1. Jeremiah Gertler, 'U.S. Unmanned Aerial Systems', Congressional Research Service, 2012.
2. Telesat, Briefing on Unmanned Aerial Vehicles (UAVs), Mar. 2011.
3. 'U.S. Government Market Opportunity for Commercial Satellite Operators: For Today or Here to Stay?', Futron Corporation, 29 Apr. 2003.
4. David Wright, Laura Grego, and Lisbeth Gronlund, 'The Physics of Space Security', American Academy of Arts and Sciences, Cambridge, MA, 2005.
5. Different sources may use different altitude 'bands'.
6. Ibid. 4.
7. Ibid. 4.
8. Mission and Spacecraft Library, 'Defense Satellite Communications System III (DSCS III)', NASA, [Online]. Available: http://space.jpl.nasa.gov/msl/QuickLooks/dscs3QL.html. [Accessed 29 Oct. 2013].
9. Ibid. 4.
10. Ibid. 4.
11. Ibid. 4.
12. Clayton K.S. Chun, Chris Taylor, Defending Space, U.S. Anti-Satellite Warfare and Space Weaponry, Osprey Publishing Limited, 2006.
13. Ibid. 4.
14. Ibid. 4.
15. Jan Kallberg, Ph.D., 'Designer Satellite Collisions from Covert Cyber War', Strategic Studies Quarterly, pp. 124-136, Spring 2012.
16. James Dunnigan, 'The Chinese Conspiracy in Orbital Space', 21 Jun. 2013. [Online]. Available: http://www.strategypage.com/dls/articles/The-Chinese-Conspiracy-In-Orbital-Space-6-21-2013.asp. [Accessed 24 Jun. 2013].
17. Ibid. 4.
18. Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/File:Orbitalaltitudes.jpg. [Accessed 4 Nov. 2013].

6.4 Electronic Warfare

'The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a warfighting domain on par with – or perhaps even more important than – land, sea, air, and space. Future wars will not be won simply by effectively using the EM spectrum and cyberspace; they will be won within the EM-cyber domain.'

Admiral Jonathan Greenert,
Chief of US Naval Operations

Electronic Warfare (EW) is defined as 'military action to exploit the electromagnetic spectrum encompassing: the search for, interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum, and actions to ensure its effective use by friendly forces.'[1] In contrast to kinetic weapons, EW usually does not cause permanent physical damage to its target. EW capabilities can be directed against RPAS data links (cf. Fig. 8) in order to disrupt the communications between the GCS and the RPA or to disrupt GPS signals. Either of these could disable RPAS operations entirely. Ground troops may also have transmissions sent directly from the RPA disrupted.

6.4.1 Principal Types of Electronic Attack

RPAS consist of three communication nodes. These are the RPA, the satellite and the GCS. Signals sent from the GCS to the satellite are referred to as the uplink, those from the satellite to the GCS as the downlink. There are primarily three ways to interfere with electromagnetic signals. They are 'jamming', 'spoofing' and 'meaconing'.

6.4.1.1 Jamming refers to disrupting communication by overpowering the signals being sent from a transmitter to a receiver by using a signal at the same frequency, but with higher power. The jamming signal overloads the targeted frequencies with so much

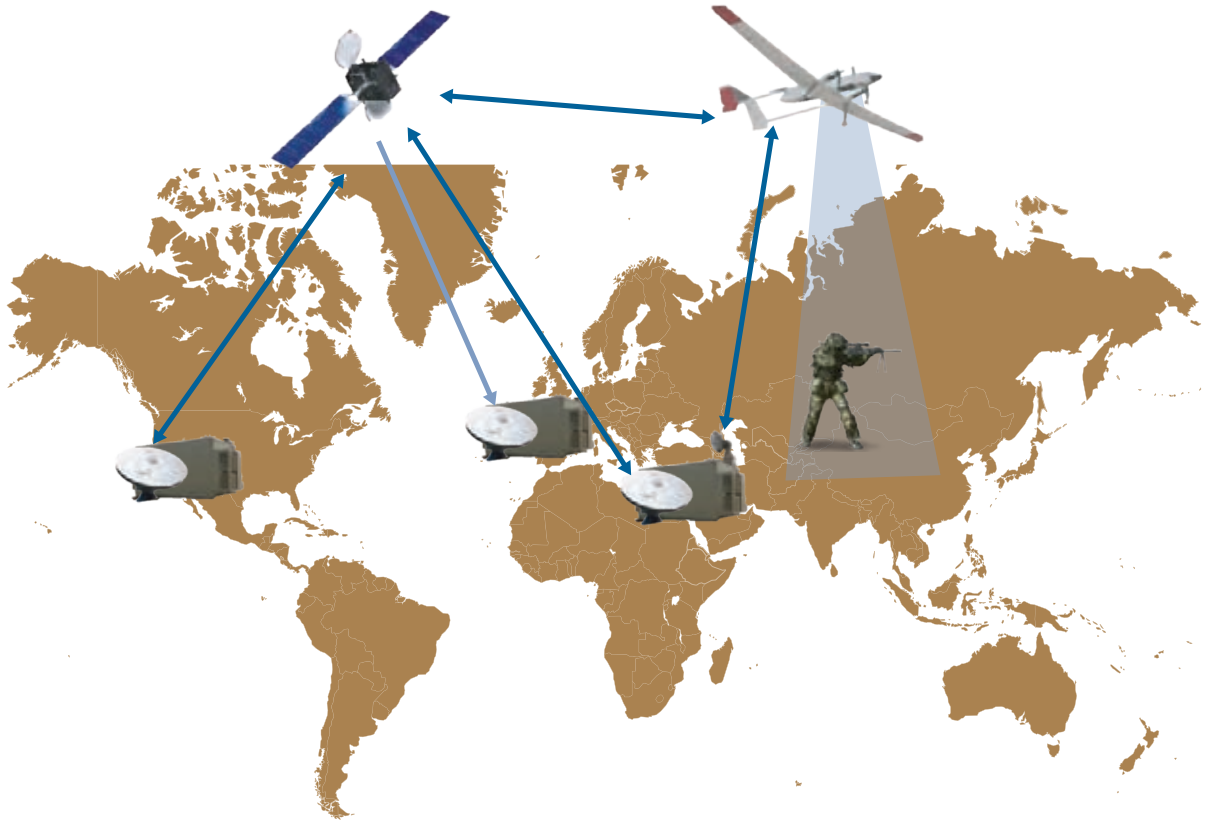


Figure 8 – RPAS Data Links.

electronic noise that communications cannot get through to the intended receivers.[2,3,4,5] Simple jammers are inexpensive to make or to purchase. For example, GPS jammers available on the commercial market can reportedly interfere with receivers 150–200 km away. Additionally, instructions for constructing an inexpensive GPS jammer are currently available on the Internet.[6] A document allegedly written by al-Qaeda on how to defend against RPAS claimed they used legacy Russian radio transmitters to successfully disrupt satellite communications in the local area.[7]

6.4.1.2 Spoofing mimics the characteristics of the original signal so the user accepts the spoofed signal instead of the correct one. Spoofing devices are technically complex since they must be able to mimic the original satellite signal in detail. In spite of this, GPS simulators that can spoof GPS receivers can also be purchased commercially.[8]

6.4.1.3 Meaconing is a composite term from 'mislead' and 'beacon'. It refers to the interception and delayed rebroadcast of navigation signals. Global Navigation Satellite Systems (GNSS) operate on the basis of time of arrival ranging. Introducing a signal delay falsifies the user's computed position which results in location errors. In the worst case, the RPA can be misdirected or forced to land in an enemy controlled area. Unfortunately, even encrypted military GPS signals are not entirely protected from sophisticated meaconing attacks.[9,10,11,12]

6.4.2 Accessibility of RPAS Receivers to Electronic Attack

EW does not stop the transmitter from sending its signals. EW attacks are always directed against the receiver to prevent it from receiving the intended signals. To be effective, the attacker must be within the area from

which broadcast signals originate. It must also be able to direct its spurious signal to the intended receiver. As common directional antennas are usually only able to accept signals from roughly their boresight direction, the positioning of the attacking transmitter is critical to ensure the signal won't be filtered out by the targeted receiver.

The RPAS contains several receivers within the different elements of the remotely piloted system. Depending on the receiver's alignment relative to the other components' transmitters, an attacker must be positioned in a very specific location to successfully conduct an EW attack.

6.4.2.1 Downlink. The receiving antennas of the RPA and the GCS are aligned to face a satellite usually in GEO. To inject a spurious signal into the antennas, the attacker must be positioned at a higher altitude than the RPA or GCS and be aligned between the RPA/GCS and satellite. Such an EW attack may be conducted from an aircraft or another satellite. Depending on the GCS' antenna alignment, an attack may also be conducted from an appropriately high point on the Earth's surface. For both cases, since the attacker is located several hundreds to a thousand times closer to the receiver than the satellite, less power is needed to override the original satellite signal.

6.4.2.2 Uplink. The receiving antenna of the satellite is aligned to face the location of the ground-based transmitter (i.e. RPA or GCS). A geostationary satellite can usually cover approximately one-third of the Earth's surface in its field of view. Any location within the satellite's coverage area can be used to conduct an EW attack on an unprotected satellite's uplink. Military satellites usually use phased-array antennas and nullifying techniques to reject signals from transmitters outside the specified area. Therefore, the attacker must be located near the AOO. As the attacker's signal must travel the same distance to the satellite as the target, the one with more power will

Table 8 – EW Threat Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

displace the genuine signal when it arrives at the satellite's receiver.

Due to the alignment of the RPA's receiving antenna, accessibility of the aircraft to adversary EW is estimated to be quite low. In contrast, the RPAS ground elements as well as the geostationary satellites are assessed as highly accessible to electromagnetic interference. Disrupting only one communications element of the RPAS will severely impact overall functionality. Consequently, the accessibility of RPAS data links to adversary EW is estimated as 'high'.

6.4.3 Availability of EW Equipment

EW equipment comes in a variety of forms. From low-cost commercial to high-grade military products, this capability is even available to non-state adversaries. Simple jammers can be obtained for less than $100 or be home built using detailed instructions from the internet. It has been assessed that even these simple devices work well against unprotected receivers.[13] Non-military satellite ground stations may also be used for EW by directing their transmissions against enemy satellites.[14] Traditionally, EW has always been characterized by a type of arms race. Unfortunately, EW attack has historically required less sophisticated technology than is needed to defend against that attack.[15] Because of this, the availability of EW equipment to potential future adversaries is assessed as 'high'.

6.4.4 Threat Assessment

The availability of EW equipment to potential future adversaries as well as the accessibility of RPAS data links to electromagnetic interference have both been assessed as 'high'. Therefore, the overall probability of EW attacks against Allied RPAS is estimated to be 'high'. (cf. Table 8)

1. NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-06), 2012.
2. David Wright, Laura Grego, and Lisbeth Gronlund, 'The Physics of Space Security', American Academy of Arts and Sciences, Cambridge, MA, 2005.
3. 'Iran government jamming exile satellite TV', Iran Focus, 14 Jul. 2005. [Online]. Available: http://www.iranfocus.com/en/?option=com_content&task=view&id=2852. [Accessed 25 Jun. 2013].
4. Peter de Selding, 'Libya Pinpointed as Source of Months-Long Satellite Jamming in 2006', Space News, 9 Apr. 2007. [Online]. Available: http://www.space.com/3666-libya-pinpointed-source-months-long-satellite-jamming-2006.html. [Accessed 25 Jun. 2013].
5. Loren B. Thompson, Ph.D., 'Lack of Protected Satellite Communications Could Mean Defeat for Joint Force In Future War', Lexington Institute, 14 Apr. 2010. [Online]. Available: http://www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war?a=1&c=1171. [Accessed 25 Jun. 2013].
6. Ibid. 2.
7. al-Qaeda, Abdallah bin Muhammad, al-Qaeda paper on drones found in Timbuktu, Mali, 17 Jun. 2011.
8. Ibid. 2.
9. Mark L. Psiaki, Steven P. Powell, Brady W. O'Hanlon, 'Correlating Carrier Phase with Rapid Antenna Motion', 1 Jun. 2013. [Online]. Available: http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/. [Accessed 30 Oct. 2013].
10. Daniel Marnach, Sjouke Mauw, Miguel Martins, Carlo Harpes, 'Detecting Meaconing Attacks by Analysing the Clock BIAS of GNSS Receivers', itrust consulting s.à r.l. & University of Luxembourg, Jun. 2013.
11. Melissa Mixon, 'Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV', The University of Texas at Austin, 2012. [Online]. Available: http://www.ae.utexas.edu/news/archive/2012/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav. [Accessed 25 Jun. 2013].
12. John Roberts, 'GPS at risk from terrorists, rogue nations, and $50 jammers, expert warns', FoxNews.com, 23 Feb. 2012. [Online]. Available: http://www.foxnews.com/tech/2012/02/23/gps-emerging-threat/. [Accessed 25 Jun. 2013].
13. NovAtel White Paper on Anti-Jam Technology, 'Mitigating the Threat of GPS Jamming', novatel.com, Jun. 2012.
14. Pierluigi Paganini , 'Hacking Satellites . . . Look Up to the Sky', INFOSEC Institute, 18 Sep. 2013. [Online]. Available: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/. [Accessed 08 Jan. 2014].
15. Ibid. 2.

6.5 Surface-to-Surface Ballistic Munitions

Surface-to-Surface Ballistic Munitions (SSBM) can be directed against the ground-based infrastructure required to maintain, launch and recover the RPA. This consists of the Support Element (LRU and GCS equipment) as well as the hangars and runways for the RPA. SSBMs may be also directed against RPA undergoing maintenance, before launch or after recovery.

6.5.1 General Overview and SSBM Capabilities

SSBM may range from homemade shells fired by makeshift mortars up to sophisticated artillery guns, rocket launchers and ballistic missiles with high range and precision.

6.5.1.1 Makeshift Mortars. Metal cylinders or tubes can be turned into very simple, but well-functioning improvised mortars. Depending on the munitions used, their range may not necessarily be less than those of military grade mortars. Usually improvised mortars lack the precision of their professionally built counterparts.

6.5.1.2 Military Mortars have a maximum effective range of roughly eight kilometres. Modern systems are usually as accurate as artillery guns while older systems may have a larger Circular Error Probable (CEP) and need observer adjustment.[1]

6.5.1.3 Artillery Guns have a maximum effective range from 25 km up to 40 km with extended range munitions.[2] Modern artillery guns are capable of autonomous ballistic trajectory computation delivering precisely predicted fire without the necessity for observer adjustment.

6.5.1.4 Rocket Launchers range from man-portable RPGs with a range hardly more than 1,000 m to self-propelled multiple rocket launchers with ranges up to 100 km depending on rocket type and calibre.

Figure 9 – Global Ballistic Missile Arsenals outside NATO.[11]

6.5.1.5 Ballistic Missiles can be subdivided into short (less than 1,000 km), medium (1,000-3,000 km) and intermediate (3,000-5,500 km) range missiles. Missiles with maximum effective ranges greater than 5,500 km are considered Intercontinental Ballistic Missiles (ICBM).[3,4]

With some exceptions, SSBM typically carry an explosive payload to deliver a kinetic effect on their target (blast, heat and fragmentation). SSBM may detonate either in an air-burst or ground-burst mode to damage the target's exterior or with a delayed fuse which permit it to penetrate the target and destroy it from within.

6.5.2 Availability of SSBM

Next to small arms, RPGs and mortars have been the weapons of choice of most non-state actors in recent conflicts. Almost 50 countries have manufactured one or more types of mortars, making it the most widely produced light weapon worldwide. Insurgent and terrorist groups have used mortars with deadly effect in almost all conflicts since the Second World War. Mortars have found favour among these groups given their wide availability, longevity, ease of operation, and low cost. Regardless, currently no non-state armed group is known to use or possess guided mortars.[5]

Artillery guns, rocket launchers and ballistic missiles are usually found only in the inventories of state-actors. Nearly 40 countries have produced or still produce artillery systems.[6] Towed guns, howitzers and rocket launchers are an inherent part of almost any modern army. Additionally, the threat from short-, medium- and intermediate-range ballistic missiles (SRBM s, MRBM s and IRBM s) is growing steadily. (cf. Fig. 9) In 2011, excluding the inventories of Russia and China, the total number of ballistic missiles outside NATO was estimated more than 5,900.[7,8,9] Correspondingly, the availability of SSBM to a potential future adversary is assessed as 'high'.

6.5.3 Accessibility of RPAS to SSBM

Any personnel and material supporting RPAS operations in the AOO will most likely be accessible to the effects of SSBM as long as it is in firing range of those weapons. Adversary target acquisition of RPAS infrastructure such as shelters, runways and GCS satellite dishes may also be quite easy as they usually cannot be hidden from view.

Satellite antennas needed for communication between the GCS, the satellite and the RPA may be the most valuable targets for an adversary as they are inherently sensitive components and vulnerable to fragmentation and blast.

6.5.4 Threat Assessment

SSBM inflict serious damage to any unprotected RPAS ground equipment and personnel inside the AOO. Nations with regular armed forces are likely to be capable of delivering high precision surface-to-surface strikes. Ballistic missiles may also deliver kinetic effects outside the AOO (such as against a

neighbouring nation that hosts logistics or airport infrastructure in support of RPAS operations.) Additionally, attacks with RPGs and mortars are often conducted by insurgents and terrorist groups as they are easy to hide, transport and set up for a quick 'hit and run' ambush. Although not very precise, they may inflict serious damage to unsheltered personnel and material.[10] As both the availability of SSBM to possible future adversaries as well as the accessibility of all RPAS ground components to those weapons has been assessed as 'high', the overall probability of attacks by SSBM is estimated as 'high'. (cf. Table 9)

1. 'Small Arms Survey Research Notes Number 2', Graduate Institute of International and Development Studies, Geneva, Feb. 2011.
2. John M. Matsumura, Randall Steeb, John Gordon IV, 'Assessment of Crusader, The Army's Next Self-Propelled Howitzer and Resupply Vehicle', RAND, Washington, D.C., 1998.
3. 'Intercontinental Ballistic Missiles', Federation of American Scientists, 25 Oct. 1998. [Online]. Available: http://www.fas.org/nuke/intro/missile/icbm.htm. [Accessed 04 Nov. 2013].
4. Colonel Robert P. Wade, 'Missile Defense Capability: Can We Effectively Counter the Threat?', United States Army War College, Carlisle, PA, 2012.
5. Ibid. 1.
6. 'List of artillery by country', Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/List_of_artillery_by_country. [Accessed 04 Nov. 2013].
7. 'The Threat', Missile Defense Agency, [Online]. Available: http://www.mda.mil/system/threat.html. [Accessed 05 Nov. 2013].
8. U.S. Department of Defense, 'Ballistic Missile Defense Review (BMDR) Fact Sheet', 2010.
9. Andrew Wade, 'Global Ballistic Missile Arsenals', Center for American Progress, 08 May 2007. [Online]. Available: http://www.americanprogress.org/issues/security/news/2007/05/08/3082/global-ballistic-missile-arsenals-2007/. [Accessed 05 Nov. 2013].
10. Jerry Meyerle, Carter Malkasian, 'Insurgent Tactics in Southern Afghanistan', CNA's Center for Naval Analyses, Aug. 2009.
11. Andrew Wade, "Global Ballistic Missile Arsenals," Center for American Progress, 8 May 2007. [Online]. Available: http://www.americanprogress.org/issues/security/news/2007/05/08/3082/global-ballistic-missile-arsenals-2007/. [Accessed 5 Nov. 2013].

Table 9 – SSBM Threat Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

6.6 Man-Portable Air Defence Systems

MANPADS are lightweight anti-aircraft weapons. Like any AD, MANPADS are directed against the (remotely piloted) aircraft by physically destroying the airframe or degrading its ability to fly. As a secondary effect, it also degrades the functionality of the carried payload or renders it useless.

6.6.1 General Overview

MANPADS are surface-to-air missiles that can be fired by an individual or a small team of people against aircraft.[1] MANPADS typically consist of three components: a disposable carriage and launch tube, containing a single missile; a disposable thermal battery or battery-coolant unit, which provides electrical power to the system prior to firing and a grip-stock assembly. Fully assembled, a MANPADS typically weighs 15–20 kg and is less than 2 metres in length. These factors make the weapon relatively easy to transport and conceal. Some of the most commonly proliferated MANPADS can easily fit into the trunk of an automobile.[2,3]

6.6.2 MANPADS Capabilities

Depending on their type, MANPADS are effective only over ranges less than about seven kilometres and at an altitude of less than 15,000 ft above their launch point. The majority of MANPADS are thermally-guided and the targeted aircraft must be within view of the operator. Because MANPADS are intended to be carried and deployed rapidly by ground forces, they are low cost, light, compact and mobile. The amount of explosive in a MANPADS missile is quite small. However a combination of effects, including blast, fragmentation and the energy of the missile hitting the aircraft at high speed can have a significant destructive impact. They require only a single operator to use, and can be very effective against low or slow aircraft.[4]

While MANPADS ranges and altitudes are modest compared to larger missile systems, they are large

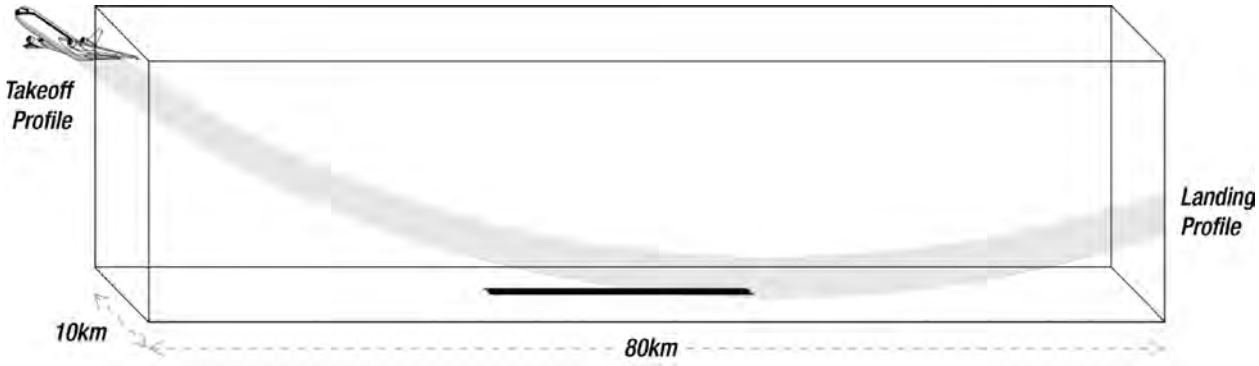


Figure 10 – Approximate MANPADS Engagement Envelope Around an Airport Runway.[10]

enough to have significant implications for the safety of aircraft taking off or landing. Figure 10 shows the approximate area around a runway from which a MANPADS could be fired with some likelihood of striking an aircraft.[5]

The same characteristics that make MANPADS suitable for battlefield use also make them useful to terrorist groups and insurgents. They have been used in terrorist attacks against civilian aircraft in a number of documented cases and have been employed as effective weapons in Afghanistan and Iraq.[6]

6.6.3 Availability of MANPADS

MANPADS have been exported widely and licensed for production in a number of countries. It is estimated that worldwide inventories include between 500,000 and 750,000 MANPADS developed or produced under licence by a number of countries. Most are part of their national military inventories while others have been safely decommissioned. However, some are known to have been illegally traded to third parties, including non-state actors.[7]

Non-state actors are able to acquire MANPADS in a variety of ways, including from grey/black markets, arms dealers, front companies, trans-shipment, intermediaries, end-use certificate falsification and corrupt government officials. Terrorist groups and other non-state actors are demonstrating increasingly sophisticated and aggressive approaches towards acquiring MANPADS.[8] Therefore, it is assessed that non-state armed groups as well as state-actors are likely to possess MANPADS or at least have the ability to acquire them when needed. Therefore, the estimated availability rating is 'high'.

6.6.4 Accessibility of the RPAS to MANPADS

Like most weapon systems, MANPADS require a basic level of operator skill to be used effectively. The batteries generally provide power for less than a minute, and the operator must be able to acquire a target and launch the missile before the battery runs out. This can be challenging without continued practice. Many of the MANPADS on the black market are early-generation designs that require a rear-aspect shot to have a high probability of locking onto the target. This limits the ability of the shooter to find a suitable firing position. This may explain why hit rates in Iraq and Afghanistan have been low compared to the number of missiles fired.[9]

Engaging an RPA is only possible if it is in the MANPADS operator's field of view. RPA are usually more difficult to detect due to their smaller size and lower noise level as compared to a manned combat aircraft. At decent operating altitudes, MANPADS cannot successfully engage RPA. Although low speed, limited manoeuvrability and lack of protective measures could make RPA highly susceptible to MANPADS attacks, based on the historical successful engagement rates in recent operations, the estimated accessibility of the RPA to MANPADS is determined to be 'moderate'.

6.6.5 Threat Assessment

The threat from MANPADS can be reduced to zero by flying at operating altitudes outside their envelope. This should be the case with most MALE RPAS. The probability of the RPAS being successfully engaged by a MANPADS is significantly higher during launch and recovery operations. This is because the RPA will be within the engagement zone of the MANPADS. Force protection measures applied to secure military airport infrastructure and its surroundings should make this risk negligible. As the availability of MANPADS to possible future adversaries has been estimated as 'high' and the accessibility of the RPA and its carried payload to those weapons has been assessed as 'moderate', the overall probability of attacks by MANPADS is estimated as 'moderate'. (cf. Table 10)

1. 'MANPADS at a Glance', Arms Control Association, Mar 2013. [Online]. Available: https://www.armscontrol.org/factsheets/manpads. [Accessed 16 Jun. 2014].
2. Australian Department of Foreign Affairs and Trade, Australian Strategic Policy Institute (ASPI), Man-Portable Air Defence Systems (MANPADS) - Countering the Terrorist Threat, Jun. 2008.
3. U.S. Department of State, Bureau of Political-Military Affairs, 'MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems', 27 Jul. 2011. [Online]. Available: http://www.state.gov/t/pm/rls/fs/169139.htm. [Accessed 05 Nov. 2013].
4. Ibid. 2.
5. Ibid. 2.
6. Ibid. 2.
7. Ibid. 2.
8. Ibid. 3.
9. Ibid. 2.
10. Ibid. 2.

Table 10 – MANPADS Threat Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1


©UN Photo


© MCD, Sgt Sjoerd Hilckmann

6.7 Asymmetric Forces

Asymmetric force may be directed towards soft components of the RPAS accessible to armed groups, terrorists and other non-state actors. Asymmetric force may also be employed by Special Operations Forces (SOF) as part of the adversary's armed forces. As the airborne RPA is usually far out of range to engage and the Control Element is usually well secured by its surrounding military compound, asymmetric forces may opt to attack RPAS operators, contractors or supporting companies in the non-military or domestic environment.

6.7.1 General Overview

Attacks by SOF against RPAS personnel outside their operational location are considered legitimate. Armed groups engaging in combat without the legitimate authority of a recognized state are considered illegal or unlawful combatants and violate International Humanitarian Law (IHL) even if they attack legitimate military targets. Violence directed indiscriminately against civilians is commonly known as terrorism, although there is neither an academic nor an international legal consensus regarding the definition of the term itself.[1,2,3,4] Aside from the legal considerations, (which are not within the scope of this paper), all aforementioned groups may impose a viable threat to RPAS personnel. The domestic (civilian) environment of RPAS personnel may also be affected, either intentionally or through collateral damage.

6.7.2 Possible Targets of Asymmetric Attacks

The following list gives examples of targets vulnerable to asymmetric attacks in the military and non-military environment.

6.7.2.1 Individuals. Attacks may be directed against 'on-duty' or 'off-duty' personnel such as pilots, sensor operators or contractors. They may be identified by traditional intelligence means, but also by exploiting social media and the internet. Once identified, the individual may be tracked until a window of opportunity to conduct an assault becomes available.

6.7.2.2 Domestic Environment. Attacks may be directed against the targeted individual's 'domestic environment' as well, such as family, relatives, neighbours or friends. It may take longer to conduct additional intelligence on the domestic environment, but it offers the possibility for blackmailing the target. The target's domestic environment may also be exposed to lethal danger if an attack is conducted on the targeted individual.

6.7.2.3 Associated Companies. Non-military companies that provide services such as satellite communications may also be subject to bombing or may suffer attacks against their employees. An attacker may opt for engaging the civil satellite ground station rather than taking the risk of an attack against a well secured military GCS.

6.7.2.4 Unhardened Ground Installations. Soft targets such as parked RPA or satellite dishes may be deliberately attacked by asymmetric forces. This would obviously have a negative impact on RPAS operations being initiated against enemy forces.

6.7.3 Threat Assessment

The probability of accessing exposed ground–based RPAS components such as satellite antennas or unprotected RPA is assessed as 'moderate'. Although they are easy to spot from a distance and may be engaged from outside the military compound with RPGs or sniper rifles, they most certainly will have robust force protection measures in place to protect them. It is more difficult to identify a GCS shelter than it is to identify the more exposed RPAS components. Hence, the rating is reduced to 'low'. Access to 'on-duty' RPAS personnel is assessed accordingly as either 'moderate' or 'low' depending on whether they are working inside protected areas.

RPAS personnel, based in their home country, usually work in shifts. In contrast to their deployed colleagues,

Table 11 – Asymmetric Forces Threat Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

they may commute between their home and assigned base and switch back and forth between combat operations during the day and family life in the evening.[5,6,7] Military personnel usually enjoy the security of a well-guarded base when on-duty. Unless their family lives in 'on-base' quarters, their family homes are most likely unprotected. The same is probably true for employees of associated civilian companies. Unprotected civilian environments can be assessed as highly susceptible to asymmetric forces. Additionally, sophisticated weapons are not required to kill an individual, which means possible attackers can choose from a variety of available threats to suit their needs. The resulting probability of an asymmetric attack against RPAS personnel in their domestic environment is considered 'high'. (cf. Table 11)

1. 'Definitions of terrorism', Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Definitions_of_terrorism. [Accessed 1 Jul. 2013].
2. 'Article 44 — Combatants and prisoners of war', in Protocol additional to the Geneva Conventions of 12th Aug. 1949 and relating to the Protection of Victims of International Armed Conflicts, 1977.
3. United States Department of State, Bureau of Counterterrorism, Country Reports on Terrorism 2012, May 2013.
4. Dean C. Alexander, 'Al-Qaeda and al-Qaeda in the Arabian Peninsula-Inspired, Homegrown Terrorism in the United States', in Defence Against Terrorism Review (DATR), NATO Center of Excellence - Defence Against Terrorism, 2012, pp. 31-46.
5. Denise Chow, 'Drone Wars: Pilots Reveal Debilitating Stress Beyond Virtual Battlefield', livescience.com, 05 Nov. 2013. [Online]. Available: http://www.livescience.com/40959-military-drone-war-psychology.html. [Accessed 06 Nov 2013].
6. Jefferson Morley, 'Boredom, terror, deadly mistakes: Secrets of the new drone war', Salon Media Group Inc., 03 Apr. 2012. [Online]. Available: http://www.salon.com/2012/04/03/boredom_terror_deadly_mistakes_secrets_of_the_new_drone_war/. [Accessed 06 Nov. 2013].
7. Mark Bowden, 'The Killing Machines - How to think about drones', The Atlantic, 14 Aug. 2013. [Online]. Available: http://www.theatlantic.com/magazine/archive/2013/09/the-killing-machines-how-to-think-about-drones/309434/. [Accessed 06 Nov. 2013].

6.8 Cyber-Warfare

兵之形，避實而擊虛

'Avoid strength, attack weakness.'

Sun Tzu, The Art of Warfare

It is well known that a system is only as effective as its weakest link. In an increasingly integrated electronic-based and connected world, the ability to effectively command and control force packages is highly dependent on the electro-magnetic spectrum and related computing and sensing technologies. The RPAS is not exempt from this dependency. With this dependency comes vulnerability and risk to RPAS effectiveness.

Cyber-warfare is conducted in a non-physical environment created by computer systems, usually referred to as cyberspace. Although there are a wide range of definitions from the dictionary to state-approved terms, they commonly agree the core of cyberspace consists of globally connected networks of hardware, software and data.[1] NATO has yet to formally recognize 'Cyber' as a domain or agree on a definition. For the purpose of this study, a cyber-attack may be defined as the unauthorized penetration of computer and communications systems belonging to individuals or organizations for the purpose of espionage and information theft, in order to damage or disrupt the functioning of these systems or to damage other systems dependent on them, even to a point of causing actual physical damage.[2]

6.8.1 General Overview

Cyberspace is rapidly becoming a central focus for future wars and hostile actions undertaken by a variety of adversaries. These may include terrorist organizations, although historically these have relied primarily on physical violence to promote their goals.[3]

Cyber-threats to RPAS may be categorized according to the attacker's intention:

- **Intelligence.** Attackers could intercept and monitor the unencrypted data or information the RPA transmits to the ground in order to derive intelligence.
- **Disruption** of the RPAS. Intentional modification of computer systems by use of malicious code, e.g. Viruses, Trojans, or Worms taking advantage of familiar weaknesses of commercial operating systems.
- **Takeover** of the RPAS by taking over communication layouts and exploiting the system's bugs, or by way of 'smart entry' into the GCS and its computer systems or RPA's avionics.[4]

6.8.2 Accessibility of Computer Related Systems to Cyber-Attacks

6.8.2.1 Computer Networks. A network attack is most effective if there is regular access to it over time. This can provide the adversary with high quality intelligence that allows the surreptitious installation of malware for future use. Such an electronic backdoor or modern day version of a Cold War 'sleeper' is virtually undetectable by existing defensive technologies. It requires long term maintenance and preservation because of the continuous update process of the defensive systems designed to uncover malicious elements or activity.[5]

6.8.2.2 Interconnection of Military Networks with Commercial Infrastructure. Critical military network infrastructure is typically separated (physically and/or logically) from all other networks, especially from the internet. Therefore, it is more difficult if not impossible to gain regular access to those networks without having physical access to one of the military network's components. In contrast, the separation of commercial networks and sensitive civilian operational systems is not sufficiently established. This is a security vulnerability that allows attackers a great deal of access to civilian network infrastructures. In turn, the integration of military and commercial systems offers opportunity for access and therefore exploitation of military networks.[6]

Table 12 – Cyber-Warfare Threat Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

6.8.2.3 Supply Chain Corruption. A way of inserting malicious code into cyber-infrastructures is by engineering that code into common-use commercial integrated circuits. The microelectronics supply chain is extremely diffuse, complex and globally dispersed. This makes it difficult to verify the trust and authenticity of electronic equipment. An increasing concern is state-sponsored attempts to corrupt supply chains to gain access to sensitive networks and communications, or to create the ability to control or debilitate critical systems.[7]

6.8.2.4 Commercial Satellite Communications (COMSATCOM). SATCOM services are often provided by civilian or commercial service providers. These satellite capabilities are designed for the purpose of maximizing services and bandwidth, and ultimately, revenues. The result is less consideration for the 'hardening' of satellite system elements leaving their infrastructure vulnerable to security threats. Gaining access could result in the disruption of operations or takeover of an RPAS through re-engineering of C2 transmissions and re-transmitting them via the compromised satellite.

6.8.3 Availability of Cyber-Weapons

Commercially available computers or other devices can be readily turned into some form of cyber-weapon. Although it is theoretically possible for an individual to do so, it is generally believed the conduct of cyber-attacks which could inflict serious damage to military operational capabilities requires at least state sponsored organizational skills and resources. However, since only COTS equipment is needed to conduct cyber-attacks, the availability of cyber-weapons is assessed as 'high'.

6.8.4 Threat Assessment

Critical military network infrastructure is usually well secured and physically and/or logically separated from any external network. Therefore, the adversary's accessibility to those protected networks is limited. Given that RPAS GCSs are usually part of secured military networks, access to the RPAS by means of adversary remote access is difficult, but cannot be ruled out. The availability of cyber-weapons to possible future adversaries has been estimated as 'high'. Despite network security measures, the accessibility of RPAS network infrastructure to intrusion is also estimated as 'high' because infections of the GCS have already taken place.[8] Therefore, the overall probability of cyber-warfare attacks against RPAS is also estimated as 'high'. (cf. Table 12)

1. Rain Ottis, Peeter Lorents, 'Cyberspace: Definition and Implications', NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.
2. Gabi Siboni, Y. R., 'What Lies behind Chinese Cyber Warfare', in Cyberspace and National Security, Tel Aviv, Institute for National Security Studies (INSS), Jun. 2013, pp. 45–60.
3. Yoram Schweitzer, Gabi Siboni, Einav Yogev, 'Cyberspace and Terrorist Organizations', in Cyberspace and National Security, Tel Aviv, Institute for National Security Studies (INSS), Jun. 2013, pp. 17-25.
4. Dror Ben-David, 'Cyber Takeov er of large UAVs', Israeli Defense, no. 15, pp. 46-47, Aug. 2013.
5. Ibid. 2.
6. Ibid. 2.
7. Bryan Krekel, Patton Adams, George Bakos, 'Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage', Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, 2012.
8. Noah Shachtman, 'Computer Virus Hits U.S. Drone Fleet', WIRED.com, 10 Jul. 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. [Accessed 07 Jan. 2014].

Figure 11 – German Chancellor Angela Merkel (1st, L) and Defence Minister Thomas de Maiziere (1st, R) Watch a Quadcopter Crashing onto the Stage During an Election Campaign Event of Her German Christian Democratic Union (CDU) Party in Dresden, Eastern Germany on 15 September 2013.[1]

6.9 Adversary RPAS

Unmanned technology does not only offer new opportunities; it also presents challenges and harbours potential threats. Adversary remotely piloted systems in the MALE / HALE category could impose the same threat to friendly RPAS operations just like any other combat aircraft, i.e. air-to-air and air-to-ground strikes as well as employing EW capabilities. Those threats have already been outlined in chapter 6.2.2, so this chapter will focus on the emerging threats from smaller RPAS which are not only restricted to military use, but are also available commercially. Small, low and slow flying RPAS could introduce new strike capabilities to the military and non-state armed groups. They could also be directed against ground-based elements of the RPAS, i.e. personnel, the GCS and the RPA itself if it is not airborne.

6.9.1 Micro and Mini RPAS

Commercially available RPAS do not usually exceed 20 kg, classifying them as 'Micro' or 'Mini' RPAS according to NATO's RPAS classification guide. Payloads range from a few hundred grams to a few kilograms for larger models. Depending on the transmitter and receiver installed, the aircraft can be remotely controlled at ranges of up to 10 km. Typically, Micro and Mini RPAS do not operate above 3,000 ft, are usually powered by a rechargeable battery, and have a low operating time of approximately one hour. Military grade Micro and Mini RPAS share most of the same limitations as their commercial counterparts although their range and endurance are usually greater.

6.9.2 Detecting the RPAS Threat – A Real Challenge

Current MALE and HALE RPAS will most likely be detected by radar because they share the size, speed

	Raven[2] (mil)	Skylark[3] (mil)	QR400[4] (COTS)	XLC V2[5] (COTS)
Take-off weight	1.9 kg	7.5 kg	1.6 kg	17 kg
Payload	180 g	1 100 g	500 g	7 500 g
Mission radius	10 km	20 - 40 km	5 km	10 km
Endurance	90 min	180 min	30 min	45 min
Engine	Electrical	Electrical	Electrical	Combustion
Manufacturer	Aero Vironment	Elbit Systems	Walkera	VARIO Helicopter

Table 13 – COTS and Military Grade RPAS.[2,3,4,5]

and operating altitude with legacy, non-stealthy combat aircraft. In contrast, Micro and Mini RPAS are very small, can be flown at very low altitudes and slow speeds. Even if a low flying object is detected, AD systems usually filter out those targets too slow and too small, in order to eliminate clutter and false indications. This filtering technique opens a window of opportunity for Micro and Mini RPAS to operate undetected until they are in visual range. When considering RPA size, this visual range can be assumed to be quite close. Destroying such a small object will most likely be a significant challenge. During German Chancellor Angela Merkel's election campaign in 2013, her security service was completely taken by surprise when a commercial quadrocopter RPAS was flown towards the stage and almost crashed into her. What fortunately turned out to be a joke clearly illustrated the possible threat that Micro and Mini RPAS impose.[6] (cf. Fig. 11)

6.9.3 Availability of Micro and Mini RPAS

Usually still referred to as model aircraft, small RPAS can be acquired easily by anyone. A simple internet search for the terms 'drone' or 'quadrocopter' reveals hundreds of those small aircraft for purchase starting at less than $100. (cf. Table 13) Operating commercial RPAS doesn't require formal pilot training; it's as simple as flying a model plane. Hence, the availability of micro and mini RPAS is assessed as 'high'.

6.9.4 Accessibility of Friendly RPAS by Adversary Micro and Mini RPAS

Micro and Mini RPAS are man-portable and the operator can easily hide as no large ground control equipment is necessary. Depending on the RPAS range, the adversary only has to be located somewhere in the vicinity of a possible target, which can be up to 10km with current COTS models. Although endurance is limited, there may still be time to loiter undetected above the target to strike when the opportunity arises, e.g. when personnel leave their shelter. Due to the challenge of timely detection of Micro and Mini RPAS, the accessibility of friendly RPAS elements to those systems is assessed as 'high'.

6.9.5 Threat Assessment

Even the smallest RPAS can carry small payloads of some hundred grams of explosives and can cause fatal injuries to personnel and catastrophic damage to external GCS communications equipment or aircraft on the ground. They may be a weapon of choice

not only for non-state armed groups or terrorists, but also for military SOF to take out critical communications infrastructure such as RPAS GCS or Satellite Ground Stations.

Perhaps the most unsettling aspect of Micro and Mini RPAS is their inherent unpredictability. This is due to the lack of detectable and observable patterns during planning or execution of adversary operations using such commonly available platforms. Terrorist groups may provide no trail regarding their preparations. It is definitely much more difficult to obtain a firearm in most countries than to buy a Mini RPAS capable of delivering a suitable amount of explosives. The availability of both Micro and Mini RPAS to possible future adversaries as well as the accessibility of friendly RPAS elements to those systems has been assessed as 'high'. Therefore, the overall probability of attacks by adversary Micro and Mini RPAS is estimated as 'high'. (cf. Table 14)

1. 'German "Pirates" stage mini-drone stunt at Merkel rally', 17 Sep. 2013. [Online]. Available: http://rt.com/news/pirates-drone-stunt-merkel-953/. [Accessed 14 Nov. 2013].
2. 'RQ-11B Raven', AeroVironment, Inc., [Online]. Available: https://www.avinc.com/uas/small_uas/raven/. [Accessed 24 Apr. 2014].
3. 'Skylark® I LE - Mini UAS', Elbit Systems, [Online]. Available: http://www.elbitsystems.com/elbitmain/area-in2.asp?parent=3&num=279&num2=279. [Accessed 24 Apr. 2014].
4. 'QR X400', walkera, [Online]. Available: http://www.walkera.com/en/goods.php?id=444. [Accessed 24 Apr. 2014].
5. 'XLC V2', Vario Helicopter, [Online]. Available: http://www.vario-helicopter.biz/us1/product_info.php?products_id=100031. [Accessed 24 Apr. 2014].
6. Ibid. 1.

Table 14 – Adversary RPAS Threat Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

© a katz / Shutterstock.com

6.10 Public Perception and Legal Dispute

'Every one of these dead non-combatants represents an alienated family, a new desire for revenge, and more recruits for a militant movement that has grown exponentially even as drone strikes have increased.'
David Kilcullen, former advisor to US General David Petraeus

The public perception of RPAS (the legal and moral aspect of their use) does not directly endanger RPAS deployment. It may lead to negative attitudes towards their use and therefore indirectly influence friendly RPAS operations. Some European countries have delayed or even refrained from acquiring RPAS because of their national public debate on the moral, ethical and legal questions of their use.

This study identified three major concerns shaping the public perception of RPAS. These are radicalizations of the target population as a result of RPAS strikes, dissent about the legitimacy of certain types of RPAS operations and the concern about using civil service providers (contractors) for former military tasks within the remotely piloted system.

6.10.1 Radicalization

Some studies claim that RPAS strikes are likely to increase terrorism and create a new desire for revenge and radicalism due to the perception they cause high collateral damage. They identified a correlation between RPAS strikes and terrorist attacks and found it likely that RPAS strikes provide motivation for retaliation. A substantive relationship between the increasing number of RPAS strikes and retaliation attacks was found.[1,2] In contrast, another study on the same subject claims that RPAS strikes are generally associated with a reduction in the rate of terrorist attacks. They are also associated with a reduction in the number of people killed as a result of terrorist attacks and tend to be linked to decreases in the use

of particularly lethal and intimidating tactics, including suicide and IED attacks.[3]

6.10.2 Legitimacy

There is opposition, internationally as well as within individual nations, about the legitimacy of RPAS precision strike operations.[4] (cf. Fig. 12) This dispute is actually a non-sequitur; the RPAS is a delivery platform. Like any other air platform it can kill, disable, support troops on the ground, destroy, harry, hinder, deny access, observe and track. Like pilots providing close air support, firing missiles, or dropping bombs, RPAS operators are expected to respect the LoAC, striking based on clear information, including assessment of the potential for collateral damage.[5]

The probability of mistakes and unintended attacks is significantly reduced compared to engagements from manned aircraft. This is due to the increased operational and tactical level interfaces involved in an armed RPAS engagement. The extended loiter time of RPAS contributes even further to the already robust decision cycle because more time is available to assess available information and employ additional resources.

Another issue which is falsely associated with RPAS operations is the perceived targeting methodology and decision making process for obtaining permission to execute a lethal strike. There are a variety of stakeholders, organizations and political parties which refer to using the RPAS precision strike capability against human targets in non-belligerent states as extrajudicial and claim they are not in accordance with IHL.[6,7] To the contrary, there are extensive assessments issued by national authorities assuring the legality of using lethal RPAS capabilities.[8]

6.10.3 Contractors

There is also dissent on the current use of civilians to conduct combat-related tasks which historically have been conducted by military personnel. Although civilians have played a central role in recent combat operations by providing combat service support, maintaining weapon systems, etc., employing them as RPAS operators or intelligence analysts is controversial.[9,10] Employing civilians as RPAS operators began during the Balkans operations when the first Predator and Global Hawk RPAS were fielded around 1995. Currently, some RPAS manufacturers offer 'Contractor Owned – Contractor Operated' (COCO) contracts providing the military, not only with RPAS, but also company 'Field Service Representatives' (FSR) including aircrew for operating the RPA.[11,12] This development raises questions concerning the legal consequences of civilian participation in armed conflict. IHL states that civilians enjoy immunity from attack during international armed conflict 'unless and for such time as they take a direct part in hostilities'. Civilians directly participating in hostilities may be legally targeted and are labelled 'unlawful combatants'.[13]

Figure 12 – Amnesty International, Report on US RPA Operations in Pakistan.[14]

Unfortunately, 'direct participation in hostilities' is not clearly defined and is interpreted differently. As a common baseline from various studies, it can be defined as any action which is intended to cause actual harm to enemy personnel or equipment. This definition, not only includes RPAS personnel directly inflicting damage, but also includes other personnel involved in gathering intelligence for the purpose of selecting targets for attack.[15,16]

6.10.4 Threat Assessment

The public debate regarding RPAS is often driven by emotion rather than fact. Dissent concerning the legal issues of employing lethal force from RPAS also adds fuel to their negative reputation within the public domain. An adversary may also leverage that debate by spreading disinformation and propaganda through global mass media and the internet to exploit public opinion for its own purposes. If an adversary succeeds in winning the propaganda war, they may influence decision makers in their willingness to employ RPAS. Eventually, this may result in restrictions to RPAS operations or even halt RPAS acquisition plans.

1. International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at Nyu School of Law, 'Living Under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan', Sep. 2012. [Online]. Available: http://www.livingunderdrones.org/wp-content/uploads/2013/10/Stanford-NYU-Living-Under-Drones.pdf. [Accessed 16 Sep. 2013].
2. Leila Hudson, Colin S. Owens, Matt Flannes, 'Drone Warfare: Blowback from the New American Way of War', Middle East Policy Council, [Online]. Available: http://www.mepc.org/journal/middle-east-policy-archives/drone-warfare-blowback-new-american-way-war. [Accessed 16 Sep. 2013].
3. Patrick B. Johnston, Anoop K. Sarbahi, 'The Impact of U.S. Drone Strikes on Terrorism in Pakistan and Afghanistan', RAND Corporation, Jul. 2013.
4. Amnesty International, 'Will I be Next? US Drone Strikes in Pakistan', Amnesty International Publications, London, Oct. 2013.
5. Jacqueline L. Hazelton, 'Drones: What Are They Good For?', 2013.
6. Kenneth Roth, 'What Rules Should Govern US Drone Attacks?', Human Rights Watch, 11 Mar. 2013. [Online]. Available: http://www.hrw.org/news/2013/03/11/what-rules-should-govern-us-drone-attacks. [Accessed 17 Sep. 2013].
7. Peter Maurer, President of the ICRC, 'The use of armed drones must comply with laws', International Committee of the Red Cross (ICRC), 10 May 2013. [Online]. Available: http://www.icrc.org/eng/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm. [Accessed 17 Sep. 2013].
8. U.S. Department of Justice, 'Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or An Associated Force (White Paper Draft)', 8 Nov. 2011. [Online]. Available: http://www.fas.org/irp/eprint/doj-lethal.pdf. [Accessed 17 Sep. 2013].
9. John Ricou Heaton, Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces, George Washington University Law School, 2004.
10. Keith E. Tobin, Piloting the USAF's UAV Fleet, Pilots, Non-Rated Officers, Enlisted, or Contractors?, Alabama: School of Advanced Airpower Studies, Air University Maxwell Air Force Base, Jun. 1999.
11. Chris Pocock, 'UK Royal Navy Is Latest Customer for Scan Eagle UAS', AINonline, AIN Defense Perspective, 05 Jul. 2013. [Online]. Available: http://www.ainonline.com/aviation-news/ain-defense-perspective/2013-07-05/uk-royal-navy-latest-customer-scan-eagle-uas. [Accessed 19 Nov. 2013].
12. 'Field Operations & Logistics', Insitu Inc., [Online]. Available: http://www.insitu.com/services/field-operations-and-logistics. [Accessed 19 Nov. 2013].
13. Michael N. Schmidt, Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees, George C. Marshall European Center for Security Studies, 2004-2005.
14. Ibid. 4.
15. Ibid. 9.
16. Ibid. 13.

© US Air Force

CHAPTER VII

Vulnerability Identification

RPAS share many of the limitations of manned aircraft, but also have additional vulnerabilities which are unique to them. The separation of the pilot from the cockpit and the reliance on sufficient data links create completely new issues not yet known to manned aviation. This chapter outlines the system components' limitations and vulnerabilities.

7.1 Remotely Piloted Aircraft

To physically destroy an airborne RPA, an adversary can employ SBAD systems, MANPADS, Combat Aircraft or other RPAS. However, engaging the RPA by any of the above-mentioned methods requires the RPA to first be detected.

7.1.1 Detection Avoidance

7.1.1.1 Visibility to Radar Systems. The visibility of an object to a radar system is measured by the Radar Cross Section (RCS). RCS is defined as the measure of a target's ability to reflect radar signals in the direction of the radar receiver.[1,2] Current MALE RPAS display an average RCS of slightly less than one square meter. This is comparable to regular non-stealth type fighter aircraft, e.g. McDonnell Douglas F/A-18, Dassault Rafale or Eurofighter Typhoon.[3,4,5] Although some RPAS have been built with stealth technology and radar absorbing materials, the vast majority of current systems lack any of those protective measures. The overall visibility of existing RPAS to radar systems is therefore assessed as 'high'.

7.1.1.2 Visibility in the Infrared Spectrum. The ability of weapons systems to discriminate between IR emissions from the target and the surrounding background leads to successful target detection. Hot engine parts, exhaust plumes, the rear fuselage area and aerodynamically heated skin are the key sources of aircraft IR emissions. The intensity of IR-radiation is not uniform in all directions. When viewed from the front and sides, the exhaust plume and airframe are the most visible source of IR energy. When viewed from the rear, the engine hot parts become the major source. In general, aircraft with a jet engine have the

highest IR intensity. For the same thrust level, turbojets have a larger IR signature level (IRSL) than turbofans, and turbofans have a larger IRSL than turboprops.[6]

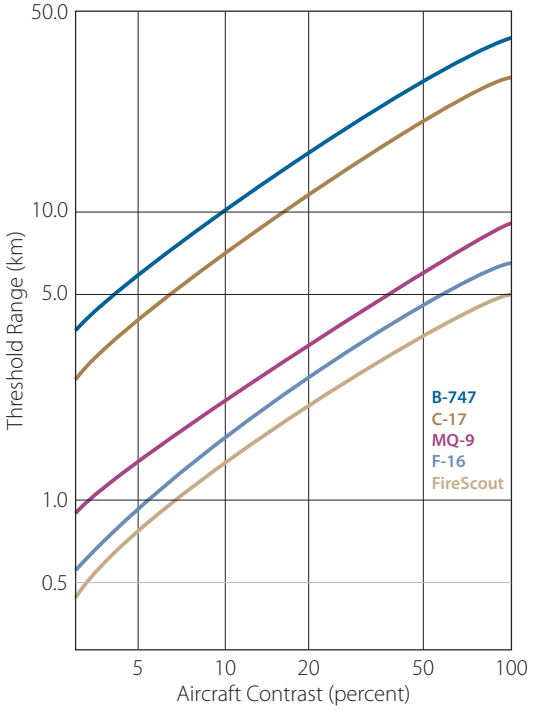
The majority of MALE RPAS configurations have a turboprop engine fitted to the back of the RPA, dispersing the exhaust through the pusher propeller. Compared to a turbojet powered aircraft, this design results in a much lower ISRL. Hence, visibility in the IR spectrum is estimated as 'moderate'. However, those RPAS are not necessarily immune to attacks by IR-guided missiles. Modern IR-detection technology with its increased sensitivity is capable of detecting IR radiation in a wider spectrum and is capable of locking-on to aircraft from all aspects.[7]

7.1.1.3 Acoustic Detectability. Many RPAS are still propeller driven and generate a significant amount of noise. Depending on their altitude, the noise emissions of a propeller can be so strong the propeller noise alone may attract the attention of ground personnel. This can generate unwanted attention or a potential attack on low flying RPAS.[8] A report on the effects of US 'drone' strike policies in Pakistan also claims that current RPAS operations are clearly audible from the ground.[9] RPAS propeller noise can be measured by a ground based stationary microphone which uses the Doppler Effect in the acoustic spectrum to compute the aircraft's altitude, speed and actual revolutions per minute of the engine. Real-time computations on such signals can be carried out with modern digital signal processing hardware and advanced algorithms.[10] As the noise perceptibility can be mitigated by operating at higher altitudes, the acoustic detectability is rated as 'low' for normal operating altitudes of current MALE systems. This rating may elevate to 'moderate' or even 'high' if certain RPAS missions or sensor constraints require low level flight.

7.1.1.4 Visual Aircraft Recognition. The range at which aircraft can be detected, recognized and identified varies with the size, shape and colour of the aircraft, viewing aspect, visibility conditions, its motion relative to and contrast with the background and eventually the visual acuity of the observer. Depending on these factors, aircraft can be seen at long ranges in clear weather. When there is rain, snow, fog, dust or haze, the visibility range may be reduced to zero.[11,12] The largest distance at which an aircraft can be seen by the human eye can be mathematically predicted from its size and contrast to the background. Given a perfect black & white contrast, an MQ-9 Reaper can be detected at a distance of almost 10 km. Lowering the contrast to 50% (grey & white) reduces the detection range to roughly 5 km. (cf. Fig. 13) As military aircraft are typically camouflaged to blend in with the surrounding sky, it can be assessed that visual detection of RPAS without electro-optical support is limited to ranges of less than 5km and is unlikely at altitudes above 15,000 ft.[13] The probability of visual aircraft recognition is therefore assessed as 'low' for normal operating altitudes of current MALE systems. This rating may elevate to 'moderate' or even 'high' if certain RPAS missions or sensor constraints require low level flight or during launch and recovery.

7.1.1.5 RPA on the Ground. During ground handling, RPA may be exposed to observation and engagement by adversaries if parked in the open or while taxiing between their parking position and the runway. As this situation is not different from any other aircraft on a military airbase, force protection measures are usually in place and support RPA operations as well.

Figure 13 – Threshold range as a function of contrast for aircraft.[17]



7.1.1.6 Avionics. Avionics built without cyber-security considerations may be vulnerable to cyber-attack. Autopilot systems have not changed since they were introduced in manned aerial vehicles and cyber-security was not a design priority. Therefore, current RPA avionics may be subject to cyber-attack either by clandestinely installing malicious hardware components or by gaining control via the RPAS data link.[14] Gaining access to the RPAS data link is discussed in chapter 7.5 whereas the exposure of RPAS hardware and software components to cyber-attacks is outlined in chapters 6.8.3, 7.4.2 and 7.4.3.

7.1.2 Engagement Avoidance

With a few exceptions, current RPAS are not equipped with a threat warning system to detect and avoid threats such as AD systems, MANPADS and combat aircraft. Integration of equipment from manned aviation may be problematic due to RPA Size, Weight and Power (SWaP) limitations.

7.1.3 Hit Avoidance

Most of the current MALE RPAS share 1980's design principles that sought to optimize long endurance and low fuel consumption. The most prominent features are wings with a very high aspect ratio combined with a rear mounted, fuel efficient propeller engine. Together, these provide the desired flight characteristics but bring with them certain disadvantages. High aspect ratio wings have a fairly high amount of inertia that prevents the RPA from conducting flight manoeuvres with a high roll angular acceleration and G-force.[15] Additionally, the average cruising speed of propeller driven RPAS is quite low, e.g. 70 knots (kts) for the MQ-1 Predator or 200 kts for the MQ-9 Reaper.[16,17] Therefore, the RPA is unable to conduct 'last ditch' manoeuvres and becomes a rigid target when compared to manned fighter aircraft.

7.1.4 Hit Tolerance

RPAS are typically capable of operating more than one RPA at a time. So the loss of a single RPA may only result in failure of the current mission if a substitute RPA is not available for mission completion. Any payload attached to the RPA will also be lost. This may result in the loss of previously acquired sensor data. However, the RPAS will remain operational as long as a substitute RPA is available. For single-aircraft RPAS, the magnitude of losing the RPA is assessed as 'high' because the entire RPAS will be rendered useless. The magnitude of losing a single RPA in a multi-aircraft RPAS is estimated as 'moderate' because the effect on the overall system may be compensated by the use of substitute aircraft. The loss of an RPA also includes the danger of revealing classified technology to the adversary. Remnants of the downed aircraft may be exploited through reverse engineering to replicate the RPA or gather intelligence about frequencies used, encryption techniques or stored data.

7.1.5 Vulnerability Assessment

7.1.5.1 Vulnerability to SBAD, Combat Aircraft & RPAS. The RPA itself is by design highly vulnerable. Current systems were never intended to operate in contested environments. The highest risk to RPA comes from enemy AD systems and combat aircraft as they are designed to detect aircraft at long ranges and can engage the RPA with radar or IR-guided missiles. Given their high radar visibility and their limited airspeed and manoeuvrability, this leads to an overall 'high' vulnerability to adversary SBAD and combat aircraft. As the magnitude of losing an RPA is rated as 'moderate' to 'high', the overall vulnerability rating with respect to SBAD and combat aircraft is assessed as 'high'. The higher rating was chosen to reflect the possibility of complete – but at least temporary – mission failure in the case of losing an RPA. Adversary RPAS may be capable of air-to-air combat and may be able to detect and engage friendly RPA. However, current systems offer very limited capabilities in that regard, which is why the vulnerability rating with reference to adversary RPA is reduced to 'moderate'. (cf. Table 15)

7.1.5.2 Vulnerability to MANPADS. MANPADS engagement towards an RPA has two perspectives, normal airborne operations and launch and recovery. Typically, the operating altitude of MALE RPA is higher than the visual acquisition range of ground personnel and therefore the threat of MANPADS may be easily mitigated. This situation is different when the RPA is operating at lower altitudes such as during launch & recovery or when it is required for operational reasons. If the RPA is in spotting range of the

adversary and visually identified, it will be within firing range of MANPADS. Accordingly, this study assesses that RPA engagement by MANPADS might be possible and is therefore assessed as 'moderate'. (cf. Table 15)

7.1.5.3 Vulnerability to Asymmetric Forces, Air-to-Ground and Surface-to-Surface Weapons. Like any other aircraft, RPA are high value targets for an adversary. If parked in the open, they are highly visible and therefore vulnerable to a kinetic engagement. Even RPGs or sniper rifles could cause catastrophic damage to the airframe and its payload if an adversary can get within the range of those types of weapons. As force protection measures are typically in place for military airfields, the vulnerability assessment for kinetic attacks against RPA on the ground is lowered to 'moderate'. (cf. Table 15)

7.1.5.4 Vulnerability to Cyber Attacks. The RPA is one of many nodes in the overall RPAS network. Concluding the network is only as strong as its weakest link and that corruption of microelectronics supply chains has not yet been adequately addressed, the vulnerability to cyber-attacks is assessed as 'high'. (cf. Table 15)

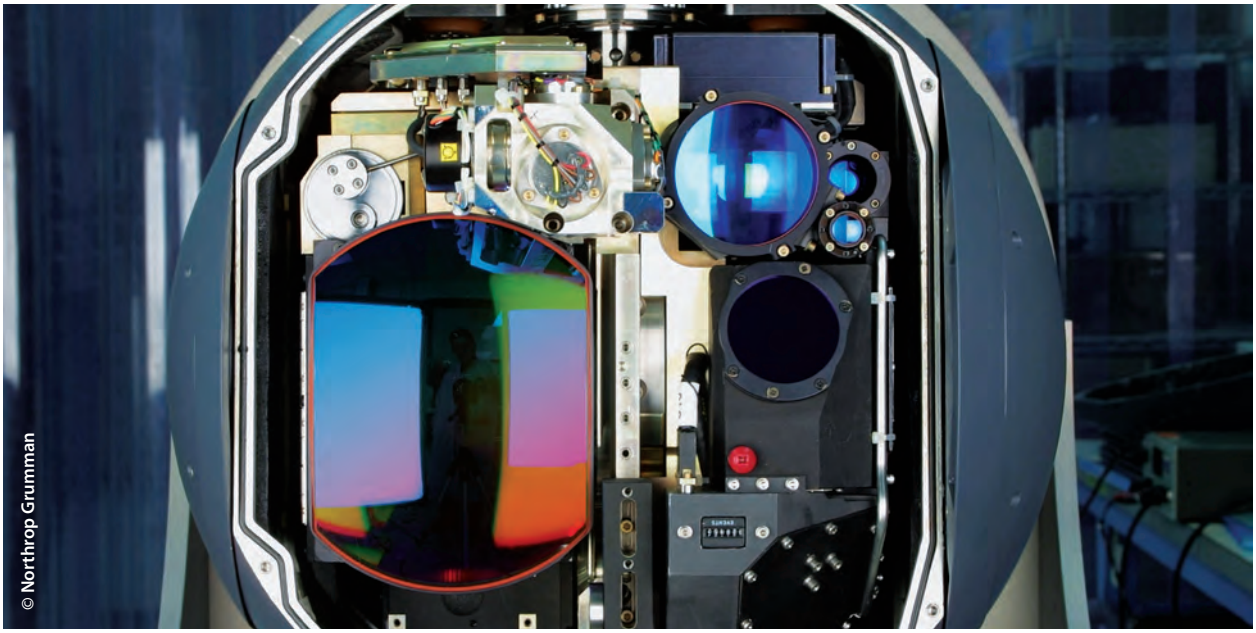
1. http://www.rfcafe.com/references/electrical/ew-radar-handbook/radar-cross-section.htm
2. IEEE Standard Definitions of Terms for Antennas, IEEE Standards Association, 1993.
3. 'RCS Simulation of the Predator UAV', Efield AB, Kista, Sweden, 2010.
4. 'Radar Cross Section (RCS)', Global Security, 11 July 2011. [Online]. Available: http://www.globalsecurity.org/military/world/stealth-aircraft-rcs.htm. [Accessed 25 Nov. 2013].
5. Allen J. Bric, 'Imaging a BQM-74E Target Drone Using Coherent Radar Cross Section Measurements', Johns Hopkins APL Technical Digest, vol. 18, no. 3, pp. 365-376, 1997.
6. Shripad P. Mahulikar, Hemant R. Sonawane, G. Arvind Rao, 'Infrared signature studies of aerospace vehicles', Progress in Aerospace Sciences, vol. 43, no. 7-8, pp. 218-245, Oct. 2007.
7. Ibid.
8. M. Drela, J. Gundlach, R. Parks and A. S. Ehrmantraut, 'System and Method for Reducing the Noise of Pusher Type Aircraft Propellers'. United States Patent 20120292441, 2012.
9. International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at Nyu School Of Law, 'Living Under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan', Sept. 2012. [Online]. Available: http://www.livingunderdrones.org/wp-content/uploads/2013/10/Stanford-NYU-Living-Under-Drones.pdf. [Accessed 16 Sept. 2013].
10. S. Sadasivan, M. Gurubasavaraj and S. Ravi Sekar, 'Acoustic Signature of an Unmanned Air Vehicle - Exploitation for Aircraft Localisation and Parameter Estimation', Aeronautical Development Establishment, 28 Feb. 2001. [Online]. Available: http://publications.drdo.gov.in/ojs/index.php/dsj/article/download/2238/1198. [Accessed 26 Nov. 2013].
11. Headquarters Department of the Army, 'Visual Aircraft Recognition FM 3-01.80 (FM 44-80)', 17 Jan. 2006. [Online]. Available: https://www.fas.org/irp/doddir/army/fm3-01-80.pdf.
12. Reg Austin, Unmanned Aircraft Systems: UAVS design, development and deployment, John Wiley & Sons Ltd, 2010.
13. Andrew Watson, Cesar V. Ramirez, Ellen Salud, 'Predicting Visibility of Aircraft', PLoS ONE, vol. 4, no. 5, May 2009.
14. Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang and Hal Aldridge, 'Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles', Purdue University, West Lafayette, Indiana and Sypris Electronics, Tampa, Florida.
15. John D. Anderson, Jr., Fundamentals of Aerodynamics (5th Edn), 2010.
16. 'MQ-1B Predator Fact Sheet', U.S. Air Force, 20 July 2010. [Online]. Available: http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx. [Accessed 26 Nov. 2013].
17. 'MQ-9 Reaper Fact Sheet', U.S. Air Force, 18 Aug. 2010. [Online]. Available: http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx. [Accessed 25 Nov. 2013].
18. Ibid. 13, p. 13.

Table 15 – RPA Vulnerability Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1



7.2 Payload

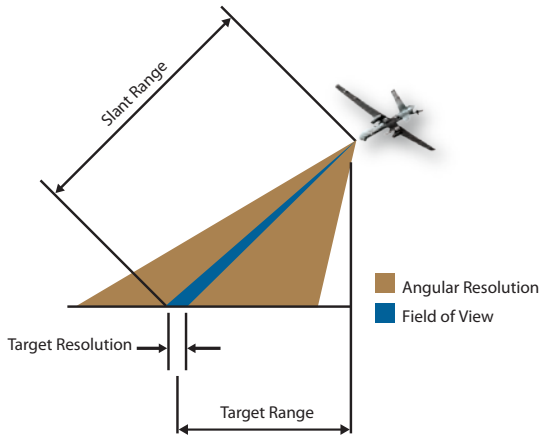
The RPA's payload consists primarily of EO/IR and/or radar sensor devices and – if applicable – a set of weapons. Payload capabilities and limitations contribute directly to the overall survivability of the RPA, primarily in terms of detection and engagement avoidance. This section discusses those sensor and weapon issues which influence RPA vulnerabilities mentioned in the previous chapters.

7.2.1 Detection Avoidance

7.2.1.1 EO/IR Sensor Stand-Off Capabilities. The EO/IR sensors primarily conduct ISR and Target Acquisition tasks. The major difference between these two applications is the field of view and the range to the target. ISR providing long-term imaging of the ground is usually conducted from a vertical perspective. Target acquisition is typically performed from a horizontal perspective. Independent from the viewing angle and target range, only the slant range to the threat directly influences RPAS survivability. (cf. Fig. 14) The maximum possible slant range depends on the operational requirements of the desired target resolution. This is expressed via the National Interpretability Rating Scale (NIIRS) or Ground Resolved Distance (GRD).[1,2] (cf. Table 16)

Even older EO/IR sensor equipment was able to achieve a GRD of less than 40 cm per image pixel at slant ranges of roughly 25-30 km and altitudes above 55,000 ft.[3] Current average operational altitudes of MALE RPAS in Afghanistan have been in the range of 20,000 ft to 25,000 ft. These operating altitudes delivered even better GRD for positive target identification.[4] However, depending on haze, dust and other vision-obscuring conditions, the effective slant ranges can be considerably lower.[5]

Figure 14 - Sensor Ranges.[11]



NIIRS	GRD (m)	Nominal Capability
1	> 9.00	Detect medium sized port
2	4.50 - 9.00	Detect large buildings
3	2.50 - 4.50	Detect trains on tracks
4	1.20 - 2.50	Identify railroad tracks
5	0.75 - 1.20	Identify theatre ballistic missiles
6	0.40 - 0.75	Identify spare tire on truck
7	0.20 - 0.40	Identify individual rail ties
8	0.10 - 0.20	Identify windshield wiper
9	< 0.10	Identify individual rail spikes

Table 16 – Sensor Resolutions.

7.2.1.2 Synthetic Aperture Radar Sensor Stand-Off Capabilities. In contrast to EO/IR sensors, Synthetic Aperture Radar (SAR) technology can provide high-resolution imagery in inclement weather, at night and/or at higher ranges. As a result of the complex information processing capability of modern digital electronics, SAR imagery can deliver a strictly vertical view of the target independent of the actual viewing angle.[6,7] Given the same slant range, a SAR can operate at considerably higher target ranges than EO/IR sensors and achieve the same imagery resolution. Although only the slant range actually contributes to the stand-off capability of the sensor, SAR may be preferred if target range is a challenge (e.g. when border crossing issues are a factor).

7.2.1.3 Weapon Stand-Off Capabilities. In current operations, many RPAS can be armed with Air-to-Ground Missiles (AGM), Laser-Guided Bombs (LGB) and/or Joint Direct Attack Munitions (JDAM). Unlike self-propelled munitions (i.e. guided missiles), the range of a LGB or JDAM depends exclusively on the airspeed and altitude of the delivery platform. Current propeller-driven MALE RPA have a cruising speed of about 200 kts[8] and future jet-propelled RPA are expected to achieve speeds of up to 400 kts[9]. Modern manned fighter aircraft are capable of bomb releases at high subsonic or even supersonic speeds and at higher altitudes.[10] The total potential (altitude) and kinetic (airspeed) energy of the weapon at release is the main contributor to its maximum range. Consequently, the same type of a LGB or JDAM will have a shorter range if released from an RPA than if released from a combat aircraft. (cf. Fig. 15)

7.2.2 Engagement Avoidance

7.2.2.1 Situational Awareness. The RPA's sensors are the operators' 'eyes and ears'. Sensors are the only direct source of information to build situational awareness. Although the RPA sensor suite can take a very detailed look of a very small area, the viewer has no awareness of anything outside the 'soda straw' view of the aircraft's sensors. Boresight cameras mounted on the RPA's nose or tail provide the crew with a broader view of the flight direction, but they still do not receive the kind of cues they get from their proprioceptive senses.[12,13,14]

Increased automation can lower an operators' task load to the point where vigilance is negatively affected and boredom may result. As increased automation shifts controllers into system management positions, monotony, loss of vigilance and boredom are more likely to occur. With recent advances in automation, it is not uncommon for an RPAS operator in search and reconnaissance missions to spend the majority of the mission merely waiting for a system anomaly to occur and to only interact with the system occasionally. This reduced need for interaction can result in a lack of sustained attention, which can

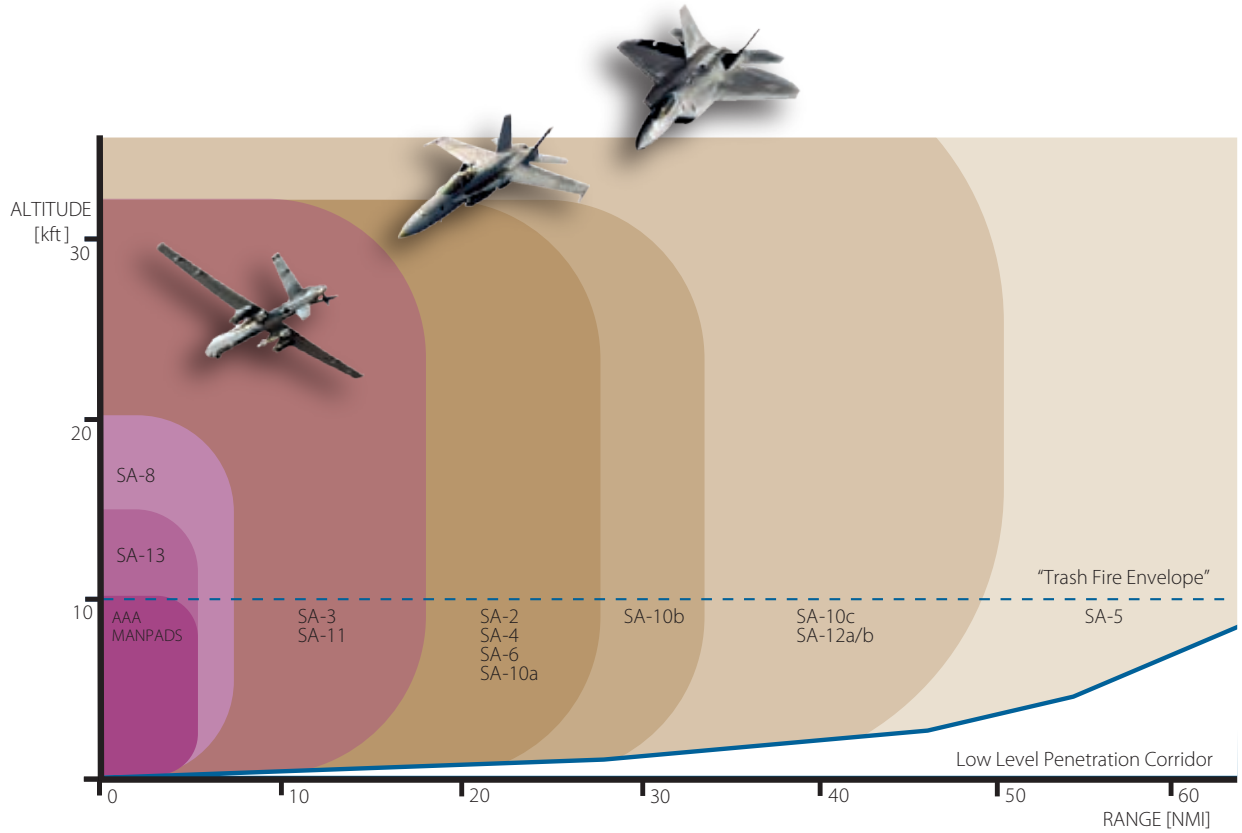
have a negative impact on the mission. Moreover, boredom may be a factor that induces complacency, which is also a significant concern in supervisory control systems.[15] In ninety-five Predator mishaps and safety incidents reported to the US Air Force over an eight-year period, 57 % of crewmember-related mishaps were consistent with situational awareness errors associated with reduced perception of the environment.[16]

7.2.2.2 Warning Receivers. RPAS sensors have not yet been designed for threat detection. This is a fundamental limitation when the remotely piloted system might be facing a threat. Moreover, the recent successes of ISR RPAS in relatively benign environments have led to a focus on the improvement of sensor payloads rather than on development of self-protection capabilities.[17] Current state-of-the-art RWR systems weigh less than 100 lbs and consume a minimal amount of electrical power. Current models of HALE/MALE RPAS could easily handle these requirements, considering there is always a trade-off between the RPA's maximum payload capacity and the additional capability these systems provide.[18] Although self-protection suites used on manned aircraft are available, few RPAS are currently equipped with them. One exception is the Global Hawk. It is designed and equipped with a self-protection suite consisting of an RWR, jamming system and towed decoy.[19,20,21]

7.2.3 Hit Tolerance

The payload is attached to the airframe and therefore an inherent part of the RPA itself. Physical destruction of the payload will most certainly cause catastrophic damage to the airframe as well. The consequences of downing the RPA were outlined in chapter 7.1.4.

Figure 15 – Stand-Off Ranges of GBU-38 JDAM, 30 degree impact angle, on-axis release.[22]



Aircraft	Release speed	Altitude	Range (R)
Predator B (cruising speed)	102 m/s	30,000 ft	7.7 NMI
Predator B (maximum speed)	128 m/s	40,000 ft	11.6 NMI
F-18	257 m/s	40,000 ft	16.6 NMI
F-22	510 m/s (supersonic)	50,000 ft	26.5 NMI

7.2.4 Vulnerability Assessment

RPAS sensor vulnerability cannot be assessed separately from the RPA, as they are an inherent part of the airframe. A threat to and vulnerability of the airframe is also a threat to or vulnerability of the payload as well. Sensor limitations contribute to the RPA's vulnerabilities and affect its survivability in terms of stand-off capability (detection avoidance) and threat detection (engagement avoidance). However, this study could not identify any sensor packages currently in use that contribute to a reduction in the overall vulnerability of the RPA so the vulnerability assessment of the sensor package is equal to that of the RPA. (cf. Table 17)

1. James B. Campbell, Randolph H. Wynne, Introduction to Remote Sensing, Fifth Edn, Guilford Press, 2012, pp. 103, 287 f.
2. 'National Image Interpretability Rating Scales', Federation of American Scientists (FAS), 16 Jan. 1998. [Online]. Available: https://www.fas.org/irp/imint/niirs.htm. [Accessed 23 Apr. 2014].
3. Lockheed Martin, Presentation on UAS EO/IR Sensor Capabilities, 2002.
4. 'Predator RQ-1 / MQ-1 / MQ-9 Reaper UAV', airforce-technology.com, 2013. [Online]. Available: http://www.airforce-technology.com/projects/predator-uav/. [Accessed 29 Nov.2013].
5. 'Video Synthetic Aperture Radar (ViSAR)', DARPA Strategic Technology Office, [Online]. Available: http://www.darpa.mil/Our_Work/STO/Programs/Video_Synthetic_Aperture_Radar_(ViSAR).aspx. [Accessed 29 Nov. 2013].
6. Y. K. Chan, V. C. Koo, 'An Introduction to Synthetic Aperture Radar (SAR)', Progress in Electromagnetics Research B, vol. 2, pp. 27-60, 2008.
7. .'Synthetic Aperture Radar' [Online]. Available: http://www.radartutorial.eu/20.airborne/ab07.en.html. [Accessed 29 Nov. 2013].
8. 'MQ-9 Reaper/Predator B', General Atomics Aeronautical, 2012. [Online]. Available: http://www.ga-asi.com/products/aircraft/pdf/Predator_B.pdf. [Accessed 09 July 2013].
9. 'Predator C Avenger', General Atomics Aeronautical, 2012. [Online]. Available: http://www.ga-asi.com/products/aircraft/pdf/Predator_C.pdf. [Accessed 09 July 2013].
10. 'JDAM Airspeed/Altitude Capability (U)', in GBU-31, GBU-32 AND GBU-35 Joint Direct Attack Munitions (JDAM), (Secret) Information extracted is unclassified, NAWS China Lake, CA 93555-6100, Naval Air Warfare Center, Weapons Division, 2002.
11. Ibid. 3.
12. Flight International, 'USAF: Current unmanned aircraft irrelevant in the Pacific', 06 Dec. 2012. [Online]. Available: http://www.flightglobal.com/news/articles/usaf-current-unmanned-aircraft-irrelevant-in-the-pacific-379839/. [Accessed 15 Apr. 2013].
13. Navy Captain Greg Maguire, Exercise Blue Knight, Nellis Test and Training Range, Nevada, 2011.
14. Anthony P. Tvaryanas, William Platte, Caleb Swigart, Jayson Colebank, Nita Lewis Miller, 'A Resurvey of Shift Work-Related Fatigue in MQ-1 Predator Unmanned Aircraft System Crewmembers', Naval Postgraduate School, Monterey, 2008.
15. M.L. Cummings, C. Mastracchio, K.M. Thornburg, & A. Mkrtchyan, Massachusetts Institute of Technology, 'Boredom and Distraction in Multiple Unmanned Vehicle Supervisory Control', 2013. [Online]. Available: http://web.mit.edu/aeroastro/labs/halab/papers/BoredomDistraction_SEP2012.pdf. [Accessed 16 Apr. 2013].
16. Anthony P.Tvaryanas, William T. Thompson, 'Recurrent Error Pathways in HFACS Data: Analysis of 95 Mishaps with Remotely Piloted Aircraft', Aviation, Space, and Environmental Medicine Vol. 79, No. 5, May 2008.
17. Robert Haffa Ph.D., Anand Datla, '6 Ways to Improve UAVs', Haffa Defense Consulting, LLC, 2012.
18. Paddy G. Forrest, 'Light Weight Low Cost Threat Warning for UAV, Aerostat and other small Platforms', Teledyne Defence Limited, Shipley.
19. 'LR-100 RWR/ESM/ELINT Receiver System', Northrop Grumman, [Online]. Available: http://www.northropgrumman.com/Capabilities/LR100/Pages/default.aspx. [Accessed 04 July 2013].
20. 'Global Hawk', Northrop Grumman, [Online]. Available: http://www.northropgrumman.com/Capabilities/GlobalHawk/Pages/default.aspx. [Accessed 04 July 2013].
21. Andreas Parsch, 'Designations of U.S. Military Electronic and Communications Equipment', [Online]. Available: http://www.designation-systems.net/usmilav/electronics.html#_JETDS_AN_Listings. [Accessed 04 July 2013].
22. Range Calculations by Boeing Company on Request of the Author, 2013.

Table 17 – Payload Vulnerability Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

© US Air Force, Rich McFadden

7.3 Human Element

'You shoot a missile, you kill a handful of people and then, this is what is strange, you go home. Your shift is over. You get in your car and drive 30 minutes to the northern suburbs of Las Vegas and you mow the lawn, talk to your kids, you go to church.'
Mary Cummings, former U.S. Navy Pilot

Although the RPA itself does not carry a human crew, there are a lot of personnel involved in the operation of the RPAS. For example, a MQ-9 Reaper Combat Air Patrol (CAP) consisting of four RPA has a strength of approximately 200 personnel. Roughly one-third of these personnel are deployed in or near the AOO to launch, recover and maintain the aircraft.[1] Attacking the personnel rather than the RPA itself may also be a favourable option for an adversary. Attacking personnel involved in RPAS operations has already begun and has allegedly proven successful. The leader of the Haqqani Network in Afghanistan claimed that 'accurate drone-strike operations against the Mujahedeen decreased 90 percent' following the December 2009 attack on a US Central Intelligence Agency (CIA) base in Khost that killed seven CIA officers.[2] RPAS personnel can be classified in three categories: the LRU, the MCE and the PED element. Depending on the mission, these RPA personnel may be working at different locations.

7.3.1 Detection, Engagement and Hit Avoidance

7.3.1.1 Launch and Recovery Unit. Depending on the RPA's effective range, the Launch and Recovery Unit (LRU) is usually located in or near the AOO. For smaller MALE RPAS, the LRU is most likely deployed inside the AOO. For larger MALE RPA with higher effective ranges and airspeeds, the LRU may be deployed to a neighbouring host nation. Currently, only HALE RPA such as the Global Hawk have their LRU located outside the AOO. Launching and recovering a MALE RPA requires a LOS Data Link from a local GCS and a suitable airport infrastructure with a runway of roughly 2,000 m. Like any other military aircraft, additional

shelters for refuelling, arming and performing maintenance are needed as well. The infrastructure needed to operate RPAS is usually part of a military compound and LRU personnel working on-base are protected, as force protection measures are usually already in place.

7.3.1.2 Mission Control Element. After the RPA has been launched, it may then be operated BLOS by a Remote Split Operations[3] (RSO) squadron from a GCS inside the home territory. Military installations hosting MCEs, GCSs or RPAS squadrons are often the topic of public debate. Therefore, their locations are well known.[4] RSO squadron personnel and their GCS are typically located inside military compounds protecting them from unwanted access and immediate threat. Home-based RPAS personnel enjoy the protection of their home country's environment, which is assumed to make enemy access more difficult. However, the perceived threat level and level of alert for military installations in the home country is usually lower compared to that of deployed locations, which may be exploited by an adversary.

7.3.1.3 Processing, Exploitation and Dissemination Element. The data links that enable RPAS RSOs also permit conducting PED from afar, via any network attached to the RPAS. Many nations operating RPAS use some kind of central 'reach back' intelligence organization to conduct their PED. This is due to the vast amount of imagery and FMV delivered by current RPAS.[5] Centralized intelligence operating bases or offices usually have more robust protective measures than typical military installations. Like the MCE, they also enjoy the protection of their home country's security environment.

7.3.1.4 Off-Duty Environment. Depending on the alert state, LRU personnel deployed in or near the AOO are likely to wear uniforms and stay within the military base if they are off-duty. Force protection measures for these personnel usually don't change whether they are on- or off-duty. Conversely, MCE or PED personnel usually have the option of leaving the protected military environment while off-duty. This provides a window of opportunity for an adversary to strike when the individual is most vulnerable. Individual targets may be identified by traditional intelligence, but also by exploiting social media and the internet.[6,7,8,9] Additionally, they may be identified by name tags, unit patches, or special insignia which some countries award to their RPAS operators.[10] (cf. Fig. 16) Once identified, targeted RPAS personnel along with their families, their social environment and their private property may be subject to attack. Despite the question of whether such an attack is a criminal act, RPAS personnel may face a real threat in their home countries. Furthermore, once an individual's family is identified, RPAS personnel may also be subject to blackmail.

Figure 16 – US Air Force RPAS Pilot Wings.

7.3.1.5 Currently Implemented Countermeasures. Current force protection measures apply primarily to deployed RPAS personnel only. Home-based RPAS personnel must rely on their home country's protected environment and the security of the military installations they're working in. This study could not identify any protective measures currently in place for non-deployed personnel in the off-duty environment. On the contrary, countless references were found clearly revealing the names and identities of RPAS personnel during interviews and other press-related activities.[11,12,13,14]

7.3.2 Hit Tolerance

7.3.2.1 Impact of RPAS Personnel Casualties. The impact of casualties depends on the affected individual's role in the RPAS mission. The attack may have a more significant effect if the individual is an operator in the LRU versus an image analyst in the PED element. RPAS usually have some redundancy if 24 hour operations are required. The most critical element in the RPAS is the aircrew (pilot and sensor operator).[15] Loss or incapacitation of a single aircrew member may

be temporarily absorbed by extending aircrew work cycles. The loss or incapacitation of more than one aircrew member may degrade operational capability and reduce availability of the RPAS until affected personnel regain full strength. Depending on the location, the time required to reinforce affected personnel may differ significantly. Personnel in the home-based MCE or PED element may be reinforced much more quickly than LRU personnel, who must first be deployed to the AOO.

Depending on their role in the RPAS, personnel being blackmailed could seriously impair mission accomplishment. For example, pilots may be forced to cause flight accidents or operators may be compelled to falsify mission data or to misfire weapons.

7.3.2.2 Post-Traumatic Stress Disorder. Even with advanced RPAS technology, moral and emotional burdens fall on the minds of RPAS operators. While they may be physically safe from enemy threat, psychologically, they're still conducting combat operations.[16] RPA often loiter over targets for hours, and operators obtain close-up views of their areas of interest and of an attack's aftermath to verify mission success. Therefore, RPAS personnel might be more psychologically affected when striking targets than pilots flying manned aircraft who drop bombs without seeing the after effects of their attack.[17]

In addition to experiencing traumatic events similar to those that may cause Post-Traumatic Stress Disorder (PTSD) in traditional combatants, RPAS crew members may face an additional challenge unique to remote operations: lack of deployment rhythm and of combat compartmentalization. The impact of fighting a war on-base and going home to family at night obliterates the clear demarcation between combat and personal life.[18,19]

In contrast to traditional expeditionary operations, in which entire units deploy overseas, RPAS operators work in the social isolation of their rotating shifts in the GCS. Deployed units foster the development of

Table 18 – Human Element Vulnerability Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

organizational identity and unit cohesion which may help service members cope with the stresses of combat. Social isolation of RPAS operations could diminish unit cohesion and thereby increase susceptibility to PTSD.[20,21] From 2005 through 2011, the percentages of US Air Force RPAS pilots with mental health issues were higher than pilots from manned aircraft.[22]

7.3.3 Vulnerability Assessment

Within the AOO, adversaries may engage RPAS personnel with any available weapons, e.g. combat aircraft, artillery or infantry. Therefore, the vulnerability of RPAS personnel is equal to that of any other military personnel deployed to the AOO. Hence, the vulnerability rating of RPAS personnel within the AOO is assessed as 'moderate' because this study assumes an adequate level of force protection for deployed personnel. Conversely, RPAS RSOs offer different opportunities for an adversary to conduct covert attacks. SOF assets or other types of asymmetric force can be employed against mission critical RPAS personnel in non-secure (civilian) environments. Due to the limited number of trained and experienced RPAS personnel available and their ability to be easily identified, aircrews may be designated by an adversary as a high value target. As this study could not identify any protective measures currently in place for the off-duty environment of non-deployed personnel, the vulnerability of RPAS personnel to attacks by asymmetric forces is estimated as 'high'. (cf. Table 18)

1. Lance Menthe, Amado Cordova, Carl Rhodes, Rachel Costello, Jeffrey Sullivan, 'The Future of Air Force Motion Imagery Exploitation', RAND Corporation, 2012.
2. PJ Neal, SMALL WARS JOURNAL, 'From Unique Needs to Modular Platforms: The Future of Military Robotics', 19 Oct. 2011. [Online]. Available: http://smallwarsjournal.com/sites/default/files/886-neal.pdf. [Accessed 16 Apr. 2013].
3. Remote Split Operations can be described as UAS operations that involve the geographical separation of the launch and recovery sites from the mission control element.
4. Ann Stefanek, Secretary of the Air Force Public Affairs, 'Air Force announces basing candidates for remote split operations squadron', U.S. Air Force Public Affairs Office, 21 Oct. 2011. [Online]. Available: http://www.shaw.af.mil/news/story.asp?id=123276815. [Accessed 02 Dec. 2013].
5. Ibid. 1.
6. Maj. Gabe Johnson, 'Air Guard selects Predator pilot for Sijan Award', Arizona National Guard, 22 Oct. 2009. [Online]. Available: http://www.nationalguard.mil/news/archives/2009/10/102609-Air.aspx. [Accessed 02 Dec. 2013].
7. Robert Riggs, 'Predator Drone TV: Eye in the Sky Protects Soldiers in Iraq and Afghanistan', 24 Sep. 2011. [Online]. Available: http://robertriggs.com/2011/09/24/predator-drone-tv-eye-in-the-sky-protects-soldiers-in-iraq-and-afghanistan/. [Accessed 02 Dec. 2013].
8. Gary Parsons , 'First Predator exchange pilot', Air Forces Monthly, 09 Feb. 2010. [Online]. Available: http://www.airforcesmonthly.com/view_article.asp?ID=1518. [Accessed 02 Dec. 2013].
9. Maj. Gabe Johnson, 'Pilot makes history after graduating from Weapons School', Nellis Air Force Base, 17 Dec. 2009. [Online]. Available: http://www.nellis.af.mil/news/story.asp?id=123182794. [Accessed 02 Dec. 2013].
10. 'UAV Operators Get Wings, Flight Pay', 08 Oct. 2009. [Online]. Available: http://christianfighterpilot.com/blog/2009/10/08/uav-operators-get-wings-flight-pay/. [Accessed 03 Dec. 2013].
11. Ibid. 6.
12. Ibid. 7.
13. Ibid. 8.
14. Ibid. 9.
15. Ibid. 1.
16. Levi Newman, 'Do Unmanned Aircraft Operators Suffer from PTSD?', Veterans United, 2012. [Online]. Available: http://www.veteransunited.com/network/do-unmanned-aircraft-operators-suffer-from-ptsd/. [Accessed 11 Jul. 2013].
17. P. C. Nolin, Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance, NATO Parliamentary Assembly, 2012.
18. Hernando J. Ortega, Jr., MD, MPH, 'Challenges in Monitoring and Maintaining the Health of Pilots Engaged in Telewarfare', Medical Surveillance Monthly Report, vol. 20, no. 3, p. 2, Mar. 2013.
19. Jean L. Otto, DrPH, MPH; Bryant J. Webber, MD (Capt, USAF), 'Mental Health Diagnoses and Counselling Among Pilots of Remotely Piloted Aircraft in the United States Air Force', Medical Surveillance Monthly Report, vol. 20, no. 3, pp. 3-8, Mar. 2013.
20. Ibid. 18.
21. Ibid. 19.
22. Ibid. 19.


© US Air Force, Master Sgt. Steve Horton

7.4 Control Element

The Control Element consists of three components: the physical infrastructure (external hardware), computer systems (internal hardware) and a non-physical (software) component. All of them may be subjected to different types of attack. The GCS and its associated communication equipment form the physical part of the control element while the software running the control element's computer systems forms the non-physical part. The physical part may be subject to attack by kinetic weapons while the non-physical part may be subject to attack through cyber-warfare. One important difference between a kinetic and cyber-attack is that a kinetic attack always requires the attacker to be in relatively close proximity to the intended target. For a cyber-attack, this is not the case.

7.4.1 Detection and Engagement Avoidance

7.4.1.1 External Hardware Components. The Control Element's prominent hardware components typically consist of a shelter or trailer containing the controls to operate the RPA and a satellite earth terminal for BLOS communications. Due to their unique size and shape, the hardware components may serve as a means to positively identify them as RPAS components to an adversary. Additionally, their persistent radio transmissions may also reveal their location to enemy electronic reconnaissance.

Deployable GCS shelters usually have standard dimensions of 12 ft or 24 ft to fit common transport requirements. They are similar in appearance to other military shelters used for a variety of purposes. Some GCS also use a 30 ft trailer to house the hardware components. This results in a more distinctive appearance as compared to other standard military C2 equipment. However, the directional antenna used for LOS communication may distinguish the GCS from other general purpose or C2 shelters.[1]

Non-deployable GCS integrated into a base's existing infrastructure help to make them indistinguishable from other multi-purpose buildings. Although

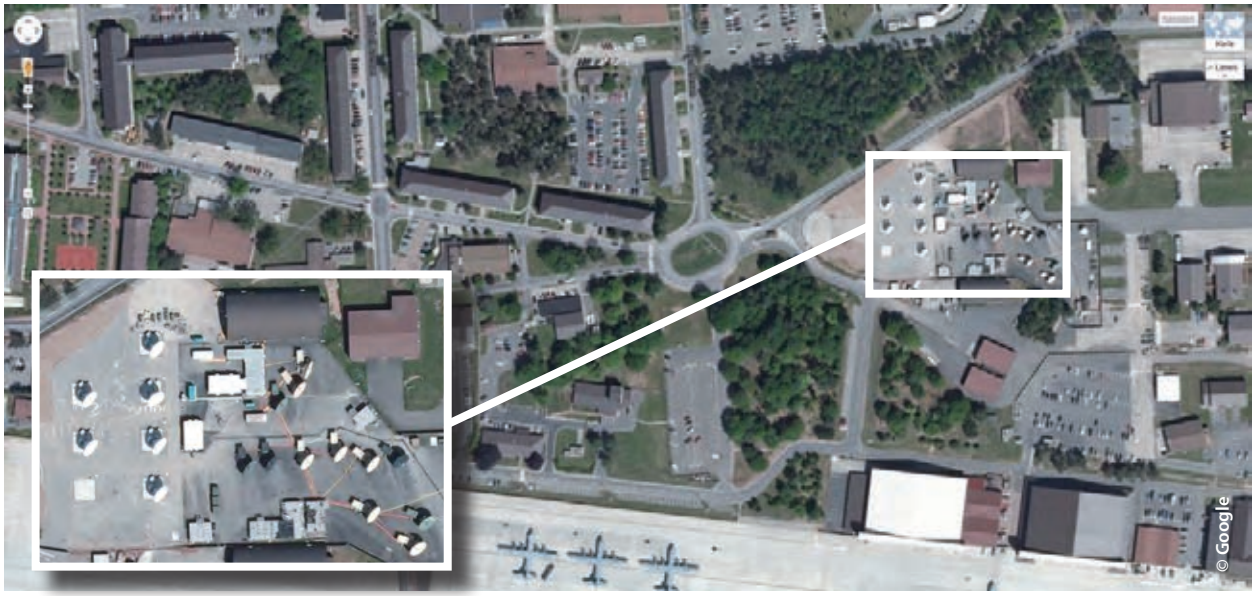


Figure 17 – Google Earth Imagery of Satellite Earth Terminals at a Military Airbase in Europe.[3]

roof mounted communication equipment may reveal the purpose of the building, an adversary would need precise intelligence, e.g. the building's blueprints, to locate the GCS inside the infrastructure. The most prominent characteristics of any GCS are the BLOS satellite earth terminals which can have antenna diameters of several metres. For example, the Predator Primary Satellite Link (PPSL) uses a 20 ft / 6.1 m satellite dish. Communication antennas of this size are easily recognizable, since they require a minimum safety distance from surrounding equipment and personnel due to the radiation hazard. Fixed installations of satellite earth terminals could even be identified by using publicly available Google Earth pictures.[2] (cf. Fig. 17)

Depending on the location of the GCS, the location of the satellite earth terminal may vary. Fixed GCS installations in the MCE may not have their own satellite dish. They could use a wired network infrastructure to link them to a distant satellite earth terminal located remotely (even on another continent). For example, RPAS operations in the Middle East may use satellite earth terminals at Ramstein Air Force Base (AFB) in Europe for BLOS communication with the RPA and use the wired portion of the military network to connect the satellite earth terminal to the MCE at Creech AFB and to the PED element at Langley AFB, both in the United States.[5] Conversely, deployed GCS usually have their own satellite earth terminal nearby and do not typically have a wired network infrastructure. Deployed GCS are more exposed to detection by enemy electronic reconnaissance as their radio transmissions originate within or close to the AOO and therefore within the possible range of an adversary. In summary, the probability of locating, identifying and engaging an RPAS control element depends on its physical location. Its exposure to enemy kinetic actions is 'high' if the control element is located inside the AOO while it is 'moderate' to 'low' if it's not. Home-based RPAS control elements may not be identified if they are located far from SATCOM equipment or if they are covertly integrated into other military infrastructure.

7.4.1.2 Internal Hardware Components. Military computer systems similar to those used in the GCS, Satellite Earth Terminals or Mission Control Centres often include COTS components or sub-components although the complete system is usually adapted and configured to the military's specific requirements. The supply chain for microelectronics is extremely diffuse, complex, and globally dispersed, making it difficult to verify the trust and authenticity of the electronic equipment used in the RPAS. Identifying the multiple

Figure 18 – Example of a Microelectronics Global Supply Chain based on the Apple iPhone 5.[9]

layers of subcontractors and suppliers contributing to the design or fabrication of a specific chip is difficult; tracing all of the contributors for a complete integrated circuit is even more so. Hence, this widely dispersed supply chain may provide an adversary with opportunities to manipulate those components or penetrate the distribution chain with counterfeit products.[6] (cf. Fig. 18)

Deliberate modification of the product assembly and delivery could provide an adversary with the prospect of gaining covert access and monitoring of sensitive systems, to degrade RPAS mission effectiveness, or to insert false information or instructions that could cause premature failure or complete remote control or destruction of the targeted RPAS.[7] Hardware-level vulnerabilities can also be exploited to completely sidestep software-based security countermeasures. For example, a team of university researchers recently demonstrated that carefully chosen alterations in portions of a chip involved in encryption processing could allow an attacker to extract encryption keys.[8]

This study could identify only one official initiative aimed at establishing reliable and trustworthy supply chains of microelectronics for military purposes. This leads to the assumption the threat from corrupted supply chains has not yet drawn the appropriate attention that it should.[10] Due to the prevalence of COTS components inside military computer systems, the vulnerability to this form of cyber-warfare is assessed as 'high'.

7.4.1.3 Software Components. To destroy, disrupt or infiltrate the software portion of the Control Element, an adversary must first gain access to the network, either directly or remotely. The software components necessary to operate an RPAS are not limited to the GCS, but also include the aircraft, satellites and ground stations if applicable, as well as support systems for logistics, maintenance or PED. This provides an adversary with a broad spectrum of possible entry points into the RPAS network.[11]

Traditionally, each RPAS was procured as a fully integrated, vendor-specific solution, consisting of the air system, ground station, communications channels, encryption technologies and payloads. These single-system variants were typically 'closed' systems utilizing proprietary interfaces throughout the system architecture. To overcome this vendor-centric approach, an open RPAS architecture is currently under development which should utilize common interface standards.[12,13]

Another current development integrates different RPAS operating systems under one single platform. This enables an operator to control several different types of RPAS from a single control station. Depending on the complexity of the RPAS, control may even be possible from a tablet computer or mobile phone.[14,15] Extensive experience with public computer operating systems such as Microsoft Windows, Apple OS or Open Source Linux show that the more widely a software platform is used, the more it is subject to attack.[16] Open architecture, common standards and cross-system operating systems for RPAS may therefore increase the exposure of friendly computer systems to cyber-attacks, as an adversary could focus his efforts on a commonly distributed platform more efficiently.

Eventually the human factor may be exploited to gain access to the RPAS. Even highly secured and physically separated military networks may be infiltrated through the identification of potential individual targets. These individuals can then serve as the optimal channel to work for the adversary within the targeted military organization. It would be preferable for the adversary to have the target do this unwittingly, but they can also be manipulated through blackmail, if necessary. The intelligence needed for such an intrusion is usually gathered through social networks or other open sources. This intelligence would be used to construct a profile of the person to be attacked and to identify penetration points. Such information gathering and the construction of a suitable profile requires comprehensive information gathering based on good organizational skills and resources.[17,18] Although current protective measures – such as those discussed in the next chapter – ensure an adequate level of cyber-security, they cannot guarantee absolute security. Hence, the exposure of the RPAS software components to cyber-attacks is assessed as 'moderate'.

7.4.2 Hit Avoidance

7.4.2.1 External Hardware Components. The best way to protect the Control Element is to keep its location or even its existence hidden from the adversary. This may work well for a Control Element based in the home country, but this study identified several public discussions in the media revealing the current and planned locations of RPAS Squadrons and Control Elements across NATO.[19,20,21] Achieving the same level of protection for deployed GCS may be more difficult as they are typically within or near the adversary's striking range. However, deployed GCS will benefit from the force protection measures available within the respective AOO, providing them with an appropriate level of defence.

7.4.2.2 Internal Hardware Components. Currently, cyber-security is considered a 'software-only' concern. Although there are some national programs in place to assure the secure production of the most sensitive microchips, they are used for only a small fraction of the chips in defence systems.[22] The greatest supply chain security exposure for defence applications comes not from the small fraction of chips designed and manufactured uniquely for defence systems but from the massive flow of commercial chips into those systems. Additionally, when purchasing computers, routers, navigation and communications equipment and most other electronics hardware, the military is heavily reliant on the commercial supply chain and therefore exposed to any associated vulnerabilities. Yet the supply chain for commercial components is almost completely unprotected against intentional compromising. A skilled attacker could embed latent malicious functionality and could exploit it months or years later to disrupt a system containing the compromised chip.[23]

7.4.2.3 Software Components. As discussed in chapters 6.8.2 and 6.8.4, military networks are usually separated from the public internet. This is done to provide the first line of physical or logical defence and protect them from unauthorized remote access. RPAS are one of many nodes in the entire network centric environment and countermeasures providing cyber-security are usually applied using a comprehensive approach. Current security software suites offer a variety of methods to counter cyber-attacks. They typically include Antivirus, Configuration Change Detection, Device Control, Host Intrusion

Prevention, Firewall and Rogue System Detection Modules. Many of these modules are COTS applications integrated into the military security system.[24] However, cyber-security is an extremely fast and adaptive battlefield. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms because they can only defend against threats already known to the software, either by its signature or behaviour. Hence, regular security updates are essential in providing an acceptable level of protection.[25]

7.4.3 Hit Tolerance

MALE RPAS conducting remote split operations usually have an inherent redundancy of their mission control infrastructure. Once the RPA is airborne and linked to the satellite, it can be controlled by any GCS that can establish a remote connection. However, the physical destruction of a single GCS or exploiting its compromised hardware or software components to produce system failures will likely disrupt the current RPAS operation. Depending on the severity of the attack, it may be possible to lose the RPA if attempts to regain control of the aircraft and automated emergency flight procedures fail or the aircraft's avionics are affected. In a worst case scenario, assuming all the deployed GCS of an RPAS necessary to launch and recover the RPA are inoperable or rendered useless and no local control element redundancy is available; RPAS operations could come to a halt in their respective AOO because current systems lack the capability of BLOS launch and recovery. Consequently, the magnitude of control element failure is assessed as 'high' with respect to LOS operations in general and for deployed GCS in particular. For remote BLOS operations and home-based GCS, the magnitude is assessed as 'moderate' due to possible threat mitigation through the use of redundant control elements.

7.4.4 Vulnerability Assessment

The Control Element's satellite earth terminals with diameters of up to several metres are easily recogniz-

Table 19 – Control Element Vulnerability Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

able and may facilitate the positive identification of the GCS to an alert adversary. Deployable GCS may be identified more easily because of the proximity of their communications equipment. But even if it is not possible to identify the GCS shelter, attacking the often highly exposed and unhardened satellite dish and its receiver could cause enough damage to render the control element useless. Such an attack can be conducted with any weapon capable of delivering the desired kinetic effect to the satellite dish. Depending on the range requirements, this could include high calibre sniper rifles. The control element's vulnerability to kinetic effects is assessed as 'high'.

The RPAS control element's vulnerability against cyber-attacks is closely linked to the vulnerabilities of the military network's COTS hardware and software. Although GCS are usually not supposed to be connected to the public internet, (making them largely immune to viruses and other network security threats), it has been proven they were infected with a key logging virus in 2011. The physical separation between classified and public networks has been compromised, largely through the improper use of discs and removable drives. In late 2008, malicious code was introduced to hundreds of thousands of US Defense Department computers and the disinfection of the compromised systems took several years.[26] The control element's vulnerability to cyber-attacks is assessed as 'high'. (cf. Table 19)

1. 'Ground Control Stations (GCS)', General Atomics Aeronautical, [Online]. Available: http://www.ga-asi.com/products/ground_control/index.php. [Accessed 05 Dec. 2013].
2. Google Earth, [Online]. Available: https://www.google.de/maps/. [Accessed 05 Dec. 2013].
3. Ibid. 2.
4. Bryan William Jones, 'Creech AFB UAV Operations', 22 Feb. 2008. [Online]. Available: http://prometheus.med.utah.edu/~bwjones/2008/02/creech-afb-uav-operations/. [Accessed 05 Dec. 2013].
5. Ibid.
6. Bryan Krekel, Patton Adams, George Bakos, 'Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage', Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp, 2012.
7. Ibid.
8. Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson, 'Stealthy Dopant-Level Hardware Trojans', University of Massachusetts Amherst, USA, TU Delft, The Netherlands and ALaRI - University of Lugano, Switzerland, Horst Goertz Institut for IT-Security, Ruhr-Universitaet Bochum, Germany, 2012, 2013.
9. 'sourcemap - where things come from', Sourcemap Inc., [Online]. Available: https://sourcemap.com/view/4588. [Accessed 12 Dec. 2013].
10. 'Trusted Foundry Program', Defense Microelectronics Activity (DMEA), [Online]. Available: http://www.dmea.osd.mil/trustedic.html. [Accessed 06 Jan. 2014].
11. Parag Batavia, Ph.D., Rich Ernst, Kerry Fisherkeller, Doug Gregory, Rob Hoffman, Ann Jennings, George Romanski, Brian Schechter, Gordon Hunt, 'The UAS Control Segment Architecture', Raytheon, 2011.
12. Ibid.
13. 'UAS Control Segment (UCS) Architecture', UCS Working Group, [Online]. Available: https://www.ucsarchitecture.org/pages/home. [Accessed 07 Dec. 2013].
14. SANDRA I. ERWIN, 'Pentagon Recruiting Software Developers For Drone "App Store"', National Defense, pp. 26-27, Oct. 2013.
15. 'BALLISTA | Unmanned Common Control System', DreamHammer Inc., [Online]. Available: http://www.dreamhammer.com/ballista.shtml. [Accessed 05 Dec. 2013].
16. 'Sophos Security Threat Report', Sophos Ltd., 2013.
17. Gabi Siboni, Y. R., 'What Lies behind Chinese Cyber Warfare', in Cyberspace and National Security, Tel Aviv, Institute for National Security Studies (INSS), Jun. 2013, pp. 45-60.
18. Geoffrey Ingersoll, 'Defence Science Board Warns Of "Existential Cyber Attack"', Business Insider Australia, 07 Mar. 2013. [Online]. Available: http://www.businessinsider.com.au/cyber-exploits-turn-weapons-on-us-2013-3. [Accessed 13 Jan. 2014].
19. Lorenzo Franceschi-Bicchierai, 'Revealed: 64 Drone Bases on American Soil', WIRED.com, 13 Jun 2012. [Online]. Available: http://www.wired.com/2012/06/64-drone-bases-on-us-soil/. [Accessed 16 Jun 2014].
20. 'DoD Current and Future U.S. Drone Activities Map', publicintelligence.net, 12 Jun 2012. [Online]. Available: http://publicintelligence.net/dod-us-drone-activities-map/. [Accessed 16 Jun 2014].
21. 'RAF Reaper drone squadron stood up at RAF Waddington', BBC News, 23 Oct 2012. [Online]. Available: http://www.bbc.com/news/uk-england-20039085. [Accessed 16 Jun 2014].
22. Ibid. 10.
23. John Villasenor, 'Compromised By Design? Securing the Defense Electronics Supply Chain', Center for Technology Innovation (CTI) in Governance Studies at Brookings and Center for 21st Century Security and Intelligence (21CSI) in Foreign Policy at Brookings, Nov. 2013.
24. 'Host Based Security System (HBSS)', Defense Information Systems Agency (DISA), [Online]. Available: http://www.disa.mil/Services/Information-Assurance/HBSS. [Accessed 10 Dec. 2013].
25. David Harley, Andrew Lee, 'Heuristic Analysis - Detecting Unknown Viruses', ESET, [Online]. Available: http://www.eset.com/us/resources/white-papers/Heuristic_Analysis.pdf. [Accessed 11 Dec. 2013].
26. Noah Shachtman, 'Computer Virus Hits U.S. Drone Fleet', WIRED.com, 10 Jul. 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. [Accessed 07 Jan. 2014].

7.5 Data Links

'Right now, most UAS don't even have Link-16, the NATO standard for data links first established in the 1990s. In the benign airspace over Afghanistan, Marine operators can control their Shadow drones just fine but they must rely on voice communications over radio to talk to troops on the ground. The biggest number-one issue is we can't talk to the people we need to... digitally. There are no encrypted data links.'

Lieutenant Colonel Kevin Murray,
Commanding Officer Marine UAS Squadron 1,
AUVSI Annual Conference 2012

Data links connect the RPA with the GCS, enabling operators to remotely control the RPA and receive transmissions. Data links can be established either by radio for LOS communications or satellites and network nodes for BLOS communications. The radio transmissions may be subject to attack by EW whereas the network nodes may be attacked by means of cyber-warfare.

The RPAS hardware and software components' vulnerabilities against cyber-threats have been outlined in the previous chapter. These vulnerabilities also apply to the data link's network nodes used for BLOS communications. Therefore, this chapter focuses on the vulnerabilities of RPAS radio transmissions only. An adversary targeting RPAS radio transmissions has two options; using transmissions to jam or spoof a targeted receiver or using a receiver to exploit a transmitted signal.

7.5.1 General Radio Antenna Characteristics

The radio signals establishing communication between the RPA, the GCS and possibly the satellite are usually transmitted and received by directional antennas. This is to ensure transmitters only broadcast in the direction of the intended receiver and receivers only receive transmissions from the intended transmitter. Some RPA also use omnidirectional antennas to broadcast their FMV stream in all directions to enable ground troops to receive the FMV signal.[1]

Figure 19 and Figure 20 illustrate an example of the radiation patterns of directional and omnidirectional antennas, whereas the receiving pattern of the respective antenna can be inferred, i.e. the antenna's receiving pattern is the same as the radiation pattern. Directional antenna receivers usually use side lobe suppression to filter out unwanted signals below a defined threshold and to only receive the preferred main lobe signals.

Modern Ku-band antennas produce a narrow main lobe beam of less than 10 degrees and low side lobes. Jammers which do not enter directly into the main lobe of the antenna can be substantially attenuated. When received via side lobes, jammers are attenuated by approximately 20 dB for the first side lobe and by an even greater amount for the additional side lobes. Antennas designed for particularly low side lobes reach an attenuation of greater than 40 dB, which means, if an adversary seeks to jam a signal via side lobe injection, it must be more than 10,000 times stronger than the original signal received by the main lobe.[2]

7.5.2 Detection Avoidance

To lower the probability of interception, radio communications between the RPAS transmitters and receivers often use highly directional antennas with narrow beams and frequencies in the Extremely High Frequency (EHF) spectrum. Additionally, the signal can either be spread over a wider spectrum or modulated with a random noise pattern to make it appear noise-like. The signal can also be rapidly moved around in the frequency spectrum to further reduce its detection. These measures significantly reduce the area from which an adversary could intercept RPAS communications.[3,4]

7.5.3 Engagement Avoidance

To interfere with RPAS radio receivers, an adversary must inject the spurious signal in line with the receiving patterns of the targeted antenna. To attain the highest probability for a successful attack, the adversary must inject the spurious signal into the main lobe. With sufficient energy, a side lobe injection may also exceed the receiver's suppression threshold and override the main lobe signal. However, even if side lobe attacks enlarge the angle for possible signal injections, it is still narrow enough that an adversary must locate the transmitter. The RPAS contains several receivers and, depending on their alignment, they may be vulnerable to electromagnetic interference from a variety of angles.

7.5.3.1 Remotely Piloted Aircraft. RPA typically use two or more antennas to maintain their data link to the GCS and the satellite. Antennas to receive signals from the GCS face downwards and may be directional or omnidirectional. Antennas to receive satellite signals face upwards and are typically directional.[5] As the omnidirectional LOS antennas are usually only used for launch and recovery, the timeframe to interfere with the LOS data link is quite short. Unfortunately, the RPA is vulnerable to a possible data link loss especially during the landing phase. This may cause the loss of control of a landing RPA and possibly the loss of the aircraft. The directional antenna for satellite communication can be considered less vulnerable to ground-based electromagnetic interference, as neither its main lobe nor side lobes face the ground. Successfully injecting signals into the RPA's satellite antenna requires either airborne or space-based EW assets.

7.5.3.2 Ground Control Station. Like the RPA, the GCS uses separate, directional antennas for LOS and BLOS communications. Depending on the position of the RPA or satellite, the LOS and BLOS antenna may have to be aimed at shallow angles and in the

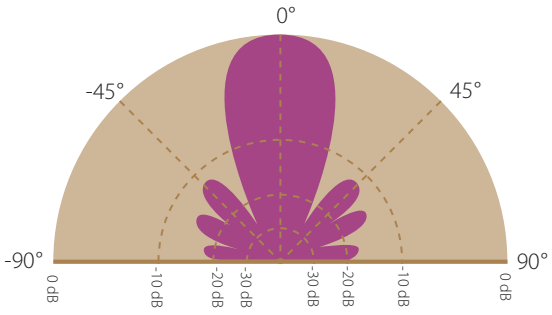


Figure 19 – Directional Antenna Radiation Pattern.

direction of enemy forces. This may possibly expose the main lobe to electromagnetic interference. Maintaining LOS communication with a low flying RPA during recovery makes the LOS antenna even more susceptible to electronic attack. As previously discussed, disrupting LOS communication during recovery operations may result in loss of aircraft. Unfortunately, critical LOS communication links can be disrupted with commercially available equipment. Simple disrupters made from 1950s technology can be fabricated in a few hours with $200 worth of readily available electronic equipment.[6] COTS terrestrial jammers can also be easily purchased commercially. These jammers are known to have typical ranges of 3-5 km in urban areas. In rural areas, their range can be up to 20 km.[7]

7.5.3.3 Satellite. Geostationary communication satellites usually cover a large area of the Earth's surface. Although military satellites using phased-array antennas and nullifying techniques can tailor their coverage to the desired AOO and filter out signals from unwanted sources, most satellite bandwidth has been provided by civilian contractors in recent operations.[8] To disrupt satellite communications, an adversary could transmit spurious signals from any location inside the satellite's footprint. Military grade equipment is not necessarily required to conduct an electronic attack on receiving antennas. Any civilian broadcasting station is capable of interfering with the satellite uplink.[9] The analysis of commercial SATCOM links over a 16-month period during OIF found 50 documented instances of interference with military communications over commercial SATCOM; five of those attacks were confirmed as originating from hostile sources.[10]

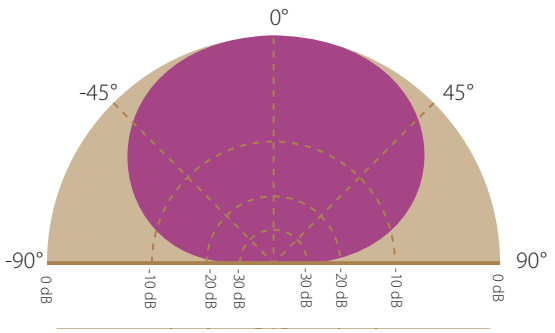


Figure 20 – Omnidirectional Antenna Radiation Pattern.

7.5.3.4 Satellite Ground Segments. Ground segment attacks or sabotage to disrupt space assets is an attractive option for low-technology or cash-strapped groups such as terrorists or transnational insurgents. Critical ground control facilities associated with space systems, both military and civilian, are targets to terrorist cells and adversary SOF. While military ground control facilities have the benefit of being operated and secured by military personnel, commercial ground control facilities generally don't have that luxury. Adversaries need only to determine which ground facilities are critical to RPAS operations – especially those that offer non-redundant vulnerabilities – and where they are located. Unfortunately, information on many of these facilities is available in open-source reference materials.[11]

7.5.4 Hit Avoidance

Immunity from the effects of jamming is an unrealistic goal, but measures should be taken to minimize their effects. Digital signal processing enables modern receivers to discriminate radio signals from different sources and to nullify interference from unexpected directions. It can also enable transmitters and receivers to encode, decode and hash the signal with a computed checksum so that it can be distinguished from other signals and partial signal losses can be corrected.[12] To prevent exploitation of RPAS broadband transmissions, the data links of many, but not all, RPAS are encrypted. Given a sufficient encryption key length and complexity, current cryptographic methods can be classified as virtually immune against any type of real-time exploitation.

7.5.5 Hit Tolerance

Depending on the level of automation and the mission phase, the impact of a data link loss can vary. Data link disruption can also occur even in a benign environment due to atmospheric disturbances. Therefore, contingency procedures are typically designed into the RPAS. In case of a temporary signal loss, current RPAS operating in BLOS mode are usually programmed to continue with their mission and head for their next assigned waypoint on their flight plan. If the disruption

exceeds a given time span, the system will execute automated contingency flight manoeuvres. Some RPAS climb to higher altitudes, some fly ascending circles or reverse their trajectory to regain their data link. If these flight manoeuvres are unsuccessful in regaining the data link, some RPAS automatically return to their base or to a pre-programmed recovery site. Some smaller systems may simply eject a parachute and execute an emergency landing on the spot. This loss may be compensated by another RPAS in the vicinity if it is available. If the data link is lost during a critical mission state, e.g. target tracking or weapon release, this option may result in mission failure. Recovery of RPAS is usually conducted in the LOS mode to avoid the inherent latency of satellite communications. This latency may cause problems with delayed situational awareness and reaction time during the RPA's landing approach. Data link disruption in this critical phase may result in catastrophic damage and loss of the aircraft.

7.5.6 Additional Considerations

7.5.6.1 Bandwidth Congestion. Current operational requirements for FMV already exceed the bandwidth capacity of available military spacecraft. The development of new FMV feeds exacerbates this issue. Current RPAS with wide-area surveillance sensors are able to produce 10 FMV streams simultaneously. That capability is expected to increase to greater than 50 FMV streams simultaneously. More bandwidth is required to facilitate ISR operations and the bandwidth pressure will only increase as wide-area surveillance tools grow more capable and new high definition sensors and advanced radars are integrated in the RPAS. To try to keep up, the military has leased bandwidth from commercial carriers for more than a decade. It is further estimated that demand for satellite communications could almost triple a decade from now.[13,14,15] Although allocation of limited bandwidth has been a known challenge in military operations (and is not unique to RPAS operations), operations in contested environments may further reduce the available electromagnetic spectrum due to enemy ECM.

7.5.6.2 RPAS Radio Transmissions Exploitation. To enable ground troops to receive the FMV stream, a separate signal can be broadcasted from the RPA. The FMV stream is usually transmitted by an omnidirectional antenna in order to provide the signal to a wider area. Like any radio transmission sent over great distances, these signals may be subject to exploitation by the enemy.[16] Militants in Iraq have reportedly intercepted Predator RPAS video feeds by taking advantage of an unprotected communications link and using COTS software programs available for as little as $25.95 on the Internet. Multiple discoveries of pirated RPAS video feeds on militant laptops have proven that militant groups have adapted their tactics and were regularly intercepting FMV feeds.[17] Shortly after these security issues were revealed, encryption of FMV streams were designated a high priority. Unfortunately, it is estimated the total U.S. RPAS fleet won't see its communications secured until 2014 as the Remotely Operated Video Enhanced Receivers (ROVER) necessary to decrypt the new FMV feed must also be upgraded.[18,19] (cf. Fig. 21)

This study assumes not all currently fielded RPAS are capable of transmitting encrypted video feeds. This is especially a concern for smaller systems with SWaP limitations that may prevent the installation of additional encryption equipment.

Figure 21 – ROVER System.

7.5.6.3 Global Positioning System. Because RPAS use a GPS data link to determine its precise location, it is highly important this link is maintained to ensure mission success. The GPS signal strength measured at the surface of the Earth is about –160dBw, which is roughly equivalent to viewing a 25-Watt light bulb from a distance of 10,000 miles. This weak signal can easily be jammed by a stronger power transmission in a similar frequency.[20,21] The GPS signals are currently transmitted on two D-band frequencies or links. The signal used commercially is transmitted only on one link whereas an encrypted military signal is transmitted on both links. This encryption prevents military GPS receivers from being spoofed by false GPS transmissions as long as these receivers are configured to use the encrypted signals only. However, those receivers could also be configured to use the unencrypted signals as an alternative if the encrypted one is too weak or disrupted.[22] A military grade GPS receiver operating with the encrypted GPS signals is virtually immune from spoofing attempts. Unfortunately, this does not prevent the receiver from being jammed. In contrast to the other highly directional antennas, a typical GPS patch antenna must be able to receive signals from virtually the entire sky. The advantage of this design is that even signals from satellites which are just above the local horizon can be received. Unfortunately, this design is susceptible to a broad range of interference and misconfigured military GPS receivers could be forced to use unencrypted signals, which can then be spoofed if an adversary is capable of successfully jamming the encrypted signals.

Since a report on GPS vulnerabilities was released by the U.S. Department of Transportation (known as the Volpe-Report[23]) in 2001, many enhancements to ensure GPS reliability have been developed. For example, modern Controlled Radiation Pattern Antennas (CRPA) capable of differentiating between the GPS satellite signal, interfering signals from other sources and providing substantial jam-resistance up to a certain degree have been developed.[24] The continuing modernization of the GPS system to include adding additional frequencies and increasing GPS signal

Table 20 – Data Link Vulnerability Matrix.

RPAS Elements \ Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

strength aims to further enhance reliability and jam-resistance.[25] However, like any radio navigation system, GPS is vulnerable to interference that can only be reduced but not totally eliminated.[26] The ability to jam communications is a simple question of power. If sufficient power is available, any frequency within the electromagnetic spectrum can be jammed.[27]

7.5.7 Vulnerability Assessment

Current systems are not yet fully automated or even autonomous and their control is contingent on uninterrupted communications. Although much effort has been spent on reliability measures such as anti-jamming, encryption or redundancy, the adverse effects of EW may not be completely averted. The communication nodes of RPAS are complex and their vulnerability to EW ranges from 'low' to 'high' depending on the antenna type and alignment. As this study assumes that a capable adversary would focus their efforts on the most vulnerable areas, the overall vulnerability rating to EW attacks is assessed as 'high'.

Disrupting RPAS data links by taking out the originators of the transmissions, i.e. the GCS, RPA and satellite, or by acquiring access to any of these components by means of cyber-warfare is also a viable option for an adversary. The vulnerability assessments to those types of attacks have been addressed in previous chapters. Their respective assessments have been brought forward in the chart below. (cf. Table 20)

1. Major Jaysen A. Yochim (US Army), US Army Command and General Staff College, 'The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack', Jan. 2010. [Online]. Available: http://www.fas.org/irp/program/collect/uas-vuln.pdf. [Accessed 16 Apr. 2013].
2. Wolfgang W. Rochus, 'UAV Data-Links: Tasks, Types, Technologies and Examples', DaimlerChrysler Aerospace, Ulm, 1999.
3. R. Poisel, Modern Communications Jamming Principles and Techniques 2nd Edn, 2011.
4. A.B. Glenn, 'Low Probability of Intercept', 2010.
5. Steve Bonter, Diana R. Dunty, Jason Greene, and Dr. William Duff, 'Predator UAV Line-Of-Sight Datalink Terminal Radio Frequency Test Report', Alion Science and Technology, Sep. 2004.
6. P. C. Nolin, Countering the Afghan Insurgency: Low Tech Threats, High-Tech Solutions, NATO Parliamentary Assembly, 2011.
7. Pierluigi Paganini , 'Hacking Satellites . . . Look Up to the Sky', INFOSEC Institute, 18 Sep. 2013. [Online]. Available: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/. [Accessed 08 Jan. 2014].
8. Loren B. Thompson, Ph.D., 'Lack of Protected Satellite Communications Could Mean Defeat for Joint Force In Future War', Lexington Institute, 14 Apr. 2010. [Online]. Available: http://www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war?a=1&c=1171. [Accessed 25 Jun. 2013].
9. Ibid. 7.
10. Ibid. 7.
11. Lieutenant Colonel Karl Ginter, Space Technology and Network Centric Warfare: A Strategic Paradox, U.S. Army War College, Feb. 2007.
12. Ibid. 3.
13. Noah Shachtman, 'Pentagon Paying China — Yes, China — To Carry Data', WIRED.com, 29 Apr. 2013. [Online]. Available: http://www.wired.com/dangerroom/2013/04/china-pentagon-satellite/?cid=co7577104. [Accessed 13 Jan. 2014].
14. Joint Defense Science Board Intelligence Science Board Task Force, 'Integrating Sensor-Collected Intelligence', Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C., Nov. 2008.
15. Marc V. Schanz, Air Force Magazine, 'The Reaper Harvest', Apr. 2011. [Online]. Available: http://www.airforcemag.com/MagazineArchive/Pages/2011/Apr.%202011/0411reaper.aspx. [Accessed 16 Apr. 2013].
16. Siobhan Gorman, Yochi J. Dreazen and Aug. Cole , 'Insurgents Hack U.S. Drones', The Wall Street Journal, 17 Dec. 2009. [Online]. Available: http://online.wsj.com/news/articles/SB126102247889095011. [Accessed 08 Jan. 2014].
17. Ibid.
18. 'U.S. Army working to encrypt UAV video feeds', Homeland Security News Wire, 21 Dec. 2009. [Online]. Available: http://www.homelandsecuritynewswire.com/us-army-working-encrypt-uav-video-feeds?page=0,0. [Accessed 08 Jan. 2014].
19. Noah Shachtman and David Axe, 'Most U.S. Drones Openly Broadcast Secret Video Feeds', WIRED.com, 29 Oct. 2012. [Online]. Available: http://www.wired.com/dangerroom/2012/10/hack-proof-drone/. [Accessed 08 Jan. 2014].
20. 'NAVSTAR GPS User Equipment Introduction', Sep. 1996.
21. Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., GPS Spoofing Countermeasures, Los Alamos, New Mexico: Los Alamos National Laboratory, Dec. 2003.
22. Ibid. 20.
23. John A. Volpe National Transportation Systems Centre, 'Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System', Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, Aug. 2001.
24. Thales Aerospace Division, 'TopShield - The ultimate GPS anti-jam solution', 2009. [Online]. Available: https://www.thalesgroup.com/en/content/top-shield-ultimate-gps-anti-jam-solution. [Accessed 09 Jan. 2014].
25. 'GPS Modernization', National Coordination Office for Space-Based Positioning, Navigation, and Timing, 25 Sep. 2013. [Online]. Available: http://www.gps.gov/systems/gps/modernization/. [Accessed 09 Jan. 2014].
26. Ibid. 23.
27. Ibid. 1.

© US Air Force, Col. Marty Franc

7.6 Support Element

'The most valuable and, ironically, most ignored UAS target is the launch recovery site – the aircraft carrier of the battlefield. Why focus on killing individual airborne platforms when the high payoff is to kill multiple airframes along with operators and sustainers in a single blow? Given the fact that the launch recovery site is a vital component of the total system, kinetic attack is a near-certainty for a capable enemy.'
Lieutenant General (ret.) Michael F. Spigelmire, former commander U.S. Army Special Operations Command and VII Corps

The Support Element includes all of the prerequisite equipment to deploy, transport, maintain, launch and recover the RPA and associated communications equipment.

7.6.1 Detection Avoidance

The Support Element is typically deployed and located in or near the AOO, depending on the RPA's effective range. Like manned aircraft, RPAS typically require an appropriate logistics footprint, e.g. shelters for refuelling, arming and maintenance. MALE RPAS usually also require an adequate airport infrastructure with a runway of roughly 2,000 m. The infrastructure necessary to operate an RPAS is usually part of a military compound. Support Element personnel working on-base should be well protected from immediate threats as a result of force protection measures already in place.

7.6.2 Engagement Avoidance, Hit Avoidance and Hit Tolerance

The exposure of deployed Support Element personnel and equipment, the precautions against threats as well as the magnitude of personnel or equipment losses are identical to those that apply to the LRU and the deployed MCE. These have already been discussed in chapter 7.3.

7.6.3 Vulnerability Assessment

Support Element functions and tasks are typically conducted at the same location as the LRU. Therefore, the Support Element and the personnel assigned to

the LRU and MCE share similar threats. Therefore, the previous vulnerability assessments for deployed personnel and equipment still apply.

Inside the AOO, the adversary may engage RPAS support personnel with all available weapons, e.g. combat aircraft, artillery or infantry. This study could not identify any unique vulnerability that may apply specifically to RPAS support personnel; their vulnerability is assessed to be the same as all other military personnel located in the AOO. (cf. Table 21)

Table 21 – Support Element Vulnerability Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

CHAPTER VIII

Threat and Vulnerability Consolidation

8.1 Threat Summary

Chapter VI identified possible threats and their estimated probability of attack against an RPAS. The probability of attack ratings were derived from two key factors; 'Availability' and 'Accessibility'. 'Availability' referred to the probability that a given weapon, weapon system or military force necessary to produce a threat to the RPAS was obtainable for an adversary. 'Accessibility' referred to the probability that an adversary could get the weapon, weapon system or military force into striking distance. If analysis determined that a given threat delivered different ratings within one factor, the highest rating was used in that specific factor. For example, if a deployed RPAS element was estimated as more 'accessible' to a certain threat than if home-based, the higher rating for the deployed RPAS component was used to determine the overall 'Accessibility' factor.

To determine the probability of attack, the lower overall rating from either the 'Availability' or the 'Accessibility' was used. For example, if a weapon system was estimated to be 'highly available' to a possible future adversary but at the same time it was determined that the enemy couldn't get 'access' to the RPAS with that specific weapon system, the overall probability of attack was rated as 'low'. The 'probability of attack' rating does not consider the possibility of success or failure of an attack. It merely rates the likelihood that possible future adversaries may be in possession of a given weapon, weapon systems or military force and NATO should anticipate their use against friendly RPAS.

The following table summarizes all threats and their overall probability of attack ratings previously discussed in chapter VI. The individual ratings are displayed below using the standard 'traffic light colour system'. (cf. Table 22)

Table 22 – Identified Threats and Overall Probability of Attack Ratings.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft	Highly Critical	Highly Critical			Highly Critical	Moderately Critical	Moderately Critical	Highly Critical	Highly Critical
Payload	Highly Critical	Highly Critical			Highly Critical	Moderately Critical	Moderately Critical	Highly Critical	Highly Critical
Human Element		Highly Critical			Highly Critical		Highly Critical		Highly Critical
Control Element		Highly Critical	Low Critical	Highly Critical	Highly Critical		Low Critical	Highly Critical	Highly Critical
Data Link		Highly Critical	Low Critical	Highly Critical	Highly Critical		Moderately Critical	Highly Critical	Highly Critical
Support Element		Highly Critical			Highly Critical		Moderately Critical		Highly Critical

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

8.2 Vulnerability Summary

Chapter VII identified the vulnerabilities of the separate RPAS elements. The overall vulnerability level was determined by applying Robert E. Ball's 'Survivability Kill Chain' methodology which was previously introduced in chapter 5.2. The following table summarizes the overall vulnerability ratings which have been individually discussed in chapter VII. The individual ratings are displayed according to the standard 'traffic light colour system'. (cf. Table 23)

Table 23 – RPAS Elements' Overall Vulnerability Ratings.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft	Highly Critical	Highly Critical			Moderately Critical	Moderately Critical	Moderately Critical	Highly Critical	Moderately Critical
Payload	Highly Critical	Highly Critical			Moderately Critical	Moderately Critical	Moderately Critical	Highly Critical	Moderately Critical
Human Element		Moderately Critical			Moderately Critical		Highly Critical		Highly Critical
Control Element		Highly Critical	Highly Critical	Highly Critical	Highly Critical		Highly Critical	Highly Critical	Highly Critical
Data Link		Highly Critical	Low Critical	Highly Critical	Highly Critical		Highly Critical	Highly Critical	Highly Critical
Support Element		Moderately Critical			Moderately Critical		Low Critical		Moderately Critical

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

8.3 Consolidated Criticality Assessment Matrix

To determine the most critical effects on RPAS operations, the respective ratings of the threat and vulnerability summary are correlated. If the ratings differ from each other, the lower rating is used. For example, if a specific threat is assessed as 'high' but the vulnerability to this threat is only assessed as 'moderate', then the overall assessment will be 'moderate'. Conversely, if a threat is assessed as 'low' and the vulnerability to this threat is assessed as 'high' the overall assessment will still be rated as 'low'. The individual ratings are displayed below according to the standard 'traffic light colour system'. The resulting criticality levels are as follows:

Highly Critical. A 'high' vulnerability assessment of a given element in combination with a 'high' probability assessment that this element may be attacked results in a rating of 'highly critical'. Issues assessed as 'highly critical' affect current RPAS operations and should be addressed as a high priority.

Moderately Critical. Different vulnerability and threat ratings in which the individual assessment is not lower than medium are considered 'moderately critical'. Issues assessed as moderately critical are not yet 'highly critical', but, as technology is continuously evolving, may become so in the future. It is recommended that 'moderately critical' issues are addressed on a mid-term perspective and with a lower priority than 'highly critical' issues.

Low Critical. A low vulnerability of an RPAS element or a low probability that this element may be attacked is rated 'less critical'. It is assessed that RPAS can sustain attacks from threats listed in this category or is not expected to face them. However, to enhance RPAS resilience, it is recommended that 'less critical' issues should be addressed with a lower priority than 'moderately critical' issues. (cf. Table 24)

Table – 24 Consolidated Criticality Assessment Matrix.

RPAS Elements / Threats	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Forces	Cyber Warfare	Adversary RPAS
Remotely Piloted Aircraft									
Payload									
Human Element									
Control Element									
Data Link									
Support Element									

Low Critical
Moderately Critical
Highly Critical

Indicated levels are not in accordance with the official NATO threat levels defined in the ACO Security Directive AD 70-1

CHAPTER IX

Recommendations

This study identified more than one hundred individual recommendations throughout the entire scope of RPAS. The recommendations listed in this chapter are structured in the same way as the vulnerability analysis in chapter VII, i.e. by RPAS element. Within the respective RPAS element, the recommendations are listed in accordance with the 'Survivability Kill Chain' methodology which was previously used in this document to identify the RPAS elements' vulnerabilities. As a result of this methodology, there is some degree of repetition among the recommendations. To aid the reader, tables were added as annexes to provide a quick reference to the individual recommendations.

9.1 Enhancing Remotely Piloted Aircraft Survivability

9.1.1 Threat Suppression Measures

9.1.1.1 Ensure Crew Rotations are Properly Scheduled. Aircrew fatigue, the physical or mental tiredness or disorder resulting from the strains and stress of missions, may be a safety factor on its own.[1] Impaired attention and judgment, reduced physical endurance and reaction time, as well as a reduced ability to assess risk and consequences of action, may result in mission failure, mishap, or fratricide. Appropriately scheduled crew rotations should be maintained to avoid consequences from aircrew fatigue which negatively impact RPAS survivability.

9.1.1.2 Sustain Properly Trained Crews at All Times. Not all NATO nations are financially able to continuously train their RPAS personnel on a regular basis. Some nations must conduct their RPAS flight training just prior to operational mission deployment. This means crews must relearn basic skills versus honing combat expertise required for operations in contested environments. In order for crews to maintain required proficiency levels, continuous flight training should be conducted year-round. Additionally, an annual proficiency and readiness test should be administered to ensure that RPAS personnel meet the requirements for operating RPAS in contested environments.

9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats. The best way

to mitigate a threat is to avoid it altogether. This method is effective in air mission planning techniques and can also be applied to RPAS operations in contested environments. Reliable intelligence regarding the adversary's force structure, its air combat and AD capabilities as well as its order of battle are essential to successful mission planning. Wherever operationally possible, RPAS should be planned to operate outside of adversary weapon systems detection and engagement envelopes.

9.1.1.4 Employ Sensor Capabilities to Detect Surface-/Air-Based Threats. Many RPAS are capable of employing a variety of payload modules. Due to SWaP limitations, mission planners must design the correct payload module loadout for the expected threats. This may enable the RPAS to observe relevant threats and conduct proper evasive manoeuvres, if required.

9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats. Equipping RPAS with lethal air-to-air or air-to-ground weapons will force the adversary to weigh the risk of losing equipment and personnel versus the benefit of destroying the RPA. RPAS could also take the role of Suppression of Enemy Air Defence (SEAD) assets if armed with High-Speed-Anti-Radiation-Missiles (HARM). Due to their extended loiter time, they may be better suited to perform this mission than manned aircraft.

9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning. The range from which an object in the sky can be spotted is dependent on its size, contrast, engine noise level and the atmospheric conditions. RPAS can improve the likelihood of avoiding MANPADS engagements by remaining outside the spotting range of airspace observers. Mission planners must be aware of the RPAS' visual and audible thresholds to determine the appropriate target range, slant range and route. These factors are especially critical for missions with long, on-station loiter times.

9.1.1.7 Control Image / Video Resolution Requirements to a Reasonable Level to Improve RPAS Stand-Off Range. The altitude, target range and slant range are dependent on the sensor's angular resolution and the desired image quality. Image quality is usually expressed in National Interoperability Rating Scale (NIIRS) or Ground Resolved Distance (GRD). A lower minimum NIIRS/GRD directly contributes to a greater stand-off range, so mission planners should always aim for the lowest NIIRS/GRD necessary to fulfil the Commander's Critical Information Requirements (CCIR).

9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats. If a required capability is unique to an RPAS and the RPAS itself cannot defend itself adequately, it can be supported by manned combat aircraft providing SEAD, escort or fighter sweeps. Mission planners should weigh the required RPAS capabilities versus the additional risk to aircrew. Combined flight training should be conducted to improve the interoperability between RPAS and manned aircraft.

9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA. Modern RPA are complex systems consisting of highly advanced and classified technology. If the loss of an RPA cannot be avoided, an automated self-destruct mechanism should guarantee that classified technology or onboard data will not be compromised. A reliable denial of adversary exploitation of friendly technology will directly support suppression of future threats.

9.1.1.10 Consider Stratospheric Employment of RPAS to Suppress Surface-/Air-Based Threats. Currently the stratosphere is out of range for most surface-based threats. RPAS flying at stratospheric altitudes could operate as very long endurance stationary weapons and ISR platforms to conduct offensive operations and wide area surveillance. Equipped with sophisticated guided and homing air-to-surface and air-to-air missiles, stratospheric RPAS could project air power similar to today's naval aircraft carriers.

9.1.2 Enhancing Detection Avoidance

9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection. Radars can typically only detect targets that are in direct line of sight. An RPAS capable of highly automated, very low alti-

tude, terrain following flight could penetrate ground-based radars and climb to higher altitudes only to conduct its actual mission. The required technology has been implemented in manned combat aircraft or cruise missile systems for decades and should be adapted for RPAS as well.

9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection. In contrast to very low altitude (terrain following) flights which require a high degree of automation and incorporation of sophisticated (expensive) avionics, RPA low level flights could be conducted under remote control with currently available systems. Data link latency and reduced situational awareness are limiting factors for conducting low level flights with RPAS. The possible degree of remotely controlled low level flights with current RPAS should be tested and RPAS pilot training should be adjusted accordingly.

9.1.2.3 Reduce the Remotely Piloted Aircraft's Radar Signature to Impede Enemy Detection. Even small RPA can have a large RCS leaving them vulnerable to radar detection. The incident energy returned to the enemy radar from the RPA should be minimised to impede enemy detection. The absence of a cockpit permits even better stealth shaping of the airframe than manned aircraft. New RPAS designs should always incorporate stealth capabilities. Radar absorbing coatings should be considered an option to reduce signatures of current RPAS. However, the benefit of a reduced radar signature should be balanced against additional costs, aerodynamic weight and reduced payload.

9.1.2.4 Reduce the Remotely Piloted Aircraft's Noise Signature to Lower the Range of Audibility. To conduct ISR missions with long loiter times, the RPA must be inaudible to ground observers. A quieter RPA can operate at lower altitudes which can permit better image quality. Current RPAS' noise signatures and aural thresholds should be analysed and, if found to be audible by ground observers when flying at its operational altitude, the noise signature should be reduced. New RPAS designs should consider noise signature reduction measures as well.

9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature to Lower the Spotting Range. Low visibility is desirable for all military aircraft. It is usually achieved by colouring the aircraft so it blends in with its environment. Current RPA typically use a standard blue-greyish colour scheme to lower their visibility against the sky. To further reduce the visual signature, modern digital or fractal camouflage schemes that break the symmetry axis should be applied to the RPA. Multi aircraft RPAS should also consider using different day and night camouflage schemes to adapt even better to their operational environment.

9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature to Impede Enemy Detection. Hot aircraft materials, such as engine exhaust or wing surfaces heated by friction with the air, emit IR / UV radiation that heat-seeking weapons can track. Reducing the thermal signature requires that aircraft parts and emissions, particularly those associated with the engine, are kept as cool as possible. In order to accomplish this, the RPA's design should use techniques currently used by manned aircraft to reduce IR signatures. These include embedding the (jet) engines into the fuselage or wings, incorporating extra shielding of hot parts; mixing cool air with hot exhaust; directing hot exhaust upward, away from ground observers; and the application of special coatings to hot spots to absorb and diffuse heat over larger areas.

9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection in the Electromagnetic Spectrum. RPAS require a reliable data link. This means a continuous emission of radio transmissions being emanated to and from the RPA. Reducing radio transmissions to an absolute minimum assists in promoting electromagnetic stealth. Future RPAS developments should consider fundamental changes in the methods currently used to communicate with the RPA. These new methods should seek to minimize radio transmissions through the use of waypoint navigation, choosing from predefined flight manoeuvres or using automated on-board sense and avoid capabilities.

9.1.3 Enhancing Engagement Avoidance

9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue. Studies have shown that humans have difficulty maintaining focus during extended periods of relatively low task demand or over long periods of inactivity. Even if the crewman is highly motivated, it is impossible to maintain effective visual attention on an unchanging object for more than thirty minutes.[2] The best way to maintain focus and physical stimulation is to implement an intermediate level of automation which requires continuous human involvement. However, a suitable balance between manual and automated control must be achieved as too little automation will negatively affect aircrew focus and therefore, RPAS survivability. An example of this is an emergency situation where the operator is unable to react quickly enough to an imminent threat. In this case, the system could take full control until the situation is resolved or the system is overridden manually.

9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness. RWR enable RPAS operators to detect radars and manoeuvre the RPA away from the threat before weapons can be employed. RWR systems can also collect information on the adversary's electronic order of battle and can contribute to the overall intelligence picture. Industry already offers relatively small and lightweight RWRs, although they will require a significant percentage of the RPAS' available power. RWR should be installed on all RPAS expected to encounter enemy radar systems. To improve mission flexibility, RWRs should be modular and interchangeable with other payloads if the RWR requirement is not anticipated.

9.1.3.3 Install Identification, Friend or Foe Transponders. Identification, Friend or Foe (IFF) transponders permit the identification of friendly, enemy and neutral forces by broadcasting a specific encrypted signal that allows categorization of objects on the battlefield or in the airspace. IFF may also support airspace coordination measures allowing RPA to operate together with other airspace users. However, not all current RPA are equipped with IFF transponders, although newer and smaller transponders especially designed for RPA applications are already in use.[3] In areas where adversary aircraft operations are expected, IFF transponders should be installed into RPAS to help integrate them into air operations.

9.1.3.4 Consider Employment of Decoy RPA to Distract from High Value or Mission Critical RPA. If a specific high value RPA cannot be hidden from enemy detection, it may be concealed within a swarm of decoy RPA. Decoy RPA should be re-usable, but expendable, and provide the same or larger radar signature as the protected RPA. They could also actively radiate false radio, IR or other signals to appear like a high value aircraft. A swarm of decoy RPA should be capable of being remotely piloted by a single operator. It also requires a high degree of automation for the decoy RPA swarm to automatically follow pre-defined flight formations and reduce pilot workloads.

9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness for RPAS Operators. RPAS on-board sensor suites are usually non-comprehensive due to SWaP constraints. As RPAS operations typically take place in a network centric environment, fusion of information from a diverse array of external sensors should compensate for this deficiency and should provide relevant, real-time situational awareness. Command, Control, Communications, and Intelligence (C3I) systems must provide relevant, consumable information to RPAS operators without latency.

9.1.3.6 Increase Operating Altitude to Avoid Engagement by SAF, AAA and Low Tier SAMs. If the RPA flies higher, there will likely be fewer threats that can reach it. As RPA operate at higher altitudes, more sophisticated and more expensive AD systems are required to successfully engage them. Due to the limited availability of expensive, high end SAMs, an adversary may reconsider using them against relatively inexpensive RPAS versus using them against higher value targets. Hence, the operating altitude of RPA should be above 10,000 to 15,000 ft to escape Small Arms Fire (SAF), AAA and low end SAMs in the so called 'trash fire' envelope. (cf. Figure 5)

9.1.3.7 Consider RPAS Operations in the Stratosphere to Avoid Engagement by Most Weapons. Currently, the stratosphere is out of range for most surface-based threats. RPAS operating at altitudes above 100,000 ft could completely avoid or react more effectively to enemy engagements. Using stratospheric RPAS also offers additional benefits (cf. 9.1.1.10 and 9.5.5.2).

9.1.3.8 Increase RPA Operational Cruise and Top Speed to Enhance its Stand-Off Capabilities. Current weaponized RPA operate at an average speed of approximately 200 kts. The maximum range of a weapon released by an RPA is roughly only half of one released from a fighter aircraft flying at significantly higher speeds. (cf. 7.2.1.3) Future armed combat RPAS should be capable of operating at high, subsonic speeds to increase their stand-off weapons ranges comparable to that of manned combat aircraft.

9.1.4 Enhancing Hit Avoidance

9.1.4.1 Increase RPA Manoeuvrability. Once a weapon engages an RPA, its survivability depends largely on its ability to outmanoeuvre the threat. Because an RPA is not constrained by human limitations to acceleration and G-loading, the propulsion and airframe design possibilities offer better manoeuvrability. Future RPAS should employ blended wing bodies, laminar and active flow controls to enable very responsive and manoeuvrable aircraft that can operate in ways impossible for manned aircraft.

9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators. RPAS operators may or may not have a combat aircraft pilot background, and not all nations currently require certified pilots to operate RPA. Most RPAS operators are not experienced in air-to-air combat. RPAS operators should receive training in basic aerial combat manoeuvring. This will help to improve situational awareness and an understanding of manoeuvrability limitations of current RPAS in order to increase the likelihood of evading enemy threats.

9.1.4.3 Incorporate Automated Laser Warning Systems. Like helicopters, slow and low flying RPAS are exposed to surface-based laser range finders, laser designators and laser beam riding weapons. In contrast to the helicopter pilot, the RPAS operator can only react to a threat with the delay of the C2 link's latency. To circumvent this problem, on board laser warning systems can aid the RPAS operator by automatically performing direct and immediate initiation of countermeasures (cf. 9.1.4.5). Laser warning systems should be considered for RPAS where operational speeds and altitudes are similar to those of manned helicopters.

9.1.4.4 Incorporate Missile Warning Systems. Missile Warning Systems (MWS) are effective in detecting and informing the operator of incoming missiles regardless of whether they are radar, IR, laser- or visually-guided. They can also provide information on the time to impact as well as the direction of the approaching missile. MWS only work after a weapon has been launched, which requires very quick reacting countermeasures. Since RPAS operators can only react to a threat with the delay of the C2 link's latency, MWS should be incorporated in combination with highly automated countermeasure systems (cf. 9.2.4.2).

9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection and Tracking. To avoid being hit by heat-seeking weapons, measures to reduce aircraft thermal radiation (c.f. 9.1.2.6) can be supplemented by active countermeasures. These methods are directed against enemy IR/UV detection and tracking sensors. They also encompass IR/UV jamming (i.e. active infrared missile countermeasures mounted near engine exhausts to confuse heat-seeking missiles) and the use of decoy flares. Combat helicopters, which operate at similar flight regimes, are particularly vulnerable to heat-seeking weapons and have been equipped with infrared jamming devices for several decades.

9.1.5 Enhancing Hit Tolerance

9.1.5.1 Consider Partial Component Redundancy. The installation of redundant components enhances

the survivability of an aircraft by reducing the impact of aircraft system damage and increasing the aircraft hit tolerance. Due to SWaP restrictions, it is very unlikely for RPA to be designed with total redundancy. However, future RPAS should consider incorporating at least partial redundancy to prevent the loss of the RPA as a result of fatal damage to only one device, part or mechanism. The miniaturization of system components may facilitate further redundancy.

9.1.5.2 Minimize the Exposure of Critical System Components. Minimizing the exposure of critical components must be considered early in the design phase of future RPAS. This technique serves primarily to reduce the likelihood of key components being critically damaged by enemy weapons. In order to improve the RPA's damage tolerance, non-redundant critical components should be oriented facing away from the most probable direction a kinetic weapon is likely to affect. Non-critical or ruggedized components should be oriented to shield the more vulnerable areas. Further miniaturization reduces the component's exposed surface area to the threat.

9.1.5.3 Incorporate Passive Damage Suppression Measures. Passive damage suppression refers to features that either contain the level of damage or reduce the effects of the damage. To improve ballistic tolerance, RPAS should incorporate passive damage suppression measures such as shielding of critical components with armour, use of self-sealing coatings for fuel tanks and application of fire resistant materials. In order to save weight, shielding should only be installed in the most likely direction of enemy weapons fire. The trade-off between additional costs, aerodynamic weight and reduced payload must be considered.

9.1.5.4 Incorporate Active Damage Suppression Components. Active damage suppression includes employment of sensors or other devices to sense the onset of a damage process. It activates mechanisms that contain the damage or reduces its effects, e.g. fire detection and extinguishing systems. In order to contain the damage once the RPA has been hit, incorporation of active damage suppression components should be considered. The trade-off between additional costs, aerodynamic weight and reduced payload must also be considered.

9.1.5.5 Incorporate Reconfigurable Flight Control Systems. RPA rely solely on their flight control system software to provide steering commands for flight controls such as flaps, ailerons, canards, elevators or tails. Reconfigurable flight control systems refer to software algorithms designed specifically to compensate for failures or damage to flight controls or lifting surfaces by using the remaining flight controls to generate compensating forces and moments. These methods are well established in modern combat aircraft. To restore the RPA's stability and performance after flight control damage, reconfigurable flight control systems should be incorporated into new RPAS.

9.1.5.6 Develop Universal/Modular RPAS Assemblies to Quickly Repair Damaged Components. The ability to rapidly repair combat damaged RPAS components after returning from missions ensures a high operational readiness rate. This can be facilitated by the development of modular components that can be swapped as a unit versus repairing individual components on the RPAS. This can also be aided by using standard universal modules that can be interchangeable between different RPA models.

9.2 Enhancing Payload to Improve System Survivability

9.2.1 Threat Suppression Measures

9.2.1.1 Equip RPA With High-Speed Anti-Radiation Missiles. Installation of HARM on RPA could enable them to deter enemy AD or EW systems from turning on their active emitters. Current RPAS capable of carrying 500 lb LGBs could also be armed with HARM. As a prerequisite, the RPA must be equipped with an appropriate warning system to provide the operator with target acquisition data once a radiation source is detected. Assuring the enemy is aware of this capability may also contribute to RPAS survivability.

9.2.1.2 Incorporate Gunfire Detection Systems and Self-Protection Missiles. The gunfire detection

systems currently available are capable of pinpointing enemy firing locations by either radar, acoustic or optical detection. Incorporating this type of system could enable RPA to immediately and automatically laser designate an enemy firing position. In combination with automatically launched self-defence missiles, the RPA could instantly react to all gunfire directed against it. The self-defence missiles should be small and lightweight enough to be carried in adequate amounts, be capable of being launched off-boresight and have pinpoint accuracy to be effective. Assuring the enemy is aware of this capability may also contribute to RPAS survivability.

9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS. In the future, advanced combat RPAS could be used to gain control of contested airspace. This requires very high performance systems, operating at high speeds, which are agile and automated. These capabilities would be required to successfully conduct air-to-air engagements at both close and long ranges. Future combat RPAS should integrate advanced air-to-air weapons to enable them to operate in the full spectrum of air-to-air combat.

9.2.1.4 Reduce the Size of Active Jamming Systems to Introduce ECM Capabilities to RPAS. Enemy tracking systems could be suppressed by the use of active jammers. Due to their sheer size and weight, currently available ECM systems can only be incorporated into the largest RPAS, e.g. Global Hawk. To cope with the SWaP restrictions inherent to an RPAS, technological advancements must reduce the size of jamming units and increase their power levels to facilitate future EW capabilities for RPAS.

9.2.2 Enhancing Detection Avoidance

9.2.2.1 Integrate Payloads Internally Into the Airframe. The multiple edges and corners of external payloads attached to the RPA's wing hard points are major sources of reflected radar energy. Stealth aircraft typically carry their payload in internal bays to minimize their radar reflectivity. To reduce the RPA's radar signature, internal payload integration should also be a design consideration for future RPAS (cf. 9.1.2.3).

9.2.2.2 Consider Use of Micro-Munitions to Support Internal Payload Integration. Smaller and lighter than conventional missiles or bombs, micro-munitions could be carried internally, supporting the stealth design of future RPA. They could also facilitate reducing the overall size of future RPA airframes. The development of small and agile micro-munitions may be a key enabling technology in the future. Micro-munitions could also support strikes with higher precision and lower collateral damage than today's RPAS armament. The development and integration of micro-munitions for use on RPA should be encouraged.

9.2.2.3 Incorporate Retractable Sensors. The required flexibility and field of view of visual sensors may prohibit a complete internal integration into the RPA. As a compromise between stealth and sensor requirements, the sensor payload could be employed only when needed and stored inside the airframe when not in use, e.g. during transit. Retractable sensor payloads could also be an option for current RPAS. Retractable sensors should be considered for future and current RPAS to reduce the RPA's radar signature.

9.2.3 Enhancing Engagement Avoidance

9.2.3.1 Incorporate 360 Degree Field of View Optical Systems. RPAS operators sense the RPA's environment via the FMV streams from on-board sensors. The limited field of view is often referred to as the 'soda-straw' view. RPAS should be upgraded with currently available optical sensors that can provide a full 360 degree view to significantly increase situational awareness.[4] A 360 degree FMV stream should be displayed either on a circular set of multiple screens inside the GCS or on a head-up display (HUD) incorporated in glasses or a helmet. Future technologies should seek to achieve a 'virtual presence' for the RPA operator inside the RPA.

9.2.3.2 Improve Sensor Sensitivity and Angular Resolution. Sensor performance has a direct effect

on the RPA's stand-off range. There have been many cases where an RPA was required to fly low to obtain better EO/IR imagery resolution.[5] Given the same target resolution requirement, increasing the sensitivity and angular resolution of the sensor will result in a greater slant range. As sensor technologies are likely to improve rapidly, integration of better sensors should be a continuous process. This should include consideration of the most recent COTS products available to enhance the RPA's stand-off capabilities.

9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPA. Depending on their sensor capabilities, HALE/MALE RPA may be forced to operate inside the engagement envelope of enemy weapon systems to provide the required image quality. Due to their size, they may be unable to avoid detection or engagement. Very small Scout-RPA carried by and launched from the HALE/MALE RPA could act as forward deployed sensor platforms. Because of their small size, they could stay undetected while the MALE/HALE RPA could remain out of range of the threat. Scout-RPA should be expendable and could also carry a warhead for engaging targets of opportunity or eventually self-destructing after use. Scout-RPAS could also be an option to enhance manned combat aircraft capabilities.

9.2.3.4 Consider Armament with Non-Lethal Weapons to Minimize Collateral Damage and Gain Operational Flexibility. Conventional warheads often produce blast and fragmentation that may cause collateral damage beyond the intended target. Modern weapons capable of detecting, tracking and engaging aircraft are heavily reliant on microelectronics. These are not only vulnerable to kinetic effects, but also to directed energy. Electromagnetic weapons could induce currents large enough to melt the circuitry of enemy weapon systems or communications infrastructure. The main advantage of electromagnetic warheads is the duration of the pulse can be so short they could spare human lives and leave buildings undamaged. This would lower the threshold for use of friendly weapons to pre-emptively engage enemy threats and enhance operational flexibility.

9.2.3.5 Consider Implementation of Extended Range Air-to-Ground Weaponry. Current RPAS typically operate at lower speeds than manned combat aircraft. Therefore, the release speed of carried weapons is also lower. (cf. 9.1.3.8) This results in a smaller weapon engagement range and a weak stand-off capability. However, extended range munitions already available for manned combat aircraft offer remarkable increases in weapon ranges even at lower airspeeds. Extended range munitions should be adapted for RPAS use to maximize their stand-off capabilities.

9.2.4 Enhancing Hit Avoidance

9.2.4.1 Incorporate Adaptive Spectral Filters to Protect EO/IR Sensors from Being Hit by Laser Energy. EO/IR sensors can be blinded by shining a laser beam into their optical components. Depending on the emitted laser energy, this effect can be temporary or cause permanent damage. EO/IR sensors should be protected with adaptive spectral filters to shield the sensitive optical components against harmful laser energy.

9.2.4.2 Incorporate Highly Automated Countermeasure Packages. Warning systems are only effective if combined with appropriate countermeasures such as flares or chaff. Current homing interceptors are typically guided by radar, IR or laser. Depending on the anticipated threat, appropriate countermeasures must be selected in mission planning. A broad spectrum of countermeasure packages for manned combat and transport aircraft is already available and should be adopted for RPAS. As RPAS operators can only react to a threat with the delay of the C2 link's latency, the implementation of countermeasures should follow a highly automated approach to gain valuable seconds when an incoming threat has been identified. To enable the RPA to adapt to different threat scenarios, countermeasure packages should be modular.

9.2.5 Enhancing Hit Tolerance

9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures. Miniaturization could ease SWaP limitations and enable the installation of

redundant payloads into the RPA. Redundant components could support each other by combining their capabilities into greater functionality. An example could be building grids from multiple small sensors which together form a single perspective, comparable to a fly's compound eye.

9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage. To protect the RPA from catastrophic damage in the event a payload package has been hit and has ignited, incorporation of a payload emergency release mechanism should be considered. This situation could be especially dangerous to the rest of the airframe if explosives are involved. Sensor packages are usually designed as removable units so different sensor modules can be configured. Weapons attached to the RPA's hard points or stored in internal bays are inherently prepared with a release mechanism. However, to avoid collateral damage, the emergency release mechanism should be initiated only by the operator and not in an automated mode.

9.3 Enhancing Survivability of the Human Element

9.3.1 Threat Suppression Measures

9.3.1.1 Protect Identities of RPAS Personnel. This study found countless articles, interviews, images and videos clearly revealing names, units and home bases of RPAS personnel. Many of these can be attributed to public media releases from the armed forces themselves. To protect RPAS personnel, public relations should be controlled to ensure no information is revealed that could lead to identification of individual personnel.

9.3.1.2 Raise RPAS Personnel's Awareness for Dealing with Social Media and the Internet. Social media and the internet are open sources for enemy intelligence gathering. RPAS personnel must be aware that any information they willingly share with the internet community may also arouse unwanted attention. Eventually this could enable an adversary to identify and track individual RPAS personnel in their domestic environment for further engagement, e.g. espionage, blackmail or lethal actions. RPAS personnel should receive training on how to deal with social media and the internet in order to not contradict other force protection measures.

9.3.1.3 Raise the Media's Awareness of Asymmetric Threats against Home-Based Combatants. Home-based RPAS personnel that actively take part in remote combat operations are considered combatants and legitimate targets for enemy operations. In a globally connected world, publishing even unclassified information may support enemy intelligence gathering. This could endanger personnel and their families. The armed forces should actively approach the media and raise their awareness of enemy intelligence gathering and asymmetric threats. The objective should be to enable reporters to responsibly balance freedom of the press against putting RPAS personnel at risk.

9.3.1.4 Consider RPAS Personnel's Family Environment when Applying Force Protection Conditions Measures. From an enemy perspective, home-based RPAS personnel may be more accessible and more vulnerable outside their assigned military base. This may put the families of RPAS personnel at risk, either intentionally or accidentally through collateral damage. Force Protection Conditions (FPCON) usually encompass the military domain only and do not reflect exceptional circumstances of remote operations. To avert asymmetric threats, FPCON should address protecting the families of RPAS personnel.

9.3.1.5 Establish Close Cooperation with Civilian Authorities. As asymmetric threats may include RPAS personnel's domestic environment, force protection measures should be adjusted accordingly (cf. 9.3.1.4). This requires close cooperation with civilian authorities to accommodate military and civilian activities.

9.3.2 Enhancing Detection Avoidance

9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations. Satellite imagery of the earth's surface can be obtained from

commercial companies like Astrium, DigitalGlobe or BlueSky.[6] This imagery can be obtained directly or over the internet by using services from Google or Microsoft. This study found publicly accessible satellite imagery of various military installations hosting RPAS and the adjacent housing areas which are likely to accommodate military personnel. This imagery may be especially valuable to asymmetric forces that do not have access to satellite capabilities. To impede enemy exploitation of commercially available satellite imagery, regulations should be established prohibiting the distribution of imagery showing friendly military installations and adjacent housing areas. As different companies fall under the jurisdiction of different nations, international consensus and eventually agreement is required.

9.3.2.2 Prohibit Wearing Name Tags, Badges or Uniforms Outside Military Compounds. Once a military installation or housing area is revealed (cf. 9.3.2.1), individual RPAS personnel and their families could be identified via on site clandestine operations. To avoid visual identification of RPAS personnel, name tags and unit badges should be removed outside military compounds. Dressing in civil clothes before leaving the barracks should also be considered. This measure may require detailed legal assessment to mitigate infringement on IHL in terms of discrimination between combatants and civilians.

9.3.3 Enhancing Engagement Avoidance

No recommendations found.

9.3.4 Enhancing Hit Avoidance

9.3.4.1 Protect the Work Areas of RPAS Personnel. Depending on their function, the areas where RPAS personnel usually work are GCSs, aircraft hangars or staff buildings. At a minimum, all of these facilities should be protected against direct fire or fragmentation. Considerations regarding protection of facilities should not be limited to the AOO only. It should also be considered for home-based infrastructure which may be exposed to asymmetric attacks.

9.3.5 Enhancing Hit Tolerance

9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve. To strengthen the human element of RPAS operations as a whole, sufficient reserve personnel should be trained and sustained. As the physical requirements for RPAS pilots / operators are lower than for operating manned aircraft, these personnel may be recruited from physically disabled or retired personnel.

9.4 Enhancing Control Element Survivability

9.4.1 Threat Suppression Measures

9.4.1.1 Consider Pre-Emptive Cyber-Attack Operations to Suppress Enemy Cyber-Capabilities. The best way to mitigate a threat is to avoid it; this is also true for the cyber-domain. Suppressing cyber-threats may require pre-emptive infiltration of enemy systems with insertion of malicious code. If necessary, the adversary's cyber-weapon may then be terminated before it can impose a cyber-threat to friendly systems. Hence, pre-emptive cyber-attacks should be considered as an option to suppress enemy cyber-capabilities. This may require further legal assessment and consensus within NATO to ensure compliance with IHL.

9.4.1.2 Apply NATO Class II Security Area Restrictions to the RPAS Control Element Infrastructure. To prevent asymmetric forces from accessing the Control Element, the GCS and its immediate vicinity should be protected independent from the given threat conditions of the surrounding military infrastructure. This added protection should comply with NATO Class II Security Area[7] restrictions at a minimum level and should apply to home-based and deployed GCS as well.

9.4.2 Enhancing Detection Avoidance

9.4.2.1 Locate Satellite Ground Terminals Away from the GCS to Prevent Visual and Electronic Identification. Satellite antennas required to estab-

lish communications within an RPAS can be quite large, making them easy for enemy reconnaissance to see. Currently, most RPAS rely on constant radio transmissions to control the aircraft, making the antennas vulnerable to enemy radio-location techniques as well. Locating satellite earth terminals adjacent to the GCS would also endanger the GCS. Satellite antennas should be positioned at a reasonable distance from the GCS so that detection of the antenna does not allow an adversary to draw conclusions regarding the actual GCS location.

9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS by Electronic Reconnaissance. As most RPAS require constant communication with the GCS, an adversary could detect these radio signals and employ direction-finding techniques to locate the source of transmission (cf. 9.4.2.1). Minimizing radio communications would lower the risk of being detected electronically. However, this requires a high degree of automation, enabling the RPA to conduct its mission with only minimal human intervention and eventually a minimum of radio transmissions (cf. 9.5.2.5).

9.4.2.3 Choose an Inconspicuous Location for the GCS. An RPAS encompasses several components. This enables an adversary to visually detect, identify and draw conclusions where other elements may be located. Locating the GCS in the vicinity of other RPAS elements, e.g. parked RPA, aircraft hangars or communications equipment, may be convenient, but could also endanger the GCS. Whenever possible, the GCS should be placed in an inconspicuous location where it blends in with other generic military equipment or infrastructure.

9.4.2.4 Remove Signs Indicating the Operational GCS Location to Avert On-Site Espionage. Enemy intelligence gathering does not stop at the front gates of military compounds. The common practice of employing locals for non-military duties offers the opportunity for enemy on-site espionage. This tactic does not apply only to deployed operations, any signs indicating the location of operational GCS should be removed to protect against enemy on-site espionage activities.

9.4.3 Enhancing Engagement Avoidance

9.4.3.1 Enable Deployable RPAS Control Elements to Leapfrog[8] and Handover Command. Modern electro-optical or electronic reconnaissance is likely to locate active command posts after a certain amount of time. To avoid being identified by enemy reconnaissance, a regular change of GCS locations should be considered. This requires having at least two movable GCS control elements per RPAS conducting regular leapfrogs and handover of command.

9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe. In recent asymmetric conflicts, home-based mission control elements of RPAS provided a high level of security simply by the amount of distance from the AOO, but a more capable opponent may be able to conduct attacks deep inside NATO territory, e.g. by long-range ballistic missiles, stealth aircraft or even RPAS. Therefore, RPAS mission control elements should be capable of redeploying in a reasonable timeframe to evade enemy engagement. A contingency plan for evacuating the stationary military infrastructure and procedures to continue operations with a mobile control element nucleus should be considered a minimum requirement.

9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It to Be Quickly Relocated to Hamper Adversary Electronic Reconnaissance. Modern electro-optical or electronic reconnaissance is likely to locate any active command post after a certain amount of time (cf. 9.4.3.1). If it is not feasible to regularly move the GCS itself, relocating detached communication antennas around a concealed GCS could be a viable option. Although relocating detached radio antennas could confuse adversary electronic reconnaissance, it may only delay locating and identification of the actual GCS.

9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary. Satellite dishes with a diameter of several metres are difficult to hide, likely to be recognized by enemy reconnaissance and highly vulnerable to blast and fragmentation. This makes

them an easy and valuable target for an adversary, especially in stationary installations. To confuse enemy intelligence and mislead possible attacks, setting up decoys should be considered.

9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS Communications. The main reason for deploying a GCS to the AOO is the requirement for an instantaneous data link during launch and recovery. This is currently only possible by using LOS communications. Further improving the latency and reliability issues associated with satellite communications could enable RPAS operators to remotely take off and land the RPA directly from inside their home country. This would make deployment of GCS equipment unnecessary.

9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability to Permit Home Station GCS Operations. Most RPAS are dependent on a permanent data link, especially during launch and recovery as there is no time to compensate for link losses. Consequently, a deployed GCS capable of establishing an instantaneous LOS data link during these critical phases is still required. Introducing a fully automated launch and recovery capability would permit using BLOS communications during these phases and eventually eliminate the necessity for a deployed GCS.

9.4.4 Enhancing Hit Avoidance

9.4.4.1 Improve Computer Security Techniques and Policies to Defend Against Cyber-Threats. Friendly RPAS have already inadvertently been infected with malicious software through the careless use of USB memory sticks.[9] In order to minimize the risk of RPAS computer systems being compromised by viruses, Trojan Horses and other malicious code, security techniques and polices must be improved. Security software suites must use the most current updates to cope with rapidly evolving cyber-threats. Computer system access policies, not only on the software site but also on the hardware site, should be as restrictive as necessary to fend off intrusion attempts or exploitation of carelessness.

9.4.4.2 Use Proprietary Software and Hardware for the Core Functions of RPAS to Minimize the Risk from Malicious Software. Viruses, Trojan Horses and other malicious code are typically only executable in the environment they are specifically designed for. Introducing a common RPAS operating system or using commercial software and hardware solutions offers financial benefits, but could compromise system security. Core system functionality like C2, navigation and control of kinetic weapons should use proprietary hardware and software solutions to minimize the risk of being infected by malicious software.

9.4.4.3 Raise RPAS Personnel's Cyber-Awareness to Prevent Infiltration of RPAS Computer Systems. Security software suites and computer system access policies can only provide the foundation for RPAS computer system protection (cf. 9.4.4.1). Personnel with regular access to RPAS computer systems may be exploited by an adversary to circumvent protective measures, either unwittingly or unwillingly. To minimize the risk of corruption, adversary recruitment or blackmail attempts, regular training that raises the awareness of those issues should be compulsory for RPAS personnel. Keeping identities of RPAS personnel classified could also help to avert those types of activities (cf. 9.3.2.2).

9.4.4.4 Shelter Stationary GCS Equipment from Kinetic Effects. Deployed control elements may be susceptible to enemy surface-to-surface or air-to-surface weapons. If the mission requires the control element to be stationary and detection avoidance measures (cf. 9.4.2) are expected to be only temporarily effective, the GCS should be reinforced against kinetic effects from direct fire or fragmentation.

9.4.5 Enhancing Hit Tolerance

9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss. The deployment of redundant GCSs at different locations contributes to RPAS survivability. If the active control element were to come under enemy fire, a redundant GCS could immediately take control of the RPA and continue the mission. However, LOS or BLOS

communication coverage of both control elements must be confirmed as a prerequisite for this option.

9.4.5.2 Isolate C2 Systems from Kinetic Weapons Payloads to Minimize the Impact of Cyber-Attacks. If an RPAS is the target of a successful cyber-attack, the adversary may successfully take over the entire system including C2, navigation, sensors and possibly kinetic weapons. Surreptitiously inserted malicious software may overcome firewalls between the subsystems of the RPAS if those systems share the same physical memory or processing units. Critical RPAS subsystems such as C2, sensors and kinetic weapons should always be separated on the Open Systems Interconnection (OSI) model's lowest possible layer[10] to minimize the effects of successful cyber-attacks.

9.5 Enhancing Data Link Survivability

9.5.1 Threat Suppression Measures

9.5.1.1 Incorporate Laser Communication Technology to Eliminate RPAS Radio Transmissions. Laser communication can provide tremendous bandwidth at data rates that are expected to be a thousand times greater than with current RF methods. Since laser communication does not operate in the RF spectrum, it is inherently a secure means of communication. To interfere with laser transmissions, an adversary must first detect the narrow laser beam. This is an especially difficult challenge since the laser is very difficult to detect for observers outside the beam. To successfully disrupt or intercept laser communications, an adversary must place an object in the laser beams path. Laser communication technology is likely to be a future 'game changer' and should be incorporated to all future RPAS.

9.5.1.2 Use On-Board Data Storage and Subsequent Analysis if Real Time Imagery is not Imperative. Legacy RPAS were not capable of providing real time imagery and had to rely on pre-programmed flight routes. Their collected data was stored on-board and analysed after recovery. Current and future RPAS should implement this traditional way of collecting information if real time imagery is not required. It can also be useful during mission phases where communication is denied by the enemy, e.g. jamming (cf. 9.5.5.4). A possible compromise could be streaming low resolution video in real time for remote control and sensor alignment while storing the high resolution video data in on-board memory for later analysis.

9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft to Reduce BLOS SATCOM Dependency. The increased use of RPAS will require a commensurate consumption of available bandwidth. This will require an improved information transfer system. Allowing RPAS operation from manned C2 aircraft with LOS to the RPA could alleviate bandwidth issues and would reduce the reliance on satellites for BLOS SATCOM. Stationing the MCE in a C2 aircraft could further enhance GCS survivability. Experimentation is already ongoing in this area and controlling the RPA's sensor payload from an airborne platform is currently being tested.[11]

9.5.2 Enhancing Detection Avoidance

9.5.2.1 Increase the Level of Automation to Minimize RPAS Radio Transmissions. An RPAS requires a reliable data link to be operated remotely. This results in continuous radio transmissions to and from the RPA. Future RPAS should incorporate highly automated functions such as waypoint navigation, pre-defined flight profiles, active and passive countermeasures or on-board sense and avoid. These methods would minimize the dependence on radio transmissions. However, the level of automation should be thoroughly balanced against the necessity for human interaction to ensure compliance with moral and legal issues associated with RPAS operations.

9.5.2.2 Use Frequency Spreading Techniques to Lower the Probability of Intercept of RPAS Data Links. Deliberately spreading radio signals over a broad spectrum makes them highly resistant to jamming unless the adversary has prior knowledge of the spread characteristics. The signal should be modulated and encrypted to make it appear like radio noise and to mask it from an unwary adversary.

9.5.2.3 Use Frequency Hopping Techniques to Lower the Probability of Intercepting RPAS Data Links. Frequency hopping techniques use the ability to quickly shift the operating frequency to counter radio communications interference. It also hampers triangulation of the transmitter by enemy electronic reconnaissance. However, frequency hopping alone does not provide complete protection against eavesdropping and jamming. To lower the probability of data link interception, frequency hopping should be used as a complementary method along with other measures such as frequency spreading or encryption.

9.5.2.4 Reduce Radio Signal Strength to Lower RPAS Data Link Detectability. The employment of transmitter power management techniques offers the possibility of reducing the signal strength to the absolute minimum required thereby lowering the detectability of RPAS communications. Conversely, signal strength management also permits the increase of signal power if needed, e.g. to overpower spurious signals.

9.5.2.5 Reduce Duty Cycles of Radio Transmissions to Lower RPAS Data Link Detectability. An excellent way to remain undetected is to eliminate all radio communications. This is an unlikely ability due to RPAS dependency on remote control or the demand for real-time imagery, so RPAS radio transmissions should be reduced as much as possible (cf. 9.4.2.2). This is accomplished through the use of improved data compression algorithms. It is especially beneficial for high resolution sensor data transfer. This would result in less data being transferred which results in lower duty cycles.

9.5.3 Enhancing Engagement Avoidance

9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping or Exploitation of RPAS Transmissions. To enhance RPAS data link survivability, all radio transmissions to and from the RPA should be appropriately encrypted. This includes downlinks from the RPA to ROVER or other types of ground-based, portable receiver systems. This would deny an adversary the ability to intercept and exploit the transmitted data for their own purposes. The encryption should be strong enough to endure enemy decryption attempts for long enough time, so deciphered data is obsolete and operationally useless.

9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes to Improve Resistance to Deception. Feeding false data into RPAS receivers is arguably more dangerous than jamming as it provides an adversary the potential of taking control of the RPA. In addition to encrypting the data link (cf. 9.5.3.1); transmitters should be required to authenticate themselves to the receiver with a unique authentication code embedded in the transmitted signal. This would ensure the receiver only accepts signals from trusted sources, which would improve resistance to enemy deception attempts. Some of the techniques that provide resistance to jamming help to resist enemy deception attempts also (cf. 9.5.2.2 and 9.5.2.3).

9.5.3.3 Maximize On-Board Data Processing and Data Compression to Minimize RPAS Radio Transmissions. Measures aimed at protecting the data link and ensuring data link integrity typically increase the size of the data stream. This further consumes the available bandwidth. High-speed, on-board data processing and data compression techniques could reduce the demand for bandwidth by transmitting only relevant data in a highly compressed manner, e.g. only individual moving objects instead of an entire FMV stream. This could enable improved countermeasures and reduce the probability of intercept which could help mask the RPA's location. The amount of on-board data processing and data compression in future RPAS should be maximized to reduce radio transmissions.

9.5.4 Enhancing Hit Avoidance

9.5.4.1 Incorporate Larger Antennas with Increased Signal Power and Higher Focus to Increase Gain. In general, antennas must discriminate between the preferred signals and unwanted noise. Increasing the signal's power and concentrating it into a narrow beam increases the likelihood of over-

coming enemy jamming. On the receiver side, a large, directional antenna ensures radio signals from outside the main lobe will be received with much less energy and the preferred signal is intensified. Larger antennas with a narrower focus increase the effective gain and ability to nullify enemy disturbances. To overcome the size limitations of current RPA, the airframe could be modified to accommodate larger antennas.

9.5.4.2 Use Frequency Spreading Techniques to Improve RPAS Data Link Persistence. Spreading radio signals over a broad frequency spectrum not only helps hide it from enemy interception, (cf. 9.5.2.2) it also makes the signal more resistant to narrowband interference. To successfully jam a broad frequency spectrum, the jammer must spread its power across the entire bandwidth. This results in the jamming signal being less effective and a correspondingly better signal-to-noise ratio for friendly RPAS communications.

9.5.5 Enhancing Hit Tolerance

9.5.5.1 Establish a 'Routing-Enabled' Airborne Network to Maintain RPAS Data Link Connectivity under Adverse Conditions. In computer-based networks, routing is the process of forwarding data packets from their source to their ultimate destination through intermediate network nodes. Adaptive routing algorithms compensate for network failures by forwarding the data packages via alternative nodes. In the future, any air platform could act as a node in an airborne network, capable of routing and forwarding network traffic. This would allow improved resistance against interference to the data link, extend the range of radio communications and enable a more flexible use of available bandwidth.

9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones to Strengthen RPAS Data Links. Although not yet commercially available, stratospheric airships are already in development.[12,13] They could act as substitutes for geostationary satellites with the advantage of being re-deployable to meet operational requirements. A distributed group of stratospheric airships could form the backbone of a deployable airborne network. These could provide redundant BLOS communication for RPAS and other air platforms. Smaller solar powered 'relay RPA' could boost the airborne network where required.[14]

9.5.5.3 Increase Transmitter Power to Achieve Better RPAS Data Link Resistance to Enemy Jamming. Increasing transmitter power is the forceful way to overcome jamming. Simply stated, the objective is to generate more transmitting power than the enemy jammer. Although, this is easily achievable by ground-based transmitters, the SWaP restrictions of an RPA make this option less feasible. Despite the current limitations of RPA, incorporating stronger transmitters in the RPAS ground (and eventually space) segments should be considered.

9.5.5.4 Use On-Board Buffer Memory and Time-Shift Functionality to Restore Imagery after Data Link Interruptions. The RPAS data link may be interrupted by atmospheric conditions, bad weather or enemy electromagnetic interference. The RPA should be capable of recording all relevant sensor data in an on-board buffer and transmit it when connectivity is re-established. If the amount of buffered data is too large to be re-transmitted within the available bandwidth, a time-shift capability should enable the operator to directly access a specific time of the buffered video (cf. 9.5.1.2).

9.5.5.5 Incorporate Additional Navigational Backup Systems to Continue Operating in GPS Denied Environments. RPA require GPS satellite signals to navigate. Loss of those signals can easily occur either by hostile jamming or simply due to atmospheric disturbances. Inertial Navigation Systems (INS) provide an adequate level of accuracy to continue flight operations but not for precision strike operations. INS are not designed to provide the sole source of navigation information in GPS denied environments. Terrain mapping, star navigation and INS navigation methods could be combined in RPAS to enable accurate navigation in GPS denied environments.

9.6 Enhancing Support Element Survivability

9.6.1 Threat Suppression Measures

No recommendations found.

9.6.2 Enhancing Detection Avoidance

9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements. The typical airport infrastructure is easily located due to its sheer size. Although RPAS ground installations benefit from being part of the airport infrastructure, this may serve to reveal their presence to enemy reconnaissance. To avoid being detected, RPAS ground components should be capable of conducting mobile operations without relying on static airport infrastructure.

9.6.2.2 Reduce RPA Launch and Landing Distance Requirements to Permit the Use of Improvised Airstrips. Current RPA typically require a prepared runway of several thousand feet in length for launch and recovery operations. As a pre-requisite for mobile operations (cf. 9.6.2.1) the RPA must become independent from prepared runways and have the capability of landing and taking off on improvised airstrips. Reducing the take-off and landing distance requirements permits greater flexibility in the use of improvised airstrips.

9.6.2.3 Camouflage and Disperse RPAS Ground Elements to Obstruct Enemy Reconnaissance Efforts. Unit camouflage and dispersion strongly reduces the detectability of RPAS ground components by blending in with the natural environment or making them appearing unsuspicious (cf. 9.4.2.3). Although this is a very basic military tactic, recent missions in the asymmetric environment have shown that combat units have not followed this principle. To thwart enemy reconnaissance efforts, RPAS ground elements must consider unit dispersion and camouflage techniques.

9.6.3 Enhancing Engagement Avoidance

9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions. Establishing operational routines like launch times, mission briefings, lunch breaks, or location routines e.g. using RPA parking areas or RPA launch and recovery corridors, offer a great opportunity for an adversary to determine when and where to strike. Unpredictability can serve to counter enemy intelligence efforts, to complement force protection, and help to avoid enemy engagements. To keep an adversary from identifying time and location related routines, routines should be changed often, but irregularly.

9.6.3.2 Introduce an RPAS Air-to-Air Refuelling Capability to Increase the Distance Between RPAS Ground Elements and the AOO. Range is limited by the amount of fuel RPA can carry. The maximum distance between the launch and recovery site and the AOO is a direct consequence of this relationship. To increase the distance between the RPAS ground elements and the AOO, the RPA should be air-refuelable. The first step in acquiring an RPAS Air-to-Air Refuelling (AAR) capability could be the adoption of current AAR procedures and the use of a manned tanker aircraft to refuel the RPAS. As a future capability requirement, fully automated AAR between solely remotely piloted systems should be an objective.

9.6.3.3 Develop an Air-to-Air Rearmament Concept to Minimize the Dependency on Deployed Ground-Based Support Units. Once an RPA has released its weapons, it must land to rearm. This imposes limitations on RPA endurance and loiter time. (cf. 9.6.3.2) Future RPA may incorporate internal weapon bays with a magazine-like functionality for standard munitions which can be rearmed via a loading bay on the RPA's top side. Fully automated docking manoeuvres between the RPA and an remotely piloted weapon carrier airship are conceivable as a future vision. This could potentially minimize or eliminate the requirement to deploy RPAS ground elements.

9.6.3.4 Consider Hypersonic Propulsion to Enable Intercontinental Employment. Theoretically, hypersonic propulsion could accelerate aircraft up to multiple times the speed of sound. This would enable them to reach any destination on the planet within a couple of hours. Hypersonic RPAS could conduct worldwide

reconnaissance as well as combat missions and would enable them to be launched and recovered from inside the home country. This capability would completely eliminate the requirement for deploying ground-based RPAS support elements.

9.6.3.5 Consider Solar Powered Propulsion for RPAS to Maximize their Endurance and Range. If endurance is preferred over airspeed like during ISR missions, solar powered propulsion may help to increase on-station time to the maximum extent possible. RPAS operations would then be limited only by maintenance requirements. Solar powered ultra-long endurance RPAS could eliminate the necessity for deploying RPAS ground elements entirely. However, due to their low airspeed and the amount of surface area required to accommodate solar panels, they might be as vulnerable to threats as current ISR RPAS and should be designed with a focus on expendability. Although this type of RPAS may require a very long travel time to its operational location, the virtually infinite endurance that comes from using solar powered propulsion would help to compensate for this capability limitation.

9.6.4 Enhancing Hit Avoidance

9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects to Enhance Survivability. As long as there is a requirement to deploy support units into theatre, they may be in range of enemy surface-to-surface or air-to-surface weapons. If detection avoidance (cf. 9.6.2) and engagement avoidance (cf. 9.6.3) measures are not an option, support element workspaces should be sheltered against kinetic effects from direct fires and fragmentation to improve support element personnel survivability.

9.6.5 Enhancing Hit Tolerance

9.6.5.1 Consider Installing Armour on Mobile RPAS Support Element Components. Static support element infrastructure could be hardened and sheltered to protect personnel and material from kinetic effects. (cf. 9.6.4.1) When conducting mobile operations, the support element must rely on their vehicles to provide a minimum level of protection. In order to withstand the impact of fragmentation and small arms fire, an adequate level of armour should be installed to all mobile RPAS support element components.

1. Christian G. Watt, Lt Col, USAF, 'Aircrew Fatigue Management', Air War College, Air University, 2009.
2. Tobias Nisser, Carl Westin, 'Human Factors Challenges in Unmanned Aerial Vehicles (UAVs): A Literature Review', Lund University School of Aviation, 2006.
3. 'Raytheon's Mini IFF Transponders to be Used on Korean Air UAVs', Unmanned Systems Technology, 19 Jun. 2013. [Online]. Available: http://www.unmannedsystemstechnology.com/2013/06/raytheons-mini-iff-transponders-to-be-used-on-korean-air-uavs/. [Accessed 01 Apr. 2014].
4. 'Bublcam: 360º Camera Technology for Everyone', Bubl Technology Inc., [Online]. Available: https://www.kickstarter.com/projects/bublcam/bublcam-360o-camera-technology-for-everyone. [Accessed 17 Feb. 2014].
5. Kine Seng Tham, Gary Langford, Ravi Vaidyanathan, 'Enhancing Combat Survivability of Existing Unmanned Aircraft Systems', Naval Postgraduate School, Monterey, California, 2008.
6. 'Commercial Sources of Aerial/Satellite Imagery with Global Coverage', Virtual Terrain Project (VTP), [Online]. Available: http://vterrain.org/Imagery/commercial.html. [Accessed 04 Mar. 2014].
7. NATO Class II Area restrictions are outlined in the Allied Command Europe (ACE) Security Directive 70-1
8. Leapfrog: to go ahead of (each other) in turn; specifically, to advance (two military units) by keeping one unit in action while moving the other unit past it to a position farther in front
9. Noah Shachtman, 'Computer Virus Hits U.S. Drone Fleet', WIRED.com, 10 Jul. 2011. [Online]. Available: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/. [Accessed 07 Jan. 2014].
10. The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it.
11. Jeremiah Gertler, 'U.S. Unmanned Aerial Systems', Congressional Research Service, 2012.
12. 'High Altitude Airship', Lockheed Martin, [Online]. Available: http://www.lockheedmartin.com/us/products/lighter-than-air-vehicles/haa.html. [Accessed 26 Mar. 2014].
13. 'StratoBus – halfway between a drone and a satellite', Thales Group, 10 Mar. 2014. [Online]. Available: https://www.thalesgroup.com/en/worldwide/space/case-study/stratobus-halfway-between-drone-and-satellite. [Accessed 27 Mar. 2014].
14. 'Atmospheric Satellites', TITAN Aerospace, 2013. [Online]. Available: http://titanaerospace.com/. [Accessed 26 Mar. 2014].


© US Air Force

CHAPTER X

Conclusions

Enhancing RPAS survivability is a complex task that not only involves the RPA itself, but includes all other RPAS elements. This study identified more than 100 individual recommendations throughout the entire RPAS. They encompass measures in the air, ground and cyber-domains. However, there is no single or generic solution that is suitable for all types of remotely piloted systems currently in use by NATO nations. Some recommendations may be easily and quickly adopted whereas others are expected to take years of development and integration. This chapter summarizes the given recommendations with respect to the identified criticality levels and the expected timeframe for successful implementation.

10.1 Remotely Piloted Aircraft and Payload

10.1.1 Critical Shortfalls and Vulnerabilities

Current RPAS were never intended to operate in contested environments. Consequently, signature reducing measures, warning receivers, countermeasures, high airspeeds and manoeuvrability were not a design priority. Payload improvements focused on incorporating improved sensors for air-to-ground imagery but not focused on providing optimal situational awareness for the aircrew are also a concern. These shortfalls make current systems not only highly visible to enemy radar systems, but also highly vulnerable to threats directed against them.

10.1.2 Improving the Performance of Existing RPA

Improving the performance of current and legacy RPA requires a comprehensive approach. It should not

only encompass technical upgrades, but also adjustments to the operational use of RPA and implementation of combat oriented flight training for aircrews.

10.1.2.1 Technical Possibilities. Due to their SWaP limitations, current RPA are not as 'upgradable' as manned aircraft. However, there are a lot of survivability enhancement solutions originally developed for manned aircraft that simply may be adapted to RPA without too much effort. The first step to improve current RPA should be to determine what techniques used for manned aircraft can be easily incorporated. Since fundamental changes of the airframe or engine are very unlikely, the focus of improving current RPA should be on integrating warning systems, countermeasures, weapons and improving operator situational awareness.

- **Warning Systems and Countermeasures.** The effects from AAA, SAF and MANPADS can be avoided by operating at appropriate altitudes, so warning systems should focus on detection of SAM and AAM. As those systems typically use radars, RWR would be the most appropriate choice. MWS that detect IR or Ultraviolet (UV) emissions from approaching missiles may complement the RWR to trigger appropriate countermeasures.
- **Weapons.** Current RPAS operate at roughly comparable altitudes to manned combat aircraft but at a significantly lower speed. This results in a reduced weapon range which correlates to a reduced standoff range for the RPA in air-to-ground combat. To mitigate this shortfall, current PGM should be upgraded with extended range kits. Upgrading current RPA with air-to-air weapons would imply incorporating an entire air combat sensor suite as well. This would most likely push current RPA to their SWaP limits. Additionally, most advanced air-to-air missiles have unit costs which equal or exceed the value of current RPA. Equipping current and especially legacy RPAS with advanced air-to-air weapons is therefore not recommended.
- **Situational Awareness.** Improving the situational awareness of RPAS aircrew inherently results in a demand for more bandwidth as more information from the RPA to the GCS must be transmitted. However, in a network centric environment, not all information must come directly from the RPA. It could also originate from other sources. In addition to the fusion of sensor information, future RPA designers should seek to achieve a 'virtual presence' of the aircrew in the RPA. A first step could be incorporating currently available, 360 degree camera systems to eliminate the so called 'soda straw' view.

10.1.2.2 Operational Possibilities. Improving the survivability of current RPA may be achieved by operationally adapting to the threat environment as well. This could be done by operating at higher altitudes, assigning manned fighter escorts or using RPAS in a threat suppression role.

- **Higher Altitude.** Current RPA already operate at altitudes above the so-called 'trash envelope' of AAA, SAF or MANPADS. Further increasing the operational altitude would force an adversary to use more sophisticated and therefore more expensive weapons to successfully engage the RPA. An adversary may then elect to refrain from engaging an RPA due to a negative cost-benefit analysis and save his weapons for higher valued targets. Aircrews, warning systems and countermeasures also benefit from increasing the operational altitude due to an increased threat reaction time.
- **Assigning Fighter Escorts.** Aircraft which offer unique capabilities such as bombers, tankers or airborne early warning are usually protected by fighter aircraft. These escorts temporarily provide local permissive airspace to operate those assets. Unique RPAS capabilities could be protected accordingly using similar TTP. However, defending RPAS capabilities should be judiciously balanced against the additional risk to manned escort aircraft.
- **RPAS in a Threat Suppression Role.** To temporarily provide a local permissive air environment for friendly air operations, existing RPAS should be considered for the SEAD mission. Although the size and weight of HARMs may only permit the installation of only one or two weapons, RPAS would offer greater endurance than manned aircraft. This could offer longer on-station times for friendly air operations and would eliminate the risk to a pilot in this high threat

scenario. As a prerequisite, the RPA must be equipped with an RWR to provide the required situational awareness of enemy radar sites.

10.1.2.3 Training Possibilities. RPAS aircrews may or may not have a background as combat aircraft pilots as not all nations recruit them from manned aviation. Some nations have introduced a separate career for RPAS personnel, qualifying them to fly only RPA. Those RPAS aircrews have never experienced real air-to-air combat. Education and training syllabi for RPAS operators should incorporate aerial combat on an elementary level to increase the probability of successfully evading threats.

10.1.3 Future Vision for Remotely Piloted Aircraft

This study has determined that it is very unlikely there will be a 'one size fits all' solution for future RPAS. Multi-role systems offering a multitude of capabilities are expected to be very expensive. This would contradict the principle of RPAS expendability due to their sheer unit price. This study recommends optimizing future RPAS for specific purposes as outlined below.

10.1.3.1 Deep Penetration RPAS. Deep Penetration RPAS would conduct reconnaissance and air strikes deep in enemy territory. They should be optimised for remaining undetected across the entire electromagnetic spectrum. This would require not only traditional stealth shaping techniques and radar absorbing materials, but also an extensively higher degree of automation to reduce C2 communications to an absolute minimum. As supersonic speed and very high altitudes would further support the survivability of a Deep Penetration RPAS, the incorporated sensors and weapons would have to be capable of providing appropriate results under these circumstances as well. Deep Penetration RPAS are expected to be high value assets, not only in financial, but technological terms as well. To avoid revealing highly classified technology and data, a deep strike RPA must incorporate a reliable self-destruct mechanism.

10.1.3.2 Combat RPAS. Combat RPAS could conduct air-to-air and air-to-ground combat alongside manned fighter aircraft. They could operate on their own in non-permissive and hostile air environments as well. The absence of a human in the aircraft would allow Combat RPAS to sustain higher G-forces and would be limited only by the airframe's aerodynamics. Combat RPAS should incorporate comprehensive sensor suites that can provide a real-time, comprehensive air picture. This would enable them to react automatically to any incoming threats. Combat RPAS should be capable of conducting automated offensive and defensive flight manoeuvres, outperforming any manned fighter aircraft. They should be capable of coordinating their flight manoeuvres as a formation automatically, enabling them to simultaneously attack single or multiple targets. In order to enable the operator to cope in such a dynamic environment, workload should be reduced to a minimum. For example, it should only consist of choosing from multiple pre-defined flight manoeuvres and approving the release of lethal weapons. Combat RPAS are expected to be the most expensive and technologically advanced RPAS.

10.1.3.3 Swarm RPAS. In contrast to highly expensive Deep Penetration or Combat RPAS, Swarm RPAS should be relatively cheap and expendable. They should be designed to operate together in large numbers, forming a swarm to simply overwhelm the adversary's defensive capabilities. These are to be the 'system of choice' for most dull, dirty and dangerous tasks. They may be individually armed, releasing their munitions and returning to their base, or may consist only of a warhead which will make the Swarm RPA an individual strike asset. They could eventually take the SEAD role from manned combat aircraft. Unarmed versions could serve as decoys, luring AD sensors and weapons away from manned aircraft and high value assets. As a prerequisite, the swarm should be capable of coordinating its flight manoeuvres automatically, permitting operation by a single aircrew. The swarm should also be capable of adapting to the loss of individual RPA, reorganizing the remaining RPA as needed during combat operations.

'Quantity has a quality all its own.'
Russian saying

10.1.3.4 Carrier RPAS. Aircraft carriers provide the ability to project military power and deterrence globally. Carrier RPAS should use this concept to project military power in a similar way. Unlike their naval counterparts, they will not carry individual aircraft, but will carry an immense stock of long-range, precision-guided air-to-air and air-to-ground munitions instead. They may also carry air surveillance radars and act as an armed, airborne early warning asset. Ultra long endurance and a massive cargo lifting capability may be achieved by using a solar powered airship instead of a conventionally powered aircraft. Integrated into a future net-centric environment, other Allied manned and remotely piloted aircraft could have remote access to the weapons load carried by the Carrier RPAS. This reach-back capability could enable unarmed Swarm RPAS to employ weapons from the Carrier RPAS to engage hostile targets. Carrier RPAS should be capable of defending itself to a certain degree, but would be dependent on additional external assets such as NATO's Airborne Early Warning and Control System (AWACS).

10.1.3.5 Reconnaissance RPAS. Armed or unarmed Reconnaissance RPAS would continue providing the capabilities that current MALE/HALE RPAS deliver, but with upgraded sensor suites to enable better situational awareness than today's systems. They would still be required to operate in benign air environments and would be enabled by Swarm or Combat RPAS. Reconnaissance in non-permissive or hostile environments would become a mission for Deep Penetration RPAS.

10.2 Ground-Based RPAS Elements

10.2.1 Critical Vulnerabilities

BLOS communications permit RPAS ground installations to be located anywhere on the globe. RPAS elements located in the AOO share the threat and force protection measures of other deployed combat support troops. This study didn't identify any risks unique to deployed RPAS personnel. However, the vulnerability assessment is significantly different for home-based RPAS installations and personnel. Because home-based RPAS personnel remotely operate RPA from several thousands of miles away from hostilities, their threat perception is lower. Home-based RPAS personnel are able to join their families and live their normal lives after their combat shifts conclude. It is because of this reason the off-duty environment was identified as a critical vulnerability. This study couldn't identify any protective measures currently in place for the off-duty environment. On the contrary, countless press-related references were found clearly revealing names and photos of RPAS personnel. This may open a window of opportunity to identify and target RPAS personnel in their home country. Attacks on RPAS personnel's families, friends and homes cannot be ruled out.

10.2.2 Improving Force Protection

10.2.2.1 Deployed RPAS Ground Elements. Improving the survivability of deployed RPAS ground components should employ established and proven measures such as camouflage and dispersion of equipment, reducing radio transmissions or increased mobility to facilitate leapfrog operations. However, the best way to protect deployed RPAS ground elements would be to not deploy them at all, so the range of RPA must be significantly improved that they can be launched and recovered from inside NATO territory. An automated air-to-air refuelling and rearmament capability for RPAS would be essential in achieving this goal. With the exemption of disposable Swarm RPAS, all envisioned future RPAS as described above (cf. 10.1.3) should strive for this capability.

10.2.2.2 Home-Based RPAS Ground Elements. The recommended key actions to protect home-based RPAS infrastructure and personnel should focus on threat suppression and detection avoidance.

- **Threat Suppression.** Pre-emptively deterring threats for home-based RPAS infrastructure and personnel must not be considered a military only task. Military FPCON should be complemented with additional protective measures provided by local civilian authorities. Comprehensive and joint civil and military force protection measures should also encompass the domestic environment to include families of RPAS personnel.

- **Detection Avoidance.** RPAS ground components locations and identities of RPAS personnel should be protected, deterring adversaries from obtaining information on where to strike. This requires adopting communication and classification guidelines as they are established for other units particularly at risk.

10.3 Command, Control, Communications and Computers

10.3.1 Critical Vulnerabilities

RPA remote control is completely dependent on a reliable data link. This is in turn dependent on a reliable network and communication infrastructure. This infrastructure is dependent on secure computer and radio systems. An adversary could select a variety of vulnerable points to attack. The following were identified as the most critical vulnerabilities.

10.3.1.1 Physical Destruction of SATCOM Equipment. Large satellite terminals are easily recognizable and fixed installations could be identified by publicly available, Google Earth pictures. Delivering enough kinetic effect to fatally damage a satellite dish does not require sophisticated weapons. Depending on the range, a high calibre sniper rifle could accomplish this.

10.3.1.2 Interference with RPAS Radio Transmissions. RPAS radio communications utilise various transmitters and receivers not only on the RPA, but also the GCS, satellites and possibly relay stations. Disrupting any one of those connections would compromise the data link of the respective RPAS. Completely repelling any jamming effect in this type of environment is highly unlikely. Given the right circumstances, all radio systems can be jammed, it only takes 1950s technology to take out 21st century communications.

10.3.1.3 Cyber-Attacks against RPAS Computer Systems. Cyber-security is an extremely fast and adaptive battlefield. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms. Reportedly, RPAS computer systems, as well as thousands of other military computers, have already been infected with malicious software. This is most likely due to the prolific use of discs and removable drives. Once discovered, it took several years to disinfect the compromised systems. Eventually, the human factor turned out to be the weakest link for gaining access to even highly secured and physically separated military networks.

10.3.1.4 Corruption of Integrated Circuit Supply Chains. The supply chain for microelectronics is extremely diffuse, complex and globally dispersed. This makes it difficult to verify the trust and authenticity of the electronic equipment used in the RPAS. Deliberate modification of the product assembly and delivery could provide an adversary with capabilities to completely sidestep any software-based security countermeasures. For example, extraction of encryption keys by carefully modifying the involved integrated circuits has already been demonstrated.

10.3.2 Improving Command, Control, Communications and Computer Security

Improvement of RPAS Command, Control, Communications, and Computer (C4) security must be comprehensive and should encompass the physical components required for RPAS communication, the computer systems (to include their software packages), the electromagnetic spectrum they operate in, and any personnel with access to the RPAS. Any of them may be subject to different types of attack and require different efforts to protect them.

10.3.2.1 Physical Components. GCS should follow the same principles of camouflage, dispersion and mobility like any other ground-based element aiming to avoid detection. However, as they cannot be hidden from view, satellite terminals should employ a different approach. They should apply remoteness, deception and redundancy techniques.

10.3.2.2 Computer Systems. The financial benefits of incorporating COTS computer hardware should be thoroughly balanced against the inherently superior security of proprietary systems. If COTS systems are preferred, trustworthy supply chains for these hardware components and their sub-components must be ensured.

10.3.2.3 Software Packages. Capable, trustworthy and updated security software suites are essential in defending computer networks. Cutting off potential entry points into the RPAS, e.g. network bridges or removable devices, would further improve cyber-security. In addition to these defensive measures, offensive and pre-emptive cyber-operations should be conducted to eliminate threats in advance.

10.3.2.4 Electromagnetic Spectrum. Use of the electromagnetic spectrum is required for all RPAS operations. This study strongly recommends the immediate incorporation of already available protective measures. Future RPAS development should focus on reducing radio communications dependency by introducing new means of data transmissions and increasing RPA automation.

10.3.2.5 Human Personnel. To prevent corruption, adversary recruitment or blackmail attempts, RPAS personnel should receive mandatory training to raise the awareness of those issues. Keeping the identities of RPAS personnel classified could also help to deter those activities. In addition, computer system access policies (both for software and hardware) should be as restrictive as necessary to defend against intrusion attempts or exploitation of human carelessness.

10.4 Automation and Human Interaction

'In three years, Cyberdyne will become the largest supplier of military computer systems. All stealth bombers are upgraded with Cyberdyne computers, becoming fully unmanned. Afterwards, they fly with a perfect operational record. The Skynet Funding Bill is passed. The system goes online on August 4th, 1997. Human decisions are removed from strategic defense. Skynet begins to learn at a geometric rate. It becomes self-aware 2:14 AM, Eastern time, August 29th. In a panic, they try to pull the plug.'

Quote taken from the Movie
'Terminator 2 – Judgment Day'

Future use of higher levels of automation is a prerequisite in enabling many of the recommendations made in this study. Future RPAS are projected to perform automated flight between waypoints selected by the operator. This will significantly lower the need for radio communications as a permanent C2 data link, making it no longer necessary. They are also predicted to automatically take-off, land, refuel, navigate and eventually conduct combat manoeuvres. These capabilities already exist, providing the prerequisites to introduce them into future RPAS. Automated target identification and engagement was introduced a decade ago in 155mm artillery sub-munitions. The automated take-off and landing of RPA on a carrier flight deck has recently been demonstrated by the U.S. Navy. Automated flight navigation is a common capability of many currently available business aircraft.

However, what is technically possible is not necessarily desirable. The automated release of lethal weapons should be considered very judiciously with respect to legal, moral and ethical questions. This study recommends two fundamental types of lethal weapon release, i.e. deliberate attack and automated defence.

- **Deliberate Attack.** For any target that requires approval by the Joint Targeting Process (this includes pre-planned, dynamic and time-sensitive targets) a deliberate human decision for weapon release must be enforced.
- **Automated Defence.** Automated weapon release should be approved for any target that is actively engaging the RPA. The threshold of what is considered an active attack should follow the same principles as for manned combat aircraft.

Although technically feasible, this study refrains from recommending an 'Automated Attack' mode for RPAS. Such an automated attack mode would entail a multitude of legal, moral and ethical questions.

10.5 Final Remarks

Remotely Piloted Aircraft Systems are still in their infancy. The current state of RPAS development is often compared to the point at which the Wright Flyer first took flight in 1903. Academia, industry, regulatory au-

thorities as well as the military are working diligently to improve RPAS and better integrate them into the civilian airspace and military force structures. The current and future vulnerability issues highlighted in this document are provided to help improve the effectiveness, efficiency and overall safety of RPAS in future combat operations and to stimulate further thought and analysis. We welcome your comments on this study or any future issues it identifies. Please feel free to contact the author of this document at the JAPCC staff via email: rpas@japcc.org

'War is not about fairness; it's about inflicting damage on your enemy without suffering damage yourself. RPA provide one of those asymmetries...'
Lieutenant General (ret.) Dave Deptula, US Air Force, 2013

ANNEX A

Recommendations to Improve RPAS Survivability Against SBAD Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.1.1.1 Ensure Crew Rotations are Properly Scheduled		x		x			
9.1.1.2 Sustain Properly Trained Crews at All Times			x	x			
9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats		x		x			
9.1.1.4 Employ Sensor Capabilities to Detect Surface-/ Air-Based Threats		x			x		
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats		x			x		
9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning		x		x			
9.1.1.7 Control Image/Video Resolution Requirements to a Reasonable Level to Improve RPAS Stand-Off Range		x		x			
9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats		x	x	x			
9.1.1.10 Consider Stratospheric Employment of RPAS to Suppress Surface-/Air-Based Threats	x	x				x	
9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection	x	x			x		
9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection		x	x	x			
9.1.2.3 Reduce the Remotely Piloted Aircraft's Radar Signature to Impede Enemy Detection	x					x	
9.1.2.4 Reduce the Remotely Piloted Aircraft's Noise Signature to Lower the Range of Audibility	x				x		
9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature to Lower the Spotting Range	x			x			
9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature to Impede Enemy Detection	x				x		
9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection in the Electromagnetic Spectrum	x					x	
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x		x		x		
9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness	x		x		x		
9.1.3.3 Install Identification, Friend or Foe Transponders	x			x			
9.1.3.4 Consider Employment of Decoy RPA to Distract from High Value or Mission Critical RPA	x	x				x	
9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness for RPAS Operators	x				x		
9.1.3.6 Increase Operating Altitude to Avoid Engagement by SAF, AAA and Low Tier SAMs		x		x			
9.1.3.7 Consider RPAS Operations in the Stratosphere to Avoid Engagement by Most Weapons	x					x	
9.1.3.8 Increase RPA Operational Cruise and Top Speed to Enhance its Stand-Off Capabilities	x				x		
9.1.4.1 Increase RPA Manoeuvrability	x					x	
9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators			x	x			
9.1.4.3 Incorporate Automated Laser Warning Systems	x		x		x		
9.1.4.4 Incorporate Missile Warning Systems	x		x		x		
9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection and Tracking	x				x		
9.1.5.1 Consider Partial Component Redundancy	x				x		
9.1.5.2 Minimize the Exposure of Critical System Components	x				x		
9.1.5.3 Incorporate Passive Damage Suppression Measures	x				x		
9.1.5.4 Incorporate Active Damage Suppression Components	x				x		
9.1.5.5 Incorporate Reconfigurable Flight Control Systems	x				x		
9.1.5.6 Develop Universal/Modular RPAS Assemblies to Quickly Repair Damaged Components	x				x		
9.2.1.1 Equip RPA With High-Speed Anti-Radiation Missiles	x	x			x		

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.2.1.2 Incorporate Gunfire Detection Systems and Self-Protection Missiles	x					x	
9.2.1.4 Reduce the Size of Active Jamming Systems to Introduce ECM Capabilities to RPAS	x					x	
9.2.2.1 Integrate Payloads Internally Into the Airframe	x				x		
9.2.2.2 Consider Use of Micro-Munitions to Support Internal Payload Integration	x				x		
9.2.2.3 Incorporate Retractable Sensors	x				x		
9.2.3.1 Incorporate 360 Degree Field of View Optical Systems	x		x		x		
9.2.3.2 Improve Sensor Sensitivity and Angular Resolution	x				x		
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x	x			x	
9.2.3.4 Consider Armament with Non-Lethal Weapons to Minimize Collateral Damage ...	x	x	x		x		
9.2.3.5 Consider Implementation of Extended Range Air-to-Ground Weaponry	x	x		x			
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x				x		
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x				x		
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x		x		x		

ANNEX B

Recommendations to Improve RPAS Survivability Against Combat Aircraft and Adversary RPAS Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.1.1.1 Ensure Crew Rotations are Properly Scheduled		x		x			
9.1.1.2 Sustain Properly Trained Crews at All Times			x	x			
9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats		x		x			
9.1.1.4 Employ Sensor Capabilities to Detect Surface-/ Air-Based Threats		x			x		
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats		x			x		
9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats		x	x	x			
9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA	x				x		
9.1.1.10 Consider Stratospheric Employment of RPAS to Suppress Surface-/Air-Based Threats	x	x				x	
9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection	x	x			x		
9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection		x	x	x			
9.1.2.3 Reduce the Remotely Piloted Aircraft's Radar Signature to Impede Enemy Detection	x					x	
9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature to Lower the Spotting Range	x			x			
9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature to Impede Enemy Detection	x				x		
9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection in the Electromagnetic Spectrum	x					x	
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x		x		x		
9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness	x		x		x		
9.1.3.3 Install Identification, Friend or Foe Transponders	x			x			
9.1.3.4 Consider Employment of Decoy RPA to Distract from High Value or Mission Critical RPA	x	x				x	
9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness for RPAS Operators	x				x		
9.1.3.7 Consider RPAS Operations in the Stratosphere to Avoid Engagement by Most Weapons	x					x	
9.1.3.8 Increase RPA Operational Cruise and Top Speed to Enhance its Stand-Off Capabilities	x				x		
9.1.4.1 Increase RPA Manoeuvrability	x					x	
9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators			x	x			
9.1.4.4 Incorporate Missile Warning Systems	x		x		x		
9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection and Tracking	x				x		
9.1.5.1 Consider Partial Component Redundancy	x				x		
9.1.5.2 Minimize the Exposure of Critical System Components	x				x		
9.1.5.3 Incorporate Passive Damage Suppression Measures	x				x		
9.1.5.4 Incorporate Active Damage Suppression Components	x				x		
9.1.5.5 Incorporate Reconfigurable Flight Control Systems	x				x		
9.1.5.6 Develop Universal/Modular RPAS Assemblies to Quickly Repair Damaged Components	x				x		
9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS	x	x	x		x		
9.2.1.4 Reduce the Size of Active Jamming Systems to Introduce ECM Capabilities to RPAS	x					x	
9.2.2.1 Integrate Payloads Internally Into the Airframe	x				x		

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.2.2.2 Consider Use of Micro-Munitions to Support Internal Payload Integration	x				x		
9.2.2.3 Incorporate Retractable Sensors	x				x		
9.2.3.1 Incorporate 360 Degree Field of View Optical Systems	x		x		x		
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x	x			x	
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x				x		
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x				x		
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x		x		x		
9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations		x		x			
9.3.4.1 Protect the Work Areas of RPAS Personnel	x	x		x			
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x	x		x		
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS to Prevent Visual and Electronic Identification		x	x	x			
9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS by Electronic Reconnaissance	x				x		
9.4.2.3 Choose an Inconspicuous Location for the GCS		x	x	x			
9.4.3.1 Enable Deployable RPAS Control Elements to Leapfrog and Handover Command	x	x	x		x		
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x	x		x		
9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It to Be Quickly Relocated …		x	x	x			
9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary		x		x			
9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS Communications	x					x	
9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability …	x					x	
9.4.4.4 Shelter Stationary GCS Equipment from Kinetic Effects		x		x			
9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss	x	x				x	
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network to Maintain RPAS Data Link Connectivity …	x					x	
9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements		x	x		x		
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements to Permit the Use of Improvised Airstrips	x	x	x			x	
9.6.2.3 Camouflage and Disperse RPAS Ground Elements to Obstruct Enemy Reconnaissance Efforts		x	x	x			
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x	x	x			
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …	x	x	x			x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept to Minimize the Dependency on Deployed ... Units	x	x	x			x	
9.6.3.4 Consider Hypersonic Propulsion to Enable Intercontinental Employment	x					x	
9.6.3.5 Consider Solar Powered Propulsion for RPAS to Maximize their Endurance and Range	x				x		
9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects to Enhance Survivability		x		x			
9.6.5.1 Consider Installing Armour on Mobile RPAS Support Element Components	x			x			

ANNEX C

Recommendations to Improve RPAS Survivability Against ASAT Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network to Maintain RPAS Data Link Connectivity …	x					x	
9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones …	x	x				x	

ANNEX D

Recommendations to Improve RPAS Survivability Against EW Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection in the Electromagnetic Spectrum	x					x	
9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness for RPAS Operators	x				x		
9.2.1.4 Reduce the Size of Active Jamming Systems to Introduce ECM Capabilities to RPAS	x					x	
9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS by Electronic Reconnaissance	x				x		
9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss	x	x				x	
9.5.1.1 Incorporate Laser Communication Technology to Eliminate RPAS Radio Transmissions	x					x	
9.5.1.2 Use On-Board Data Storage and Subsequent Analysis if Real Time Imagery is not Imperative	x	x			x		
9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft to Reduce BLOS SATCOM Dependency	x	x	x		x		
9.5.2.1 Increase the Level of Automation to Minimize RPAS Radio Transmissions	x					x	
9.5.2.2 Use Frequency Spreading Techniques to Lower the Probability of Intercept of RPAS Data Links	x				x		
9.5.2.3 Use Frequency Hopping Techniques to Lower the Probability of Intercepting RPAS Data Links	x				x		
9.5.2.4 Reduce Radio Signal Strength to Lower RPAS Data Link Detectability	x				x		
9.5.2.5 Reduce Duty Cycles of Radio Transmissions to Lower RPAS Data Link Detectability	x				x		
9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping or Exploitation of RPAS Transmissions	x	x			x		
9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes to Improve Resistance to Deception	x	x			x		
9.5.3.3 Maximize On-Board Data Processing and Data Compression to Minimize RPAS Radio Transmissions	x				x		
9.5.4.1 Incorporate Larger Antennas with Increased Signal Power and Higher Focus to Increase Gain	x				x		
9.5.4.2 Use Frequency Spreading Techniques to Improve RPAS Data Link Persistence	x				x		
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network to Maintain RPAS Data Link Connectivity …	x					x	
9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones …	x	x				x	
9.5.5.3 Increase Transmitter Power to Achieve Better RPAS Data Link Resistance to Enemy Jamming	x				x		
9.5.5.4 Use On-Board Buffer Memory and Time-Shift Functionality …	x		x		x		
9.5.5.5 Incorporate Additional Navigational Backup Systems …	x		x		x		

ANNEX E

Recommendations to Improve RPAS Survivability Against SSBM Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations		x		x			
9.3.4.1 Protect the Work Areas of RPAS Personnel	x	x		x			
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x	x		x		
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS to Prevent Visual and Electronic Identification		x	x	x			
9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS by Electronic Reconnaissance	x				x		
9.4.2.3 Choose an Inconspicuous Location for the GCS		x	x	x			
9.4.3.1 Enable Deployable RPAS Control Elements to Leapfrog and Handover Command	x	x	x		x		
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x	x		x		
9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It to Be Quickly Relocated …		x	x	x			
9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary		x		x			
9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS Communications	x					x	
9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability …	x					x	
9.4.4.4 Shelter Stationary GCS Equipment from Kinetic Effects		x		x			
9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss	x	x				x	
9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements		x	x		x		
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements to Permit the Use of Improvised Airstrips	x	x	x			x	
9.6.2.3 Camouflage and Disperse RPAS Ground Elements to Obstruct Enemy Reconnaissance Efforts		x	x	x			
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x	x	x			
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …	x	x	x			x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept to Minimize the Dependency on Deployed ... Units	x	x	x			x	
9.6.3.4 Consider Hypersonic Propulsion to Enable Intercontinental Employment	x					x	
9.6.3.5 Consider Solar Powered Propulsion for RPAS to Maximize their Endurance and Range	x				x		
9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects to Enhance Survivability		x		x			
9.6.5.1 Consider Installing Armour on Mobile RPAS Support Element Components	x			x			

ANNEX F

Recommendations to Improve RPAS Survivability Against MANPADS Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.1.1.1 Ensure Crew Rotations are Properly Scheduled		x		x			
9.1.1.2 Sustain Properly Trained Crews at All Times			x	x			
9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats		x		x			
9.1.1.4 Employ Sensor Capabilities to Detect Surface-/ Air-Based Threats		x			x		
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats		x			x		
9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning		x		x			
9.1.1.7 Control Image / Video Resolution Requirements to a Reasonable Level …		x		x			
9.1.1.10 Consider Stratospheric Employment of RPAS to Suppress Surface-/Air-Based Threats	x	x				x	
9.1.2.4 Reduce the Remotely Piloted Aircraft's Noise Signature to Lower the Range of Audibility	x				x		
9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature to Lower the Spotting Range	x			x			
9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature to Impede Enemy Detection	x				x		
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x		x		x		
9.1.3.6 Increase Operating Altitude to Avoid Engagement by SAF, AAA and Low Tier SAMs		x		x			
9.1.3.7 Consider RPAS Operations in the Stratosphere to Avoid Engagement by Most Weapons	x					x	
9.1.4.1 Increase RPA Manoeuvrability	x					x	
9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators			x	x			
9.1.4.3 Incorporate Automated Laser Warning Systems	x		x		x		
9.1.4.4 Incorporate Missile Warning Systems	x		x		x		
9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection and Tracking	x				x		
9.1.5.1 Consider Partial Component Redundancy	x				x		
9.1.5.2 Minimize the Exposure of Critical System Components	x				x		
9.1.5.3 Incorporate Passive Damage Suppression Measures	x				x		
9.1.5.4 Incorporate Active Damage Suppression Components	x				x		
9.1.5.5 Incorporate Reconfigurable Flight Control Systems	x				x		
9.1.5.6 Develop Universal/Modular RPAS Assemblies to Quickly Repair Damaged Components	x				x		
9.2.3.2 Improve Sensor Sensitivity and Angular Resolution	x				x		
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x	x			x	
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x				x		
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x				x		
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x		x		x		
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network to Maintain RPAS Data Link Connectivity …	x					x	

ANNEX G

Recommendations to Improve RPAS Survivability Against Asymmetric Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats		x			x		
9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning		x		x			
9.1.1.7 Control Image / Video Resolution Requirements …		x		x			
9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA	x				x		
9.2.1.2 Incorporate Gunfire Detection Systems and Self-Protection Missiles	x					x	
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x	x			x	
9.2.3.4 Consider Armament with Non-Lethal Weapons …	x	x	x		x		
9.2.4.1 Incorporate Adaptive Spectral Filters to Protect EO/IR Sensors from Being Hit by Laser Energy	x			x			
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x				x		
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x				x		
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x		x		x		
9.3.1.1 Protect Identities of RPAS Personnel		x	x	x			
9.3.1.2 Raise RPAS Personnel's Awareness for Dealing with Social Media and the Internet			x	x			
9.3.1.3 Raise the Media's Awareness of Asymmetric Threats against Home-Based Combatants		x	x	x			
9.3.1.4 Consider RPAS Personnel's Family Environment when Applying Force Protection Conditions Measures		x		x			
9.3.1.5 Establish Close Cooperation with Civilian Authorities		x		x			
9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations		x		x			
9.3.2.2 Prohibit Wearing Name Tags, Badges or Uniforms Outside Military Compounds		x	x	x			
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x	x		x		
9.4.1.2 Apply NATO Class II Security Area Restrictions to the RPAS Control Element Infrastructure		x	x	x			
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS to Prevent Visual and Electronic Identification		x	x	x			
9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS by Electronic Reconnaissance	x				x		
9.4.2.3 Choose an Inconspicuous Location for the GCS		x	x	x			
9.4.2.4 Remove Signs Indicating the Operational GCS Location to Avert On-Site Espionage		x		x			
9.4.3.1 Enable Deployable RPAS Control Elements to Leapfrog and Handover Command	x	x	x		x		
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x	x		x		
9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It to Be Quickly Relocated …		x	x	x			
9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary		x		x			
9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS Communications	x					x	
9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability …	x					x	
9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss	x	x				x	
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x	x	x			
9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects to Enhance Survivability		x		x			

ANNEX H

Recommendations to Improve RPAS Survivability Against Cyber Threats

Recommendation Chapter	Technical Development	Operational Planning	Education & Training	Short Term (< 1 year)	Mid Term (1 - 5 years)	Long Term (> 5 years)	Overall Criticality
9.4.1.1 Consider Pre-Emptive Cyber-Attack Operations to Suppress Enemy Cyber-Capabilities		x		x			
9.4.4.1 Improve Computer Security Techniques and Policies to Defend Against Cyber-Threats	x	x	x	x			
9.4.4.2 Use Proprietary Software and Hardware for the Core Functions of RPAS …	x				x		
9.4.4.3 Raise RPAS Personnel's Cyber-Awareness to Prevent Infiltration of RPAS Computer Systems			x	x			
9.4.5.1 Establish a Redundant RPAS Control Element to Permit Failsafe Control in Case of GCS Loss	x	x				x	
9.4.5.2 Isolate C2 Systems from Kinetic Weapons Payloads to Minimize the Impact of Cyber-Attacks	x					x	
9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping or Exploitation of RPAS Transmissions	x	x			x		
9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes to Improve Resistance to Deception	x	x			x		
9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA	x				x		

ANNEX 1

Short-Term Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.1 Ensure Crew Rotations are Properly Scheduled	x	x				x			x	
9.1.1.2 Sustain Properly Trained Crews at All Times	x	x				x			x	
9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats	x	x				x			x	
9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning	x					x	x			
9.1.1.7 Control Image / Video Resolution Requirements ...	x					x	x			
9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats	x	x							x	
9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection	x	x							x	
9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature ...	x	x				x			x	
9.1.3.3 Install Identification, Friend or Foe Transponders	x	x							x	
9.1.3.6 Increase Operating Altitude ...	x					x				
9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators	x	x				x			x	
9.2.3.5 Consider Implementation of Extended Range Air-to-Ground Weaponry	x									
9.2.4.1 Incorporate Adaptive Spectral Filters ...							x			
9.3.1.1 Protect Identities of RPAS Personnel							x			
9.3.1.2 Raise RPAS Personnel's Awareness for Dealing with Social Media and the Internet							x			
9.3.1.3 Raise the Media's Awareness of Asymmetric Threats ...							x			
9.3.1.4 Consider RPAS Personnel's Family Environment ...							x			
9.3.1.5 Establish Close Cooperation with Civilian Authorities							x			
9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations		x			x		x		x	
9.3.2.2 Prohibit Wearing Name Tags, Badges or Uniforms Outside Military Compounds							x			
9.3.4.1 Protect the Work Areas of RPAS Personnel		x			x				x	
9.4.1.1 Consider Pre-Emptive Cyber-Attack Operations ...								x		
9.4.1.2 Apply NATO Class II Security Area Restrictions ...							x			
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS ...		x			x		x		x	
9.4.2.3 Choose an Inconspicuous Location for the GCS		x			x		x		x	
9.4.2.4 Remove Signs Indicating the Operational GCS Location ..							x			
9.4.3.3 Locate SATCOM Antennas Away from the GCS ...		x			x		x		x	
9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary		x			x		x		x	
9.4.4.1 Improve Computer Security Techniques and Policies ...								x		
9.4.4.3 Raise RPAS Personnel's Cyber-Awareness to Prevent Infiltration of RPAS ...								x		
9.4.4.4 Shelter Stationary GCS Equipment from Kinetic Effects		x			x				x	
9.6.2.3 Camouflage and Disperse RPAS Ground Elements ...		x			x				x	
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x			x		x		x	
9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects ...		x			x		x		x	
9.6.5.1 Consider Installing Armour on Mobile RPAS Support Element Components		x			x				x	

ANNEX J

Mid-Term Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.4 Employ Sensor Capabilities to Detect Surface-/ Air-Based Threats	x	x				x			x	
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats	x	x				x	x		x	
9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA		x					x	x	x	
9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection	x	x							x	
9.1.2.4 Reduce the Remotely Piloted Aircraft's Noise Signature ...	x					x				
9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature ...	x	x				x			x	
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x	x				x			x	
9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness	x	x							x	
9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness for RPAS Operators	x	x		x					x	
9.1.3.8 Increase RPA Operational Cruise and Top Speed ...	x	x							x	
9.1.4.3 Incorporate Automated Laser Warning Systems	x					x			x	
9.1.4.4 Incorporate Missile Warning Systems	x	x				x			x	
9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection and Tracking	x	x				x			x	
9.1.5.1 Consider Partial Component Redundancy	x	x				x			x	
9.1.5.2 Minimize the Exposure of Critical System Components	x	x				x			x	
9.1.5.3 Incorporate Passive Damage Suppression Measures	x	x				x			x	
9.1.5.4 Incorporate Active Damage Suppression Components	x	x				x			x	
9.1.5.5 Incorporate Reconfigurable Flight Control Systems	x	x				x			x	
9.1.5.6 Develop Universal/Modular RPAS Assemblies ...	x	x				x			x	
9.2.1.1 Equip RPA With High-Speed Anti-Radiation Missiles	x									
9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS		x							x	
9.2.2.1 Integrate Payloads Internally Into the Airframe	x	x							x	
9.2.2.2 Consider Use of Micro-Munitions to Support Internal Payload Integration	x	x							x	
9.2.2.3 Incorporate Retractable Sensors	x	x							x	
9.2.3.1 Incorporate 360 Degree Field of View Optical Systems	x	x							x	
9.2.3.2 Improve Sensor Sensitivity and Angular Resolution	x					x				
9.2.3.4 Consider Armament with Non-Lethal Weapons ...	x						x			
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x	x				x	x		x	
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x	x				x	x		x	
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x	x				x	x		x	
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x			x		x		x	
9.4.2.2 Reduce Radio Transmissions ...		x		x	x		x		x	
9.4.3.1 Enable Deployable RPAS Control Elements to Leapfrog and Handover Command		x			x		x		x	
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x			x		x		x	

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.4.4.2 Use Proprietary Software and Hardware for the Core Functions of RPAS …								x		
9.5.1.2 Use On-Board Data Storage and Subsequent Analysis if Real Time …				x						
9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft …				x						
9.5.2.2 Use Frequency Spreading Techniques …				x						
9.5.2.3 Use Frequency Hopping Techniques …				x						
9.5.2.4 Reduce Radio Signal Strength to Lower RPAS Data Link Detectability				x						
9.5.2.5 Reduce Duty Cycles of Radio Transmissions to Lower RPAS Data Link Detectability				x						
9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping …				x				x		
9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes …				x				x		
9.5.3.3 Maximize On-Board Data Processing and Data Compression …				x						
9.5.4.1 Incorporate Larger Antennas with Increased Signal Power and Higher Focus …				x						
9.5.4.2 Use Frequency Spreading Techniques to Improve RPAS Data Link Persistence				x						
9.5.5.3 Increase Transmitter Power to Achieve Better RPAS Data Link Resistance …				x						
9.5.5.4 Use On-Board Buffer Memory and Time-Shift Functionality …				x						
9.5.5.5 Incorporate Additional Navigational Backup Systems …				x						
9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements		x			x				x	
9.6.3.5 Consider Solar Powered Propulsion for RPAS …		x			x				x	

ANNEX K

Long-Term Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.10 Consider Stratospheric Employment of RPAS ..	x	x				x			x	
9.1.2.3 Reduce the Remotely Piloted Aircraft's Radar Signature ...	x	x							x	
9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection ...	x	x		x					x	
9.1.3.4 Consider Employment of Decoy RPA ...	x	x							x	
9.1.3.7 Consider RPAS Operations in the Stratosphere ...	x	x				x			x	
9.1.4.1 Increase RPA Manoeuvrability	x	x				x			x	
9.2.1.2 Incorporate Gunfire Detection Systems and Self-Protection Missiles	x						x			
9.2.1.4 Reduce the Size of Active Jamming Systems to Introduce ECM Capabilities to RPAS	x	x		x					x	
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x				x	x		x	
9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS ...		x			x		x		x	
9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability …		x			x		x		x	
9.4.5.1 Establish a Redundant RPAS Control Element ...		x		x	x		x	x	x	
9.4.5.2 Isolate C2 Systems from Kinetic Weapons Payloads ...								x		
9.5.1.1 Incorporate Laser Communication Technology ...				x						
9.5.2.1 Increase the Level of Automation to Minimize RPAS Radio Transmissions				x						
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network ...		x	x	x		x			x	
9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones ...			x	x						
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements ...		x			x				x	
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …		x			x				x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept ...		x			x				x	
9.6.3.4 Consider Hypersonic Propulsion to Enable Intercontinental Employment		x			x				x	

ANNEX L

Technical Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.9 Incorporate a Self-Destruct Mechanism to Deter Enemy Exploitation of the RPA		x					x	x	x	
9.1.1.10 Consider Stratospheric Employment of RPAS …	x	x				x			x	
9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection	x	x							x	
9.1.2.3 Reduce the Remotely Piloted Aircraft's Radar Signature …	x	x							x	
9.1.2.4 Reduce the Remotely Piloted Aircraft's Noise Signature …	x	x				x				
9.1.2.5 Reduce the Remotely Piloted Aircraft's Visual Signature …	x	x				x			x	
9.1.2.6 Reduce the Remotely Piloted Aircraft's Thermal Signature …	x	x				x			x	
9.1.2.7 Limit RPAS Radio Transmissions to Avoid Detection …	x	x		x					x	
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x	x				x			x	
9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness	x	x							x	
9.1.3.3 Install Identification, Friend or Foe Transponders	x	x							x	
9.1.3.4 Consider Employment of Decoy RPA …	x	x							x	
9.1.3.5 Enhance Sensor Fusion to Improve the Situational Awareness …	x	x		x					x	
9.1.3.7 Consider RPAS Operations in the Stratosphere …	x	x				x			x	
9.1.3.8 Increase RPA Operational Cruise and Top Speed …	x	x							x	
9.1.4.1 Increase RPA Manoeuvrability	x	x				x			x	
9.1.4.3 Incorporate Automated Laser Warning Systems	x					x				
9.1.4.4 Incorporate Missile Warning Systems	x	x				x			x	
9.1.4.5 Incorporate Active Countermeasures Against Thermal Detection …	x	x				x			x	
9.1.5.1 Consider Partial Component Redundancy	x	x				x			x	
9.1.5.2 Minimize the Exposure of Critical System Components	x	x				x			x	
9.1.5.3 Incorporate Passive Damage Suppression Measures	x	x				x			x	
9.1.5.4 Incorporate Active Damage Suppression Components	x	x				x			x	
9.1.5.5 Incorporate Reconfigurable Flight Control Systems	x	x				x			x	
9.1.5.6 Develop Universal/Modular RPAS Assemblies …	x	x				x			x	
9.2.1.1 Equip RPA With High-Speed Anti-Radiation Missiles	x									
9.2.1.2 Incorporate Gunfire Detection Systems and Self-Protection Missiles	x						x			
9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS		x							x	
9.2.1.4 Reduce the Size of Active Jamming Systems …	x	x		x					x	
9.2.2.1 Integrate Payloads Internally Into the Airframe	x	x							x	
9.2.2.2 Consider Use of Micro-Munitions to Support Internal Payload Integration	x	x							x	
9.2.2.3 Incorporate Retractable Sensors	x	x							x	
9.2.3.1 Incorporate 360 Degree Field of View Optical Systems	x	x							x	
9.2.3.2 Improve Sensor Sensitivity and Angular Resolution	x					x				

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x				x	x		x	
9.2.3.4 Consider Armament with Non-Lethal Weapons …	x						x			
9.2.3.5 Consider Implementation of Extended Range Air-to-Ground Weaponry	x									
9.2.4.1 Incorporate Adaptive Spectral Filters …							x			
9.2.4.2 Incorporate Highly Automated Countermeasure Packages	x	x				x	x		x	
9.2.5.1 Consider Payload Redundancy to Compensate for Sensor Failures	x	x				x	x		x	
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x	x				x	x		x	
9.3.4.1 Protect the Work Areas of RPAS Personnel		x			x				x	
9.4.2.2 Reduce Radio Transmissions to Impede Locating the GCS …		x		x	x		x		x	
9.4.3.1 Enable Deployable RPAS Control Elements …		x			x		x		x	
9.4.3.5 Improve Latency and Reliability Issues Associated with BLOS …		x			x		x		x	
9.4.3.6 Incorporate a Fully Automated RPA Launch And Recovery Capability …		x			x		x		x	
9.4.4.1 Improve Computer Security Techniques and Policies …								x		
9.4.4.2 Use Proprietary Software and Hardware for the Core Functions of RPAS …								x		
9.4.5.1 Establish a Redundant RPAS Control Element …		x		x	x		x	x	x	
9.4.5.2 Isolate C2 Systems from Kinetic Weapons Payloads …								x		
9.5.1.1 Incorporate Laser Communication Technology …				x						
9.5.1.2 Use On-Board Data Storage and Subsequent Analysis …				x						
9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft …				x						
9.5.2.1 Increase the Level of Automation to Minimize RPAS Radio Transmissions				x						
9.5.2.2 Use Frequency Spreading Techniques to Lower the Probability of Intercept …				x						
9.5.2.3 Use Frequency Hopping Techniques …				x						
9.5.2.4 Reduce Radio Signal Strength to Lower RPAS Data Link Detectability				x						
9.5.2.5 Reduce Duty Cycles of Radio Transmissions …				x						
9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping …				x				x		
9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes …				x				x		
9.5.3.3 Maximize On-Board Data Processing and Data Compression …				x						
9.5.4.1 Incorporate Larger Antennas with Increased Signal Power and Higher Focus …				x						
9.5.4.2 Use Frequency Spreading Techniques to Improve RPAS Data Link Persistence				x						
9.5.5.1 Establish a 'Routing-Enabled' Airborne Network …		x	x	x		x			x	
9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones …			x	x						
9.5.5.3 Increase Transmitter Power to Achieve Better RPAS Data Link Resistance …				x						
9.5.5.4 Use On-Board Buffer Memory and Time-Shift Functionality …				x						
9.5.5.5 Incorporate Additional Navigational Backup Systems …				x						
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements …		x			x				x	
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …		x			x				x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept …		x			x				x	
9.6.3.4 Consider Hypersonic Propulsion to Enable Intercontinental Employment		x			x				x	
9.6.3.5 Consider Solar Powered Propulsion for RPAS …		x			x				x	
9.6.5.1 Consider Installing Armour on Mobile RPAS Support Element Components		x			x				x	

ANNEX M

Operational Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.1 Ensure Crew Rotations are Properly Scheduled	x	x				x			x	
9.1.1.3 Use Proper Mission Planning Techniques to Avoid Surface-/Air-Based Threats	x	x				x			x	
9.1.1.4 Employ Sensor Capabilities to Detect Surface-/ Air-Based Threats	x	x				x			x	
9.1.1.5 Properly Weaponize the RPA to Suppress Surface-/Air-Based Threats	x	x				x	x		x	
9.1.1.6 Consider Visual and Aural Thresholds in Mission Planning	x					x	x			
9.1.1.7 Control Image / Video Resolution Requirements …	x					x	x			
9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats	x	x							x	
9.1.1.10 Consider Stratospheric Employment of RPAS …	x	x				x			x	
9.1.2.1 Incorporate Terrain Following Flight Technology to Avoid Radar Detection	x	x							x	
9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection	x	x							x	
9.1.3.4 Consider Employment of Decoy RPA to Distract from High Value …	x	x							x	
9.1.3.6 Increase Operating Altitude to Avoid Engagement …	x					x				
9.2.1.1 Equip RPA With High-Speed Anti-Radiation Missiles	x									
9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS		x							x	
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x				x	x		x	
9.2.3.4 Consider Armament with Non-Lethal Weapons …	x						x			
9.2.3.5 Consider Implementation of Extended Range Air-to-Ground Weaponry	x									
9.3.1.1 Protect Identities of RPAS Personnel							x			
9.3.1.3 Raise the Media's Awareness of Asymmetric Threats …							x			
9.3.1.4 Consider RPAS Personnel's Family Environment …							x			
9.3.1.5 Establish Close Cooperation with Civilian Authorities							x			
9.3.2.1 Prohibit Proliferation of Commercial Satellite Imagery of RPAS Installations		x			x		x		x	
9.3.2.2 Prohibit Wearing Name Tags, Badges or Uniforms Outside Military Compounds							x			
9.3.4.1 Protect the Work Areas of RPAS Personnel		x			x				x	
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x			x		x		x	
9.4.1.1 Consider Pre-Emptive Cyber-Attack Operations …								x		
9.4.1.2 Apply NATO Class II Security Area Restrictions …							x			
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS …		x			x		x		x	
9.4.2.3 Choose an Inconspicuous Location for the GCS		x			x		x		x	
9.4.2.4 Remove Signs Indicating the Operational GCS Location …							x			
9.4.3.1 Enable Deployable RPAS Control Elements …		x			x		x		x	
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x			x		x		x	
9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It …		x			x		x		x	
9.4.3.4 Consider the Use of Decoy SATCOM Antennas to Mislead the Adversary		x			x		x		x	

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.4.4.1 Improve Computer Security Techniques and Policies …								x		
9.4.4.4 Shelter Stationary GCS Equipment from Kinetic Effects		x			x				x	
9.4.5.1 Establish a Redundant RPAS Control Element …		x		x	x		x	x	x	
9.5.1.2 Use On-Board Data Storage and Subsequent Analysis …				x						
9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft …				x						
9.5.3.1 Use Strong Encryption to Prevent Enemy Eavesdropping …				x				x		
9.5.3.2 Incorporate RPAS Transmitter-Receiver Authentication Processes …				x				x		
9.5.5.2 Consider the Use of Stratospheric RPAS as Airborne Network Backbones …			x	x						
9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements		x			x				x	
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements …		x			x				x	
9.6.2.3 Camouflage and Disperse RPAS Ground Elements …		x			x				x	
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x			x		x		x	
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …		x			x				x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept …		x			x				x	
9.6.4.1 Shelter RPAS Support Element Workspaces from Kinetic Effects …		x			x		x		x	

ANNEX N

Education & Training Recommendations to Improve RPAS Survivability

Recommendation Chapter	SBAD	Combat Aircraft	ASAT	EW	SSBM	MANPADS	Asymmetric Force	Cyber Warfare	Adversary RPAS	Overall Criticality
9.1.1.2 Sustain Properly Trained Crews at All Times	x	x				x			x	
9.1.1.8 Escort RPA to Suppress Surface-/Air-Based Threats	x	x							x	
9.1.2.2 Conduct Low Level Flights to Avoid Radar Detection	x	x							x	
9.1.3.1 Keep RPAS Pilots/ Operators Focused to Counteract Crew Fatigue	x	x				x			x	
9.1.3.2 Incorporate Radar Warning Receivers to Increase Situational Awareness	x	x							x	
9.1.4.2 Incorporate Aerial Combat Training for RPAS Operators	x	x				x			x	
9.1.4.3 Incorporate Automated Laser Warning Systems	x					x				
9.1.4.4 Incorporate Missile Warning Systems	x	x				x			x	
9.2.1.3 Consider Employment of Air-to-Air Weapons in Future Combat-RPAS		x							x	
9.2.3.1 Incorporate 360 Degree Field of View Optical Systems	x	x							x	
9.2.3.3 Consider Micro/Mini Scout-RPA as Payload of HALE/MALE RPAS	x	x				x	x		x	
9.2.3.4 Consider Armament with Non-Lethal Weapons …	x						x			
9.2.5.2 Consider Emergency Release of Payloads to Avoid Cascading Damage	x	x				x	x		x	
9.3.1.1 Protect Identities of RPAS Personnel							x			
9.3.1.2 Raise RPAS Personnel's Awareness for Dealing with Social Media …							x			
9.3.1.3 Raise the Media's Awareness of Asymmetric Threats …							x			
9.3.2.2 Prohibit Wearing Name Tags, Badges or Uniforms Outside Military Compounds							x			
9.3.5.1 Establish Sufficient Quantities of Qualified RPAS Personnel in Reserve		x			x		x		x	
9.4.1.2 Apply NATO Class II Security Area Restrictions …							x			
9.4.2.1 Locate Satellite Ground Terminals Away from the GCS …		x			x		x		x	
9.4.2.3 Choose an Inconspicuous Location for the GCS		x			x		x		x	
9.4.3.1 Enable Deployable RPAS Control Elements …		x			x		x		x	
9.4.3.2 Enable Stationary RPAS MCEs to Redeploy in a Reasonable Timeframe		x			x		x		x	
9.4.3.3 Locate SATCOM Antennas Away from the GCS and Permit It …		x			x		x		x	
9.4.4.1 Improve Computer Security Techniques and Policies …								x		
9.4.4.3 Raise RPAS Personnel's Cyber-Awareness …								x		
9.5.1.3 Allow RPAS to be Operated from a Manned C2 Aircraft …				x						
9.5.5.4 Use On-Board Buffer Memory and Time-Shift Functionality …				x						
9.5.5.5 Incorporate Additional Navigational Backup Systems …				x						
9.6.2.1 Develop a Mobile Operations Concept of RPAS Ground Elements		x			x				x	
9.6.2.2 Reduce RPA Launch and Landing Distance Requirements …		x			x				x	
9.6.2.3 Camouflage and Disperse RPAS Ground Elements …		x			x				x	
9.6.3.1 Avoid Observable Routines to Deny Enemy Predictions on Future Actions		x			x		x		x	
9.6.3.2 Introduce a RPAS Air-to-Air Refuelling Capability …		x			x				x	
9.6.3.3 Develop an Air-to-Air Rearmament Concept …		x			x				x	

ANNEX O

Acronyms and Abbreviations

AAA	Anti-Aircraft-Artillery
AAR	Air-to-Air Refuelling
ACE	Allied Command Europe
AD	Air Defence
AFB	Air Force Base
AGM	Air-to-Ground Missile
AOO	Area of Operations
ASAT	Anti-Satellite
AWACS	Airborne Early Warning and Control System
BDE	Brigade
BLOS	Beyond Line of Sight
BN	Battalion
BVR	Beyond Visual Range
C2	Command and Control
C3I	Command, Control, Communications, Intelligence
C4	Command, Control, Communications, Computer
CAP	Combat Air Patrol
CCIR	Commander's Critical Information Requirements
CEP	Circular Error Probable
CIA	Central Intelligence Agency
C-IED	Counter Improvised Explosive Device
COCO	Contractor Owned - Contractor Operated
COMSATCOM	Commercial Satellite Communications
COTS	Commercial-off-the-Shelf
COY	Company
CRPA	Controlled Radiation Pattern Antenna
dB	Decibel
dBSM	Decibel Relative to One Square Meter
DEW	Directed-Energy Weapons
DSCS	Defence Satellite Communications System
EA	Electronic Attack
ECM	Electronic Counter Measures
EHF	Extremely High Frequency
EMP	Electromagnetic Pulse
EO/IR	Electro-Optical/Infrared

ESM	Electronic Support Measures
EW	Electronic Warfare
FLIR	Forward Looking Infrared
FMV	Full-Motion Video
FPCON	Force Protection Conditions
FSR	Field Service Representatives
ft	feet
GCS	Ground Control Station
GEO	Geostationary Orbit
GHz	Gigaherz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRD	Ground Resolved Distance
HALE	High Altitude Long Endurance
HARM	High-Speed-Anti-Radiation-Missile
HUD	Head-Up Display
IADS	Integrated Air Defence System
ICBM	Intercontinental Ballistic Missile
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IFF	Identification, Friend or Foe
IHL	International Humanitarian Law
INS	Inertial Navigation System
IR	Infrared
IRBM	Intermediate-Range Ballistic Missile
IRSL	Infrared Signature Level
IRST	Infrared Search and Track
ISR	Intelligence, Surveillance and Reconnaissance
JDAM	Joint Direct Attack Munitions
JFC	Joint Force Commander
KEW	Kinetic-Energy Weapons
kts	knots
LEO	Low Earth Orbit
LGB	Laser-Guided Bomb
LoAC	Law of Armed Conflict
LOS	Line of Sight
LRU	Launch and Recovery Unit
MALE	Medium Altitude Long Endurance
MANPADS	Man-Portable Air Defence System
MCE	Mission Control Element
MEO	Medium Earth Orbit
MRBM	Medium-Range Ballistic Missile
MWS	Missile Warning System
NATO	North Atlantic Treaty Organization
NIIRS	National Interpretability Rating Scale

OAF	Operation Allied Force
ODF	Operation Deliberate Force
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OUP	Operation Unified Protector
OSI	Open Systems Interconnection
PED	Processing, Exploitation and Dissemination
PGM	Precision-Guided Munitions
PL	Platoon
PPSL	Predator Primary Satellite Link
PTSD	Posttraumatic Stress Disorder
RCS	Radar Cross Section
REGT	Regiment
ROA	Remotely Operated Aircraft
ROVER	Remotely Operated Video Enhanced Receiver
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System(s)
RPG	Rocket-Propelled Grenade
RSO	Remote Split Operation
RWR	Radar Warning Receiver
SAF	Small Arms Fire
SAM	Surface-to-Air Missile
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communication
SBAD	Surface-Based Air Defence
SEAD	Suppression of Enemy Air Defence
SECT	Section
SHORAD	Short-Range Air Defence
SOF	Special Operations Forces
SQDN	Squadron
SRBM	Short-Range Ballistic Missile
SSBM	Surface-to-Surface Ballistic Munitions
SWaP	Size, Weight and Power
TTP	Tactics, Techniques and Procedures
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System(s)
UV	Ultraviolet

Joint Air Power Competence Centre

von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org