

November 2016




# Future Unmanned System Technologies

Legal and Ethical Implications  
of Increasing Automation



**Joint Air Power  
Competence Centre**

Cover picture  drone: © Nerthuz / shutterstock, justice: © Kaspars Grinvalds / shutterstock

© This work is copyrighted. No part may be reproduced by any process without prior written permission. Inquiries should be made to:  
The Editor, Joint Air Power Competence Centre (JAPCC), [contact@japcc.org](mailto:contact@japcc.org)

#### **Disclaimer**

This paper is a product of the Joint Air Power Competence Centre (JAPCC). It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO) and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Comments and queries on this document should be directed to the Combat Air Branch, JAPCC. Please visit our website [www.japcc.org](http://www.japcc.org) for the latest information on JAPCC, or e-mail us at [contact@japcc.org](mailto:contact@japcc.org).

#### **Authors and Contributors from the JAPCC**

Lieutenant Colonel André Haider (DEU A)  
Ms Maria Beatrice Catarrasi (ITA LEGAD)

#### **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](mailto:contact@japcc.org)  
Website: [www.japcc.org](http://www.japcc.org)

 Denotes images digitally manipulated



# 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](http://www.japcc.org)  
NCN: +234 or 239 2201 | E-Mail: [contact@japcc.org](mailto:contact@japcc.org)

## FROM:

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

## SUBJECT:

Future Unmanned System Technologies

Legal and Ethical Implications of Increasing Automation

## DISTRIBUTION:

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

Over the last decades NATO has seen a rapid growth in unmanned system technology, particularly in the air domain. The level of automation built into unmanned aircraft has not only increased significantly, but has also reached a level of sophistication at which they are seemingly capable of performing many tasks 'autonomously' and with no necessity for direct human supervision. This development raises concerns amongst the public and expert forums as international law does not currently address the potential legal and ethical issues which may arise from the use of highly automated weapon systems.

The aim of this document is to outline the potential legal and ethical implications of introducing highly automated unmanned systems to the national inventories of NATO's members and partners. As there is not yet a definition of an autonomous weapon in NATO, it also proposes tiers of automation which may be used as a common baseline within NATO to define what autonomy actually is, where it begins and how it delineates itself from automation.

I invite you and your staff to read through this study. We welcome any comments you may have with regard to this document or future issues it identifies. Please feel free to contact the JAPCC's Combat Air Branch via e-mail: [CombatAir@japcc.org](mailto:CombatAir@japcc.org).

**Joachim Wundrak**

Lieutenant General, DEU AF

Executive Director, JAPCC

# TABLE OF CONTENTS

## CHAPTER I

### Introduction

1.1	Aim and Methodology .....	2
1.2	Assumptions.....	2

## CHAPTER II

### Background and Rationale

2.1	History of Automation .....	3
2.2	Current and Potential Future Unmanned System Technologies .....	4
2.3	The Legal and Ethical Dimension of Military Automated, Autonomic, or Autonomous Weapon System Applications .....	5

## CHAPTER III

### The Difference between Automation, Autonomy and Autonomicity

3.1	Automation.....	8
3.2	Autonomy.....	9
3.3	Autonomicity.....	10
3.4	The Perception of Autonomous Behaviour in Automated and Autonomic Systems .....	10
3.5	Human-Machine Interaction.....	10
3.6	Recommended Terminology .....	11

## CHAPTER IV

### Legal Foundations Applicable to Automated, Autonomic, or Autonomous Weapon Systems

4.1	International Human Rights Law.....	14
4.2	International Humanitarian Law.....	14
4.3	Customary Law and Treaty Law .....	15

## CHAPTER V

### Principles of International Law

5.1	Review of Weapons in Accordance with Article 36 of Additional Protocol I.....	17
5.2	The Principle of Distinction between Civilians and Combatants .....	20
5.3	Principle of Proportionality .....	24
5.4	Principle of Precaution .....	26

## CHAPTER VI

### Responsibilities with Regard to AWS

6.1	Responsibility of the Automated Weapon System .....	28
6.2	Responsibility of the Military Commander .....	29
6.3	Responsibility of the Operator.....	29
6.4	Responsibility of the Manufacturer.....	29
6.5	Responsibility of the Programmer.....	30
6.6	Responsibility of the Deploying Nation .....	30
6.7	Assessment .....	31

## **CHAPTER VII**

### **Ethical Issues**

7.1	The Public Perception of an Autonomous Weapon.....	32
7.2	Arguments Against Automated, Autonomic, or Autonomous Weapon Systems.....	32
7.3	Arguments in Favour of Automated, Autonomic, or Autonomous Weapon Systems.....	33
7.4	Asimov's Three Laws of Robotics.....	33
7.5	Assessment .....	34

## **CHAPTER VIII**

<b>Conclusions.....</b>	<b>35</b>
-------------------------	-----------

## **ANNEX A**

<b>Bibliography.....</b>	<b>37</b>
--------------------------	-----------

## **ANNEX B**

<b>Acronyms and Abbreviations.....</b>	<b>41</b>
--	-----------





**Figure 1 – The Northrop Grumman X-47B demonstrated the first ever carrier-based launches and recoveries by an ‘autonomous’ unmanned aircraft as well as the first ever conducted ‘Autonomous’ Air-to-Air Refuelling.**

## CHAPTER 1

### Introduction

The number of unmanned systems in NATO nations’ military inventories has grown rapidly and is still increasing throughout all domains. Unmanned Aircraft Systems (UAS) currently represent the largest share of those systems. At the same time, the level of automation built into these unmanned systems has not only increased significantly, but has also reached a level of sophistication at which they are seemingly capable of performing many tasks ‘autonomously’ and with no necessity for direct human supervision. Although it is

a common understanding within NATO that autonomous capabilities should not be integrated into lethal weapon systems, there are systems already in service which can be considered to almost have approached that limit, e.g., highly automated cannon-based air defence systems such as Skyshield<sup>1</sup> or Close-In Weapon Systems (CIWS) such as Phalanx.<sup>2</sup> These systems are capable of firing at incoming targets automatically, within seconds of detection of a target, assuming this mode of operation has been activated.

Under the umbrella of the ‘Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be

1. On behalf of the German Bundeswehr, Rheinmetall has developed the ‘Mantis’ (Modular, Automatic and Network capable Targeting and Interception System) air defence system which is a modified and improved version of the ‘Skyshield’ with six fully automated turrets. According to Rheinmetall, it is the most advanced system of its kind worldwide, and it reliably protects military installations such as forward operating bases and other vital facilities from incoming rockets, artillery and mortar rounds. Rheinmetall Defence, Fresh success for Rheinmetall in air defence: MENA nation places new €83 million order (accessed 6 Oct. 2016); available from [http://www.rheinmetall-defence.com/en/rheinmetall\\_defence/public\\_relations/news/archive\\_2014/details\\_5120.php](http://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/news/archive_2014/details_5120.php).
2. At sea, the Phalanx Close-In Weapon System – a rapid-fire, computer-controlled, radar-guided gun system – is designed to defeat anti-ship missiles and other close-in air and surface threats. The Land-based Phalanx Weapon System is part of the U.S. Army’s Counter Rocket, Artillery and Mortar systems used to detect and destroy incoming rounds in the air before they hit their ground targets. Raytheon, Phalanx Close-In Weapon System – Last Line of Defense for air, land and sea, (accessed 6 Oct. 2016); available from <http://www.raytheon.com/capabilities/products/phalanx/>.



**Figure 2 – An unmanned search and tracking sensor unit (l.) and an unmanned gun (r.) of the Skyshield Air Defence System.**

Excessively Injurious or to Have Indiscriminate Effects,’ the United Nations (UN) conducted informal expert meetings on the topic of Lethal Autonomous Weapon Systems (LAWS) in 2014, 2015 and 2016.<sup>3</sup> Succeeding a Multinational Capability Development Campaign (MCDC) on the ‘Role of Autonomous Systems in Gaining Operational Access,’<sup>4</sup> Allied Command Transformation (ACT) is currently working on a ‘Counter Unmanned Autonomous Systems’ concept for the Alliance.<sup>5</sup> However, international law, as well as NATO doctrine, does not currently address the potential legal and ethical issues which may arise from the use of highly automated weapon systems.

## 1.1 Aim and Methodology

The aim of this document is to outline potential legal and ethical implications of introducing highly automated unmanned systems to the national inventories of NATO’s members and partners.

The study provides a brief overview of the current state of technology in the field of system automation and looks at possible future developments. As there is no definition of an autonomous weapon in NATO yet<sup>6</sup>, it also proposes a set of levels or tiers of automation/autonomy which may be used as a common baseline within NATO to define what autonomy actually is, where it begins and how it delineates itself from automation.

After introducing the basic principles of International Humanitarian Law (IHL), often also referred to as Law of Armed Conflict (LOAC), the study outlines the legal requirements a highly automated unmanned system has to meet if NATO nations seeks to introduce this kind of technology and wants to comply with IHL. Moreover, it discusses the potential consequences and responsibilities if automated functions violate international law or cause unintended harm.

Finally, the study briefly discusses the ethical implications of using highly automated systems in military operations and gives an assessment of what may or may not be accepted in NATO.

## 1.2 Assumptions

The study assumes that technological development with regard to unmanned system automation will continue to evolve quickly and will soon reach a level at which direct human supervision is technologically no longer required, despite the fact that a number of delegations to the 2016 UN expert meeting on LAWS stressed that they had no intention of developing such systems.<sup>7</sup>

3. The United Nations Office at Geneva (UNOG), Background – Lethal Autonomous Weapons Systems (accessed 6 Oct. 2016); available from [http://www.unog.ch/80256EE600585943/\(httpPages\)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument).

4. NATO Allied Command Transformation, Multinational Capability Development Campaign (MCDC) 2013–2014, Role of Autonomous Systems in Gaining Operational Access, Policy Guidance, Autonomy in Defence Systems (Artur Kuptel and Andrew Williams, MCDC, 2014)

5. NATO Allied Command Transformation, Innovation Hub, How to Counter Unmanned Autonomous Systems? (accessed 6 Oct. 2016); available from <http://innovationhub-act.org/AxSCountermeasures>.

6. The NATO Glossary of Terms and Definitions does not contain a definition for ‘Autonomy’ or an ‘Autonomous Weapon System’ yet. However, it refers to ‘Autonomous Munitions’ when defining ‘Arming Delay Device’ but without providing any further explanation on the autonomous munitions term. North Atlantic Treaty Organization (NATO), NATO Glossary of Terms and Definitions (AAP-06) (NATO, 2015)

7. Tasking machines to make decisions on the life and death of a human being without any human intervention was considered by many delegations to be ethically unacceptable. Several delegations made the point that they had no intention of developing or acquiring weapon systems of this nature. The United Nations Office at Geneva (UNOG), Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS) (accessed 6 Oct. 2016); available from [http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/DDC13B243BA863E6C1257FDB00380A88/\\$file/ReportLAWS\\_2016\\_Advanced-Version.pdf](http://www.unog.ch/80256EDD006B8954/(httpAssets)/DDC13B243BA863E6C1257FDB00380A88/$file/ReportLAWS_2016_Advanced-Version.pdf).





**Figure 3 – Highly Automated Railway Control Room.**

## CHAPTER 11

### Background and Rationale

#### 2.1 History of Automation

Ideas of intelligent and self-acting machines can be found throughout human history. Centuries-old tales of flying magic carpets can be considered the first vision of an autonomous flying vehicle. Ancient Greek myths include concepts of animated statues or sculptures, envisioning machine intelligence embodied in an actuated physical system. Leonardo da Vinci drew sketches of a programmable mechanism designed to control a spring-propelled cart. These ideas have persisted throughout history, with periodic attempts to achieve some limited set of 'autonomous' functionality using the technology of the time. Although these efforts some-

times produced extremely complex mechanical devices that mimicked human action, they are more properly characterized as works of art than of engineering.<sup>8,9</sup>

Sailboats were likely the first self-propelled vehicles, and possibly the first to have some form of automated steering so that the craft stayed on course, even with shifting winds. Simple guidance systems for torpedoes, which kept them at a constant speed and depth, were already developed by 1860. The first gyroscopic autopilot was invented only nine years after the Wright brothers made their first flight in 1903. By the time of World War II, torpedoes were able to home in on their targets using sonar and the pioneering German ballistic missile V2 navigated itself deep into the British island.<sup>10,11</sup>

With the advent of digital computers and control electronics, 'artificially intelligent' systems were developed

8. Computer History Museum, *Where to? A History of Autonomous Vehicles* (accessed 6 Oct. 2016); available from <http://www.computerhistory.org/atchm/where-to-a-history-of-autonomous-vehicles>.

9. David P. Watson and David H. Scheidt, 'Autonomous Systems,' *Johns Hopkins APL Technical Digest*, vol. 26, no. 4 (2005): 368; available from <http://www.jhuapl.edu/techdigest/TD/td2604/Watson.pdf>.

10. Computer History Museum, *supra* note 8.

11. David P. Watson and David H. Scheidt, *supra* note 9.

that could plan and execute relatively complex operations with little or no human interaction. In the early 1960s nuclear-equipped ballistic missiles were some of the first so-called ‘autonomous’ vehicles to be guided by digital computers.<sup>12, 13</sup>

As the cost of sensors, actuators, and most significantly, processors has dropped over the past decades, there has been significant growth in system automation research for all operational modalities: air, ground, surface, sub-surface, and space. Today, we are witnessing the maturation and transition of this research into a variety of systems to include applications like prototypes of driverless cars or Unmanned Aircraft Systems (UAS), not only in the military but also in the civilian domain.<sup>14, 15</sup>

## 2.2 Current and Potential Future Unmanned System Technologies

Within our modern society, our infrastructure and economy is permeated with civilian automated systems, e.g., traffic flow management systems, manufacturing robots, driverless harvesters, navigation systems, or even robot vacuum cleaners and lawnmowers. Military systems include waypoint navigation for unmanned aircraft (flying by mouse-click), Ground Moving Target Indication (GMTI) and auto-tracking, face-recognition software, guided weapons and much more.

Basically, everything necessary to build a fully automated weapon system is already developed. The different branches of the respective technologies merely have to be brought together. For example, future unmanned combat aircraft may be comprised of the following components:

**System Health and Self-Diagnosis System.** This system could monitor the aircraft’s status and trigger corrective actions if it detected something outside its range of pre-defined values. These systems, such as indicators of engine status, are well established in many of today’s motorized vehicles. In automated mode the System Health and Self-Diagnosis System could report system components requiring service to the maintenance unit, similar to the F-35’s Autonomic Logistics Information System (ALIS).<sup>16</sup> It could also trigger an Automatic Air-to-Air Refuelling (A3R) procedure as tested with the X-47B<sup>17</sup> or initiate an emergency landing on a nearby airfield like the Global Hawk.<sup>18</sup>

**Auto-Pilot.** The auto-pilot would enable the aircraft to not only navigate to its pre-planned mission area but also calculate the route on its own, taking all available data into account, e.g., meteorological information or intelligence about adversary threats. This data could be uploaded during mission preparation prior to launch, updated in real-time during flight or gathered by on-board sensors, enabling the auto-pilot to immediately adapt to new conditions. Assisted by GPS, today’s unmanned aircraft, like the Global Hawk,<sup>19</sup> are already flown by simple ‘point and click’ waypoint navigation or automatically launched and recovered like the Heron<sup>20</sup>, leaving the respective trajectory calculations and control of the aircraft’s surfaces completely with the auto-pilot. Even an automated landing of an unmanned aircraft on an aircraft carrier has been conducted successfully.<sup>21</sup>

**Combat Software Module.** In combat, the aircraft would utilize this respective software application to defend itself or engage adversary targets on its own.

12. Computer History Museum, *supra* note 8.

13. David P. Watson and David H. Scheidt, *supra* note 9.

14. Computer History Museum, *supra* note 8.

15. David P. Watson and David H. Scheidt, *supra* note 9.

16. The Autonomic Logistics Information System (ALIS) serves as the information infrastructure for the F-35, transmitting aircraft health and maintenance action information to the appropriate users on a globally-distributed network to technicians worldwide. Lockheed Martin, Autonomic Logistics Information System (accessed 6 Oct. 2016); available from <http://www.lockheedmartin.com/us/products/ALIS.html>.

17. Defense Systems, Navy extends UAV range with first in-flight refueling (accessed 6 Oct 2016); available from <https://defensesystems.com/articles/2015/04/27/navair-x47b-uas-midair-refueling.aspx>.

18. Once mission parameters are programmed into Global Hawk, the air vehicle can autonomously taxi, take off, fly, remain on station capturing imagery, return, and land. Northrop Grumman, RQ-4 Global Hawk Factsheet (accessed 6 Oct. 2016); available from [http://www.northropgrumman.com/capabilities/rq4block20globalhawk/documents/hale\\_factsheet.pdf](http://www.northropgrumman.com/capabilities/rq4block20globalhawk/documents/hale_factsheet.pdf).

19. *Ibid.*

20. Israel Aerospace Industries (IAI), Heron (accessed 6 Oct 2016); available from [http://www.iai.co.il/2013/18900-16382-en/BusinessAreas\\_UnmannedAirSystems\\_HeronFamily.aspx](http://www.iai.co.il/2013/18900-16382-en/BusinessAreas_UnmannedAirSystems_HeronFamily.aspx).

21. United States Navy, X-47B Makes First Arrested Landing at Sea (Brandon Vinson, USS George H.W. Bush Public Affairs, 2013); available from [http://www.navy.mil/submit/display.asp?story\\_id=75298](http://www.navy.mil/submit/display.asp?story_id=75298).

Its Artificial Intelligence (AI) could predict possible adversary actions almost instantaneously and initiate the appropriate manoeuvres accordingly, giving it superiority over any manned aircraft and making it capable of surviving even the most hostile environments. Recent research has already provided artificially intelligent software for training US Air Force pilots in air-to-air combat simulations. Even at the current (early) stage of this technology, the pilots could not score a single kill once the software had been sufficiently trained. The pilots described it as ‘the most aggressive, responsive, dynamic and credible AI seen-to-date.’<sup>22</sup>

#### **Sensor-Suite with Target Identification Module.**

The sensor suite would provide the auto-pilot and the combat software module with comprehensive situational awareness, enabling them to compute trajectories and combat manoeuvres accordingly. Sophisticated sensor-suites providing this level of awareness can already be found in modern aircraft, e.g., the F-35.<sup>23</sup> For air-to-ground combat, the software would also provide Ground Moving Target Indication (GMTI) and positive identification of designated targets before potentially taking lethal actions against them. Today, GMTI is already included in most of the current UAS operating electro-optical/infrared (EO/IR) sensors or providing full-motion video (FMV).<sup>24</sup> Even publically available software is already capable of recognizing facial patterns and identifying the respective person and/or objects with a very high level of accuracy on a personal computer’s picture archive.<sup>25,26</sup>

**Self-guided Air-to-Air and Air-to-Ground Weaponry.** A mission tailored set of lethal payloads would enable the unmanned combat aircraft to conduct combat operations and engage targets as identified and assigned by the aforementioned software modules. The current stage of self-guided weapons technology would be sufficient to achieve this capability.

As outlined above, all the necessary technology to build a fully automated UAS is already developed and readily available on the market. So the question is no longer if such systems can or should be built; the question is actually when these systems come into service, what missions will be assigned to them and what implications will arise from that development?

## **2.3 The Legal and Ethical Dimension of Military Automated, Autonomic, or Autonomous Weapon System Applications**

In the civil arena, the use of highly automated robotic systems is already quite common, e.g., in the manufacturing sector. But what is commonly accepted in the civilian community may be a significant challenge when applied to military weapon systems. A fully automated or ‘autonomous’ manufacturing robot that does not make decisions about the life or death of human beings will most likely not raise the same legal and ethical questions, if any, that a military weapon system would.

22. Psibernetix Inc, Flagship Defense AI: ALPHA (accessed 6 Oct. 2016); available from <http://www.psibernetix.com/projects/defense>.

23. According to Lockheed Martin, the F-35 has the most powerful and comprehensive integrated sensor package of any fighter aircraft in history, giving pilots 360-degree access to ‘real-time’ battlefield information. Lockheed Martin, F-35 Capabilities - Multi-Mission Capability for Emerging Global Threats (accessed 6 Oct. 2016); available from: <https://www.f35.com/about/capabilities>.

24. As an example, the Kestrel Land MTI is a software solution that automatically detects movement in electro-optical (EO) and infrared (IR) full motion video (FMV) from manned and unmanned aircraft. SentientVision Pty Ltd, KESTREL LAND MTI (accessed 6 Oct. 2016); available from <http://www.sentientvision.com/products/kestrel-land-mti>.

25. Microsoft Corporation, Windows Live Photo Gallery and Movie Maker (accessed 6 Oct. 2016); available from <https://www.microsoft.com/en-US/download/details.aspx?id=26689>.

26. Google, Google Photos (accessed 6 Oct. 2016); available from <https://www.google.com/photos/about>.

27. International Humanitarian Law (IHL) or ‘jus in bello’ is the set of laws that come into effect once a war has begun. Its purpose is to regulate how wars are fought, without prejudice to the reasons of how or why they had begun. This branch of law relies on customary law, based on recognized practices of war, as well as treaty laws (such as the Hague Regulations of 1899 and 1907), which set out the rules for conduct of hostilities. Other principal documents include the four Geneva Conventions of 1949, which protect war victims—the sick and wounded (First); the shipwrecked (Second); prisoners of war (Third); and civilians in the hands of an adverse party and, to a limited extent, all civilians in the territories of the countries in conflict (Fourth)—and the Additional Protocols of 1977, which define key terms such as combatants, contain detailed provisions to protect non-combatants, medical transports, and civil defence, and prohibit practices such as indiscriminate attack.

Any application of military force in armed conflict is usually governed by International Humanitarian Law (IHL)<sup>27</sup> which itself derives from and reflects the ethically acceptable means and customs of war for the time being. Moreover, IHL has been altered and amended over time, taking both the development of human ethics and weaponry into account, e.g., by condemning the use of certain types of weapons and methods of warfare.<sup>28</sup>

The proliferation of unmanned systems, and especially the increasing automation in this domain, have already generated a lot of discussion about their use.<sup>29</sup> The deployment of such systems may entail a paradigm shift and a major qualitative change in the conduct of hostilities. It may also raise a range of fundamental legal and ethical issues to be considered before such systems are developed or deployed. Therefore, this document is not only focussing on the predominant legal aspects but on the ethical dimension as well.

28. Treaties with regard to the use of certain types of weapons include the 1925 Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases, and of Bacteriological Methods of Warfare; the 1972 Biological and Toxin Weapons Convention (BTWC) and the 1993 Chemical Weapons Convention; the 1980 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW); the 1997 Ottawa Treaty on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction.

29. The United Nations Office at Geneva (UNOG), *supra* note 3.



## CHAPTER III

### The Difference between Automation, Autonomy and Autonomicity

The challenge with defining 'automation' and delineating it from 'autonomy' is that these terms are currently buzzwords for many kinds of modern applications and they are used unreflectingly throughout the robotic community. These terms are mostly used without differentiation and the robotic community does not provide an understanding of what the terms actually imply.

Moreover, several government agencies, academia and even individual authors have provided various definitions of 'autonomy' and 'automation'.<sup>30,31,32</sup> The JAPCC also addressed this issue four years ago, calling for a concise, correct and foremost common use of terminology in NATO.<sup>33</sup> However, there is no agreed NATO definition yet.<sup>34</sup> Discussing all of the various methods used to define the two terms would exceed the scope of this document. Therefore this chapter only provides a short summary based on the least common denominator in most of the different approaches. It also provides a definition proposal for the term 'autonomic'<sup>35</sup> aimed at covering those systems which seemingly exceed the definition of 'automation' but are not yet 'autonomous'.

30. The concept of 'level of automation' has been considered by many authors such as Bright (1958), Sheridan (1980), Marsh and Mannari (1981), Kern and Schumann (1985), Kotha and Orne (1989), Draper (1995), Milgram (1995), Anderson (1996), Schwartz (1996), Billings (1997), Endsley and Kaber (1999), Duncheon (2002), or Ruff (2002).

31. U.S. National Institute of Standards and Technology, Autonomy Levels for Unmanned Systems (ALFUS) Framework (accessed 6 Oct 2016); available from [https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP\\_1011-I-2-0.pdf](https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP_1011-I-2-0.pdf).

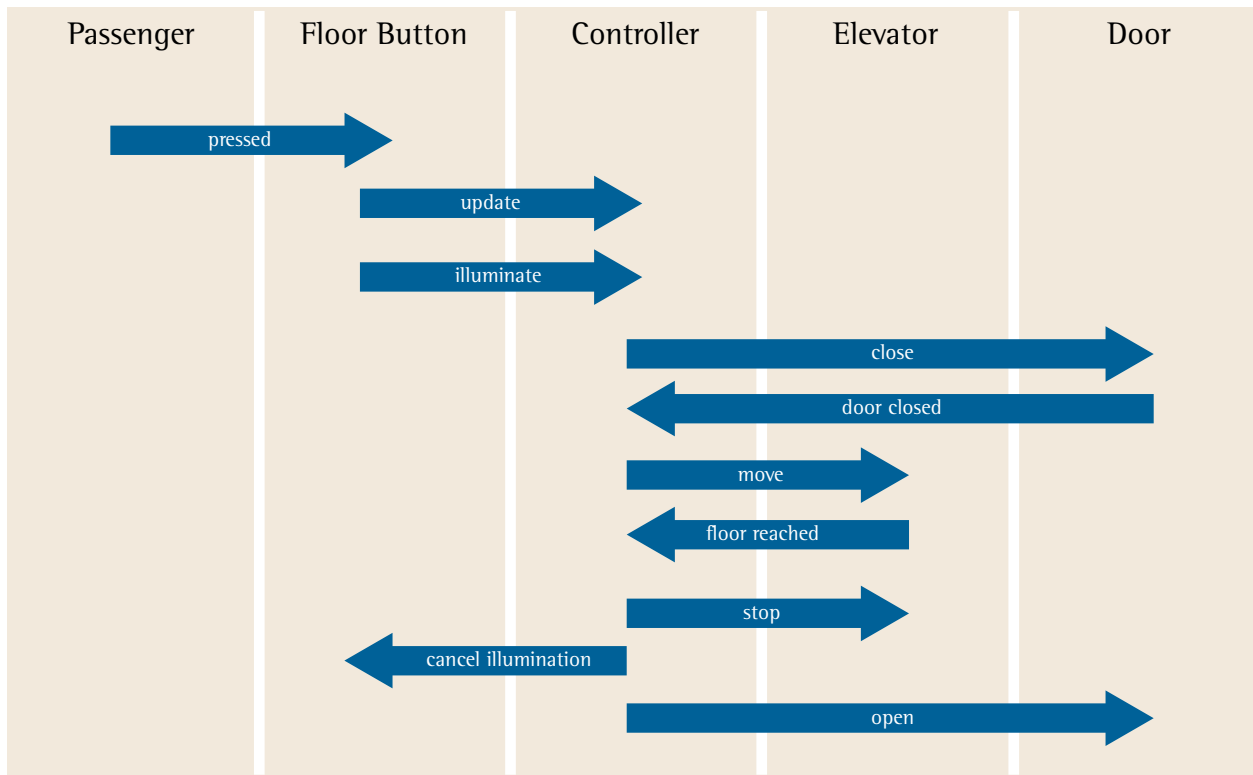
32. Society of Automotive Engineers (SAE), Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (SAE International, 2014).

33. Joint Air Power Competence Centre (JAPCC), Machines Do Not Think! The Contradiction with Autonomous Systems (accessed 11 Oct. 2016); available from: <https://www.japcc.org/portfolio/flyer-9>.

34. NATO AAP-06, supra note 6.

35. The concept of autonomic computing was introduced by the IBM Company in 2001. It should create a computing environment with the ability to manage itself and dynamically adapt to change in accordance with business policies and objectives. Self-managing environments can perform such activities based on situations they observe or sense in the IT environment rather than requiring IT professionals to initiate the task. These environments are self-configuring, self-healing, self-optimizing, and self-protecting. IBM Corporation, An architectural blueprint for autonomic computing (accessed 6 Oct. 2016); available from <http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf>.





**Figure 4 – Illustration of an Elevator’s Control Sequence.**

### 3.1 Automation

In the classical sense, ‘automation’ is an industrial term which allegedly derives from autom(atic) (oper)ation and is believed to be invented by the Ford Motor Company in 1948.<sup>36</sup> At that time automation referred to the fast growth in mechanization where machines took over more and more physical tasks in manufacturing which were formerly conducted by humans. Contemporary interpretations of automation still follow this classical definition but have evolved to reflect the advances in technology and now also refer to the computerization of control and information handling.

The Oxford Online Dictionary provides the following definitions related to automation:

**Automation.** ‘The use or introduction of automatic equipment in a manufacturing or other process or facility.’

**Automatic.** ‘Working by itself with little or no direct human control.’

**Automatism.** ‘The performance of actions without conscious thought or intention.’

Technically, every automated system follows a logical sequence of tasks using some sort of control loop providing feedback if a desired state has been reached and, if not, triggering a pre-defined action to achieve it. One example for such a simple control loop is a car’s cruise control system. As long as the desired state (speed) is not achieved, the controller triggers the necessary engine parts to achieve it. A more complex but still simple control sequence can be found in elevators as shown in Figure 4.

Of course, the more a system is automated, the more complex the control sequences will get. An aircraft’s auto-pilot system, for example, has to control multiple

36. The term automation, inspired by the earlier word automatic, was not widely used before 1947, when the Ford Motor Company established the first automation department. Jeremy Rifkin, *The End of Work: The Decline of the Global Labor Force and the Dawn of the Post-Market Era* (New York, Putnam Publishing Group, 1995).

times more sensors, controllers and even sub-systems to keep the aircraft at the desired direction, speed and altitude. However, even the most complex control sequence is still adhering to the simple principle of sensing a desired state and triggering a respective pre-defined action to achieve it. The defining elements of automation are therefore:

**Predetermination.** Every task conducted by the machine is following a pre-defined sequence based on a logical outcome between sensing a component's current status and comparing it to the desired state.

**Finiteness.** The machine's courses of action are always bound to a limited number of pre-defined actions which are triggered by the software in order to achieve a desired end-state.

**Predictability.** Following the principles of predetermination and finiteness, any task conducted by the machine will be predictable.

## 3.2 Autonomy

In contrast to 'automation' being a technical term, 'autonomy' is historically rooted in moral, political, and legal philosophy. The ancient Greek's term 'autonomos' consists of the two syllables 'auto' and 'nomos' which literally translate to 'self' and 'law'; hence, when combined, were understood to mean 'one who gives oneself one's own law'.<sup>37</sup>

Immanuel Kant, a German philosopher of the 18<sup>th</sup> century, argued that the supreme principle of morality is a standard of rationality that he called the 'Categorical Imperative'.<sup>38</sup> At the heart of his moral theory is the idea of autonomy which he described as '[...] the will of every rational being as a will that legislates universal law.' This contains first and foremost the idea of laws consciously made and laid down by oneself, which can also be expressed as the right to self-determination.<sup>39</sup> In a similar way, the Oxford Online Diction-

ary refers to Autonomy as 'the right or condition of self-government' and 'the capacity of an agent to act in accordance with objective morality.'

So far, machines are limited to actions that fall within the rules in their programming and are unable to make a deliberate and conscious decision. Indeed, it is questionable if the term 'decision' is even applicable in this context. The Oxford Online Dictionary defines 'decision' as 'a conclusion or resolution reached after consideration,' whereas 'consideration' means 'careful thought' which in turn implies 'an idea or opinion produced by thinking.' Therefore, it is most likely that machines never achieve true autonomy in the philosophical sense. However, current technology that can learn or adapt its functioning in response to changing circumstances in the environment obviously exceeds the boundaries of pure automation, resulting in the proliferated but actually incorrect use of the terms 'Autonomy' and 'Decision Making' for such systems.

If ever achieved, a truly autonomous system could be defined by:

**Consciousness.** Based on 'true' artificial intelligence the machine would develop its own will and make deliberate but unrestrained decisions.

**Self-determination.** The machine would no longer follow a pre-defined sequence but learn from preceding outcomes and determine its own courses of action without being bound to its original programming.

**Infiniteness.** The ability to learn and build up 'experience' as well as to exceed its original programming would enable the machine to possibly generate an infinite number of potential courses of action.

**Unpredictability.** Following the principles of consciousness, self-determination and infiniteness, actions conducted by the machine would no longer be predictable.

37. The ancient Greek word 'autonomos' had its antonym in the word 'eteronomos'. 'Autonomos' translates to 'I give myself my laws' or 'the law comes from me' whereas 'eteronomos' translates to 'someone else gives me his laws' or 'the rules come to me from another subject different from me'.

38. Immanuel Kant, *Fundamental Principles of the Metaphysics of Morals* (accessed 6 Oct. 2016); available from <http://www.gutenberg.org/ebooks/5682>.

39. Ibid.

### 3.3 Autonomicity

As aforementioned, current technology already exceeds the boundaries of automation but has not yet reached the threshold of autonomy. This is because current attempts to develop artificially intelligent technology still lacks the ability to provide machines with their own will, which is the prerequisite for un-coerced decision-making and hence self-determination.

Inspired by the human autonomic nervous system, which acts largely unconsciously, the IBM company started the so-called 'autonomic computing' initiative in 2001 to develop self-managing computer systems. These systems are guided by general policies and rules and are capable of self-configuration, self-healing, self-optimization and self-protection.<sup>40</sup>

In contrast to the definition of autonomy, an autonomic system does not govern itself and cannot make unrestrained decisions because it is bound to a set of rules in which it is limited to operate.

Broadly following IBM's original concept, an autonomic system in the context of future unmanned systems can be defined by:

**Objectives.** Although the machine would no longer be forced to follow pre-defined sequences and would possibly be capable of learning from preceding outcomes to determine the best course of action, it would still act according to the overarching goal defined by humans.

**Scope.** The individual actions available to the machine are pre-defined, but to achieve the objective it has freedom to act within its defined boundaries and can independently select from these actions as necessary.

**Certainty.** Although the sequential and temporal conduct of individual actions by the machine is not predictable, the individual action itself is. It is therefore

assured that the machine acts only within the boundaries of its defined objective.

### 3.4 The Perception of Autonomous Behaviour in Automated and Autonomic Systems

Often highly automated or autonomic systems are perceived as autonomous because their behaviour is seemingly unpredictable. In fact, it is not the system but the environment in which it operates which is unpredictable. An automated or autonomic system will always produce exactly the same result and conduct exactly the same actions if the environmental variables remain consistent. Reality, however, is characterized by inconsistencies.

To illustrate this perception of autonomy of a factual autonomic system, a quadcopter used for finding and rescuing people from inside a collapsed building is a good example. The quadcopter is programmed with a set of pre-defined instructions commanding it how to act if it detects an obstacle or a person.<sup>41</sup> In the exact same virtual test environment the robot will always conduct the same actions because the environmental variables, and therefore the sensor input, are constant. In the real world, every collapsed building is disparate and will therefore feed the robot's sensors with different variables. The quadcopter will still follow the same pre-defined instructions but the environment dictates which ones to select. As we cannot predict the environmental variables the robot's behaviour appears autonomous, whereas, in fact, it is not.

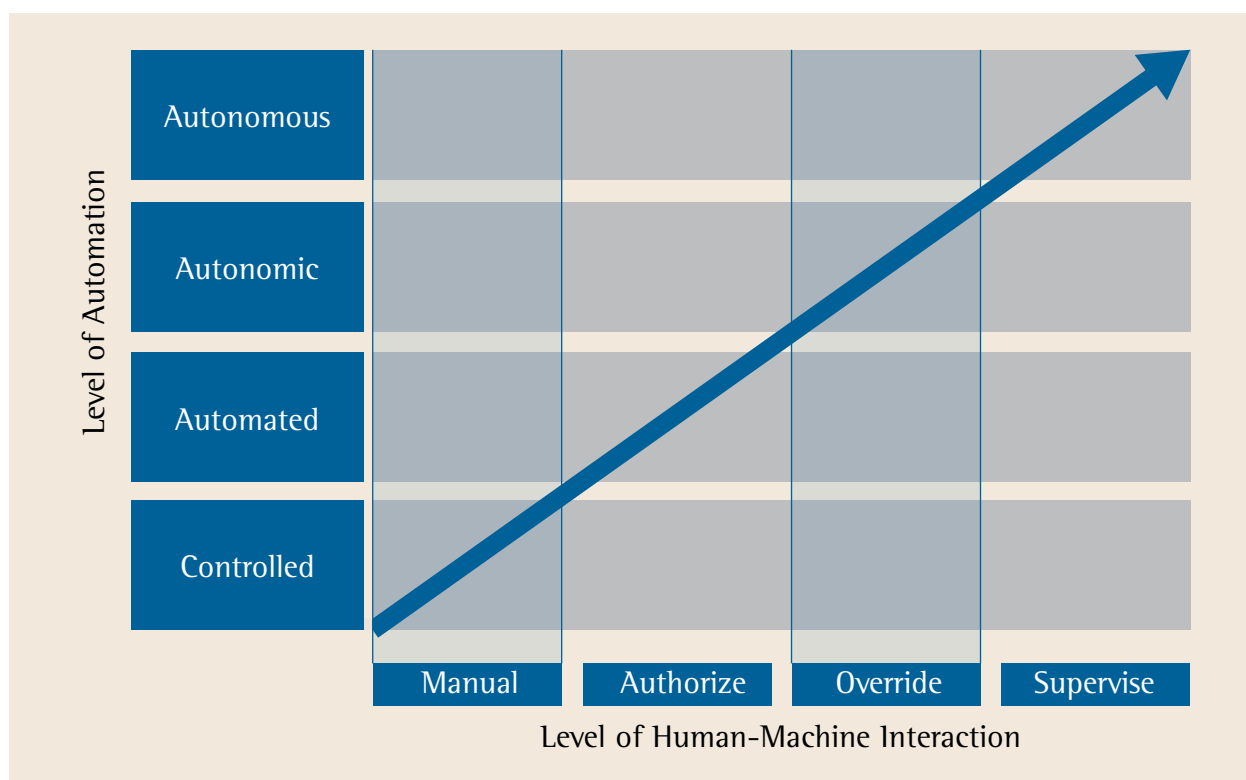
### 3.5 Human-Machine Interaction

Depending on the degree of automation the machine will or will not require a certain level of human interaction to operate. This can range from complete manual control to no interaction at all. Simply put, the higher the degree of automation the lesser the requirement for human interaction.

40. IBM Corporation, *supra* note 35.

41. Shaojie Shen, Nathan Michael, Vijay Kumar, University of Pennsylvania, Autonomous Aerial Navigation in Confined Indoor Environments (accessed 6 Oct. 2016); available from <https://www.youtube.com/watch?v=IMSozUpFFkU>





**Figure 5 – Relation between Level of Automation and Human – Machine Interaction.**

Various concepts sometimes differentiate between up to ten levels of human-machine interaction.<sup>42</sup> As a common baseline, four basic levels can be identified:

**Manual Control.** The machine only executes commands initiated by the operator.

**Authorization.** The machine generates recommendations for action and offers them (or just the preferred one) to the operator for approval before executing it.

**Override.** The machine selects the preferred action and informs the operator prior to execution. Unless the operator does not abort the operation, the machine will execute it.

**Supervision.** The machine selects the preferred action and executes it without human interaction. The operator may be informed during or after the operation.

### 3.6 Recommended Terminology

**Levels of Automation.** Typically, the degree of automation has a direct relationship with the required level of Human-Machine Interaction. Figure 5 illustrates this dependency. As outlined in this chapter it is unlikely that full robot autonomy will be achieved in the near future. Therefore this document deems it appropriate to refer to 'Levels of Automation' instead of 'Levels of Autonomy.'

**Automated, Autonomic, or Autonomous Weapon System (AWS).** For editorial reasons, 'AWS' is used throughout the study to generally and interchangeably refer to an automated, autonomic or autonomous weapon system at the same time. If only a specific level of automation should be addressed it will be explicitly stated and spelled out.

**Lethal Automated, Autonomic, or Autonomous Weapon Systems (LAWS).** AWS may be also capable

<sup>42</sup> Concepts of level of automation, *supra* note 30.

of delivering weapon effects. Such AWS are referred to as Lethal Automated, Autonomic or Autonomous weapon Systems (LAWS).<sup>43</sup>

**Automation, automated.** An automated system follows a pre-defined and finite thus predictable sequence of actions according to initial or continued human authorization.

**Autonomicity, autonomic.** An autonomic system selects from a pre-defined and finite set of actions to achieve its given objective without supervision unless a human intervenes.

**Autonomy, autonomous.** An autonomous system independently decides its own courses of action to achieve its given objective without human intervention.

<sup>43</sup> The term 'LAWS' is also used by the United Nations and refers to 'Lethal Autonomous Weapon Systems' and does not explicitly distinguish between 'automated', 'autonomic' and 'autonomous'. However, in principle both interpretations of the term imply the absence of human control over the machine's actions. UNOG, *supra* note 3.



**Figure 6 - Jean Henri Dunant (8 May 1828 – 30 October 1910), also known as Henry Dunant, was the founder of the Red Cross and the first recipient of the Nobel Peace Prize. The 1864 Geneva Convention was based on Dunant's ideas.**

## CHAPTER IV

### Legal Foundations Applicable to AWS

International Humanitarian Law (IHL) provides no dedicated principles with respect to AWS and some argue that, because of this fact, they are to be considered illegal and should be banned for military applications.<sup>44</sup> However, it is a general principle of law that prohibitions have to be clearly stated or otherwise do not apply. Conclusively, the aforementioned argument for banning AWS is inappropriate.<sup>45</sup> Nevertheless, IHL states that if a specific issue is not covered by

a dedicated arrangement, general principles of established customs such as the principle of humanity and public conscience apply. This so called 'Martens Clause'<sup>46</sup> first appeared in the preamble to the 1899 Hague Convention, stating:

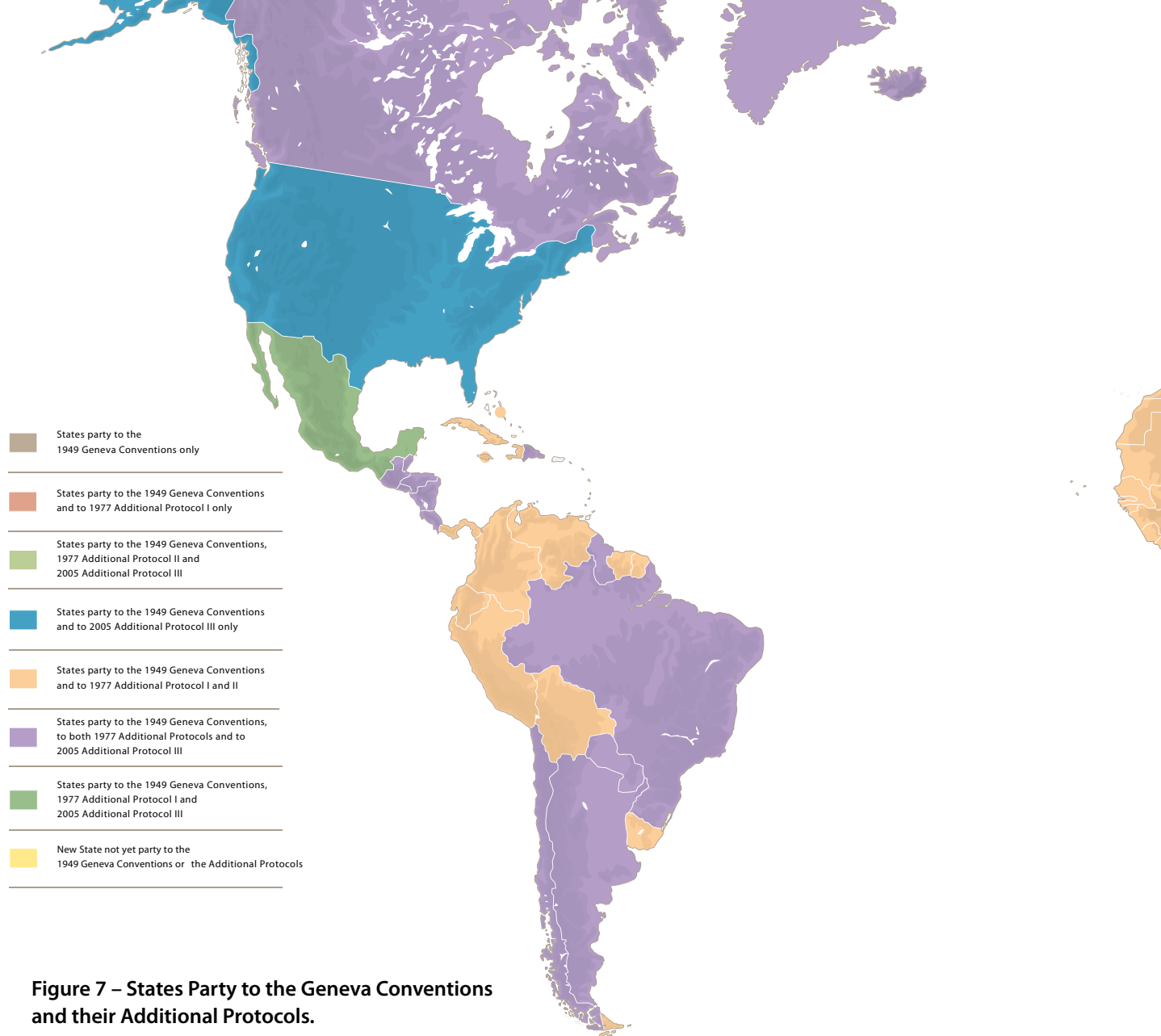
***'Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.'***<sup>47</sup>

44. Human Rights Watch, International Human Rights Clinic (IHRC) at Harvard Law School, Losing Humanity – The Case against Killer Robots (accessed 6 Oct. 2016); available from <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>.

45. The legal principle of 'ubi lex voluit, dixit; ubi noluit, tacuit' is applicable here. It translates to 'When the law wanted to regulate the matter in further detail, it did regulate the matter; when it did not want to regulate the matter in further detail, it remained silent' or 'In the interpretation of a law, an excessively expansive interpretation might perhaps go beyond the intention of the legislator, thus we must adhere to what is in the text of the law and draw no material consequences from the law's silence.'

46. The Martens Clause is found in several treaties relating to International Humanitarian Law. The clause is stated in the preamble of the 1899 and 1907 Hague Conventions, the First and Second Additional Protocol to the Geneva Conventions as well in the main body of the 1949 Geneva Conventions themselves.

47. Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (The Hague, 29 Jul. 1899) [hereinafter HC II]



**Figure 7 – States Party to the Geneva Conventions and their Additional Protocols.**

Consequently, there is no loophole in international law regarding the use of AWS. New technologies have to be judged against the established principles before labelling them illegal in principle. The following sections briefly highlight applicable law regarding the appropriate legal assessment of AWS.

#### 4.1 International Human Rights Law

International Human Rights Law (IHRL) refers to the indisputable fundamental rights to which a human is inherently entitled. It applies to all persons and at all

times, i.e., both in peacetime and in armed conflict.<sup>48</sup> Human rights principles such as the prohibition of torture, cruel, inhumane or degrading treatment are absolute and cannot be limited or suspended.<sup>49</sup> They are laid down in the Universal Declaration of Human Rights (UDHR), proclaimed by the United Nations General Assembly in Paris on 10 December 1948.<sup>50</sup>

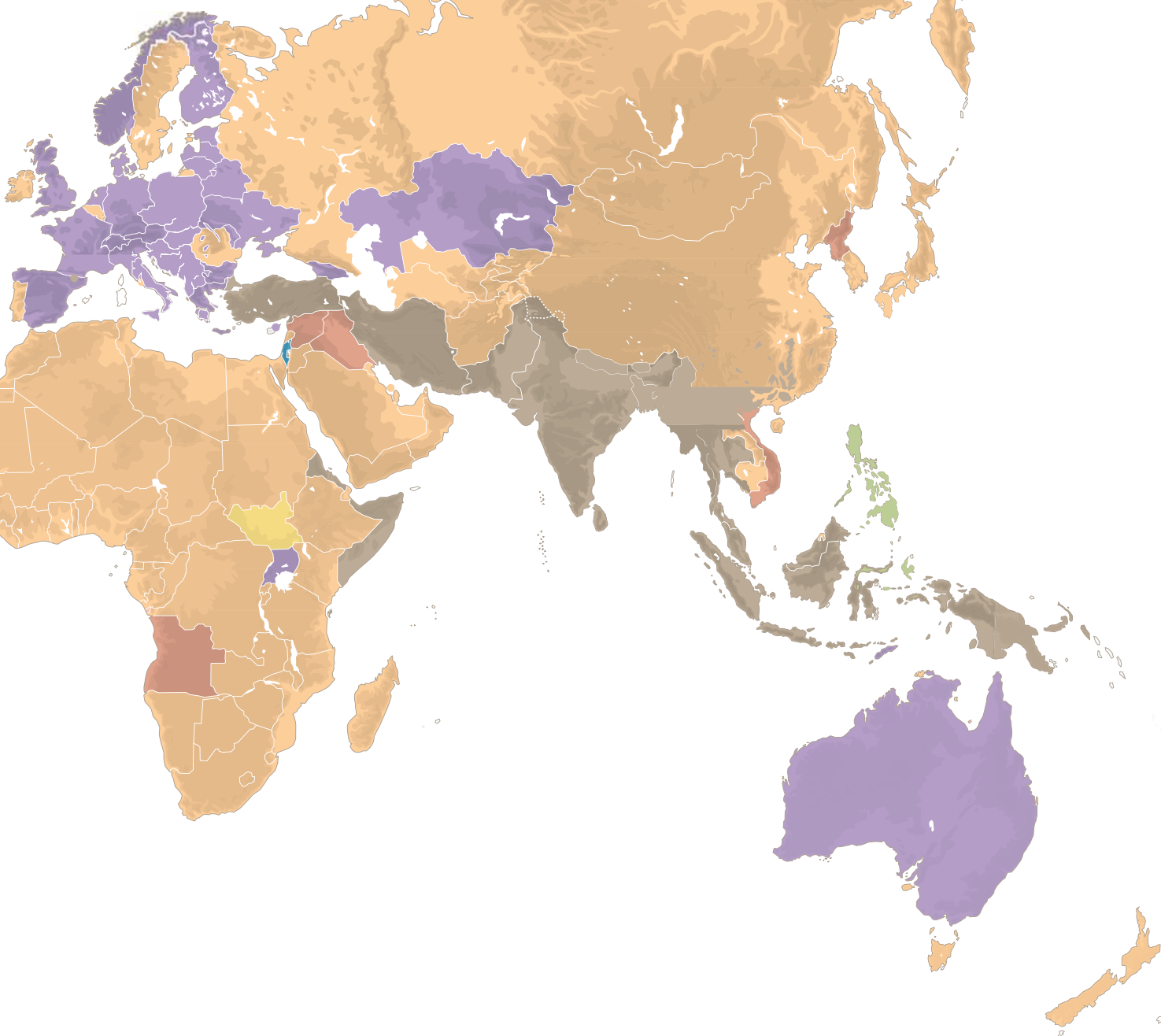
#### 4.2 International Humanitarian Law

In addition to IHRL, which applies at all times, IHL sets rules during armed conflict and military occu-

48. International human rights law is a system of international norms designed to protect and promote the human rights of all persons. These rights, which are inherent in all human beings, [...] are interrelated, interdependent and indivisible. [...] Human rights entail both rights and obligations. International human rights law lays down the obligations of states to act in certain ways or to refrain from certain acts, in order to promote and protect the human rights and fundamental freedoms of individuals or groups. United Nations Human Rights Office of the High Commissioner, *International Legal Protection of Human Rights in Armed Conflict* (New York and Geneva, 2011).

49. Ibid.

50. Universal Declaration of Human Rights (UDHR) (United Nations General Assembly, Paris, 10 Dec. 1948): available from <http://www.un.org/en/universal-declaration-human-rights>.



pation. It regulates the conduct of war and the behaviour during the conduct of hostilities. IHL consists mainly of a series of international treaties concluded in The Hague between 1899 and 1907 and in Geneva between 1864 and 1949, including additional protocols approved in 1977 and 2005. Figure 7 illustrates which states are party to the Geneva Conventions and their Additional Protocols. Together with IHRL, IHL is a complementary source of obligations for parties during an armed conflict.<sup>51</sup>

### 4.3 Customary Law and Treaty Law

Both, IHRL and IHL have origins in customary law and treaty law.

**Customary law** is the oldest pillar on which international law is built. It comprises long established international customs and consistent rules from confirmed practices between states. They express universal values which are generally accepted within the international community and follow the general principles of the law recognized by civilized nations.<sup>52</sup>

51. A complete list of the respective treaties can be found at: International Committee of the Red Cross (ICRC), *Treaties, States Parties and Commentaries*, available from <https://ihl-databases.icrc.org/ihl>.

52. The sources of international law can be found in Article 38 (1) of the Statute of the International Court of Justice: 'The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states; (b) international custom, as evidence of a general practice accepted as law; (c) the general principles of law recognized by civilized nations; [ . . . ]. International Court of Justice (ICJ), *Statute of the International Court of Justice* (accessed 10 Oct. 2016); available from <http://www.icj-cij.org/documents/?p1=4&p2=2>.

Although not laid down in a dedicated treaty, these customs and rules are considered a source of international law, mandatory for every state and, as such, are recognized by the International Court of Justice (ICJ) in The Hague. The original four Geneva Conventions, internationally recognized as the core of IHL, have been ratified by all states, are universally applicable, and binding for every state.<sup>53</sup>

**Treaty law** is the second pillar on which international law is built. Simply put, treaty law can be seen as a contract between states. As such, treaty law does only apply to those states which are a party to the respective treaty. With regard to armed conflict, treaty law particularly includes the three Additional Protocols to the Geneva Conventions as well as the three Hague Conventions, hence binding only those states which ratified them (cf. Figure 7).

53. International Committee of the Red Cross (ICRC), The Geneva Conventions of 1949 and their Additional Protocols (accessed 10 Oct 2016); available from <https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols>.





## CHAPTER V

### Principles of International Law

During armed conflict the IHL's principles of distinction, proportionality and precaution apply. This also implies the obligation for states to review their weapons to confirm they are in line with these principles. This chapter briefly introduces each of the principles and discusses the requirements which have to be met by an AWS to comply with them.

#### 5.1 Review of Weapons in Accordance with Article 36 of Additional Protocol I

The question if AWS would be illegal as such can be answered by referring to Article 36 of the 'Protocol Addi-

tional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts' (AP I).<sup>54</sup> The article states that:

***'In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.'***<sup>55</sup>

Article 36 provides three criteria for basically any type of technology to fall under the provisions of that article. With regard to AWS, it firstly has to be classified as a 'weapon, means or method of warfare.' Secondly, it has to be considered as 'new' and lastly it has to be in development, acquisition or adoption by a state party to the protocol.<sup>56, 57</sup>

54. Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (8 Jun. 1977) [hereinafter AP I]

55. Ibid., Article 36.

56. Marie Jacobsson, 'Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments', *International Law Studies*, vol. 82, pp. 183–191.

57. Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol I' *International Review of the Red Cross*, vol. 85, no. 850, pp. 397–415, 2003.

Article 36 does not impose a prohibition on any specific weapon in general.<sup>58</sup> In fact it accepts any weapon, means or method of warfare unless it violates international law and it puts responsibility on the states to determine if its use is prohibited. Therefore, an AWS cannot be classified as unlawful as such. Like any other weapon, means or method of warfare, it has to be reviewed with respect to the rules and principles codified in international law.

### 5.1.1 Prohibited Weapons in Accordance with Article 35 of Additional Protocol I

If an AWS should be in accordance with IHL as stated in Article 36, it has first and foremost to meet the requirements of Article 35 AP I which states that:

***'It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering ... [and] ... are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.'***<sup>59</sup>

Whether there is a case of superfluous injury or unnecessary suffering is controversial and needs to be balanced against the principle of 'military necessity'.<sup>60</sup> However, the International Committee of the Red Cross (ICRC) commentary regarding AP I lists some internationally agreed prohibitions on weapons to include fragmentation projectiles of which the fragments cannot be traced by X-rays or incendiary weapons in inhabited areas, in particular if delivered by aircraft.<sup>61</sup>

The ICRC's commentary to AP I further states that all methods of war conflicting with the rules of the Proto-

col and the Geneva Conventions are of a nature to cause superfluous injury or unnecessary suffering.<sup>62</sup> In reverse, this can be interpreted that AWS which do comply with the rules of IHL can be expected to not impose superfluous injury or unnecessary suffering and are therefore not prohibited.

### 5.1.2 Classification as a 'Weapon, Means or Method of Warfare'

**Weapons.** Although there is no internationally agreed definition of the terminology, 'weapon' is likely to imply an 'offensive capability that can be applied to a military object or enemy combatant'.<sup>63</sup> Hence, an AWS capable of striking targets can be clearly attributed to meet the requirements for a 'weapon' as it involves the use of force.

**Means or method of warfare** can be interpreted as 'those items of equipment which, whilst they do not constitute a weapon as such, nonetheless have a direct impact on the offensive capability of the force to which they belong'.<sup>64</sup> Advances in technology may lead to software and unarmed platforms which contribute to, or be classified as, means or methods of warfare. In cases where software and/or systems cannot employ weapons without a human decision, this is not a problem. However, when the software and/or system has the ability to 'autonomously' trigger the launch of a weapon, without a human in the decision loop, more extensive review under Article 36 may be necessary.

### 5.1.3 Classification as 'New'

To assess if a weapon, means or method of warfare is 'new' according to Article 36 two different factors

58. The legal principle of 'ubi lex voluit, dixit; ubi noluit, tacuit' is applicable here. Supra note 45.

59. AP I, supra note 54, Article 35.

60. The principle of military necessity is codified in several international treaties, e.g., article 51(5)(b) of the 1977 Additional Protocol I prohibits an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated; article 3(8)(c) of the 1996 Amended Protocol II to the Convention on Certain Conventional Weapons prohibit any placement of mines, booby-traps and other devices "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated; article 8(2)(b)(iv) of the 1998 ICC Statute states that intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects [...] which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated would constitute a war crime.

61. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW) (United Nations Office at Geneva, 21 Dec. 2001) [hereinafter CCW]

62. a contrario ex Article 35 (2) Protocol I 1977 Protocol additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts

63. Justin McClelland, supra note 57.

64. Ibid.



have to be taken into account, i.e., the technical development and the time at which the system is being developed, acquired or adopted.

**Technical Development.** A weapon, means or method of warfare does not necessarily require completely new technology built from scratch to qualify as 'new.' Weapons have been traditionally subject to improvements throughout their lifetime. In this case the impact of the respective upgrade to the weapon's characteristics has to be determined. For example, upgrading an RPA with lighter materials or more efficient engines may enhance its durability and range but would not change its characteristics as it still operates in the same manner. However, installing hardpoints and weapons to an RPA which previously operated unarmed only will significantly change its capabilities and operational use, hence qualifying it as 'new.'

**Time.** Simply put, every weapon affected by an arms acquisition process initiated after the respective state had become a party to the protocol and which had not been part of its military inventory so far is to be considered 'new.' The fact that a weapon has already been in service with other states would not prevent the receiving state from applying this principle.<sup>65</sup>

#### 5.1.4 Ratification of the Protocol

The ICRC argues that Article 36 applies to all states, regardless of whether or not they are party to Addi-

tional Protocol I.<sup>66</sup> This is derived from the fact that states are generally prohibited from using illegal weapons or using their weapons in an illegal manner. This obligation would require any state to review their military inventory to be in compliance with international humanitarian law.<sup>67</sup>

#### 5.1.5 Assessment

From a time perspective, any modern arms acquisition falls under the provision of Article 36 which, in turn, the ICRC considers as a customary rule applicable to all states.<sup>68</sup> Consequently, the only, and therefore decisive, factor to determine if future system automation may create a 'new weapon, means or method of warfare' is its impact on the weapon's characteristics. Admittedly, it is hard to assess if and how a certain degree of automation will potentially change a weapon's characteristics. The definitions of automation, autonomicity and autonomy (cf. Chapter 3) may help to delineate regular weapon system lifecycle improvements from new weapons, means or method of warfare. The automation of routine functions to simply mitigate the workload of the weapon system's operator can be considered 'passive.' The human is still in charge and makes the necessary decisions of if and how the weapon should act. The threshold to qualify for a 'new' weapon may be reached if automation extends to a point where the weapon actively takes over 'decisions' within the targeting process from the operator, potentially blurring the operator's personal obligation, or even ability, to respect the rules and principles of international law.

65. Without necessarily being 'new' in a technical sense, these arms are new for the state which is intending to acquire them after becoming a Party to the Protocol. Thus their introduction is subject to the evaluation provided for in Article 36. [...] This obligation applies to countries manufacturing weapons, as well as those purchasing them. [...] The purchaser should not blindly depend on the attitude of the seller or the manufacturer, but should proceed itself to evaluate the use of the weapon in question with regard to the provisions of the Protocol or any other rule of international law which applies to it. ICRC, Commentary of 1987 – New Weapons (accessed 10 Oct. 2016); available from <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F095453E41336B76C12563CD00432AA1>.

66. The requirement that the legality of all new weapons, means and methods of warfare be systematically assessed is arguably one that applies to all states, regardless of whether or not they are party to Additional Protocol I. It flows logically from the truism that states are prohibited from using illegal weapons, means and methods of warfare or from using weapons, means and methods of warfare in an illegal manner. The faithful and responsible application of its international law obligations would require a state to ensure that the new weapons, means and methods of warfare it develops or acquires will not violate these obligations. ICRC, Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977 (ICRC, Geneva, 2006)

67. Ibid.

68. Ibid.



Figure 8 – Fighters who take the oath during a ceremony on 21<sup>st</sup> June 2014 in Donetsk.

## 5.2 The Principle of Distinction between Civilians and Combatants

**'In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.'**<sup>69</sup>

State practice<sup>70</sup> established the principle of distinction between civilians and combatants as a norm of customary international law,<sup>71</sup> dating back centuries. This

principle was incorporated into treaty law in 1977 and codified in Articles 48, 51(2) and 52(2) of AP I.

This is corroborated by the fact that numerous states which are not party to AP I stipulate that a distinction must be made between civilians and combatants and that it is prohibited to direct attacks against civilians.<sup>72</sup> In addition, under the Statute of the International Criminal Court (ICC), 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities' constitutes a war crime in international and non-international armed conflicts.<sup>73</sup> Therefore, AWS have to meet the require-

69. AP I, supra note 54, Articles 48, 51 (1),(2) and 52 (2).

70. The customary practices of armies as they developed over the ages and on all continents.

71. State practice establishes the principle of distinction between civilians and combatants as a norm of customary international law applicable in both international and non-international armed conflicts. This principle is codified in Articles 48, 51(1),(2) and 52(2) of 1977 Additional Protocol I, as well as in Protocol II, Amended Protocol II and Protocol III to the 1980 Convention on Certain Conventional Weapons and in the 1997 Ottawa Convention banning anti-personnel landmines. At the Diplomatic Conference leading to the adoption of the Additional Protocols, it was stated that Articles 51 and 52 of Additional Protocol I were so essential that they 'cannot be the subject of any reservations whatsoever since these would be inconsistent with the aim and purpose of Protocol I and undermine its basis.' International Committee of the Red Cross (ICRC) [hereinafter ICRC], Customary IHL, Rule 1. The Principle of Distinction between Civilians and Combatants (accessed 10 Oct. 2016); available from [https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1\\_rul](https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul).

72. Numerous military manuals, including those of states not, or not at the time, party to Additional Protocol I, stipulate that a distinction must be made between civilians and combatants and that it is prohibited to direct attacks against civilians, in particular the manuals of France, Israel, United Kingdom and United States. In addition, there are numerous examples of national legislation which make it a criminal offence to direct attacks against civilians, including the legislation of states not, or not at the time, party to Additional Protocol I, in particular the legislation of Italy. ICRC, supra note 71.

73. Article 8(2)(b),(c), Rome Statute of the International Criminal Court (ICC), circulated as document A/CONF.183/9 of 17 Jul. 1998 and corrected by process-verbaux of 10 November 1998, 12 Jul. 1999, 30 Nov. 1999, 8 May 2000, 17 January 2001 and 16 Jan. 2002. [hereinafter Rome Statute] (accessed 10 Oct. 2016); available from <http://legal.un.org/icc/statute/romefta.htm>.

ments of the principle of distinction between civilians and combatants to be compliant with IHL.

### 5.2.1 The Principle of Distinction of Specifically Protected Persons and Objects

In addition to the principle of distinction between civilians and combatants, the Geneva Conventions and the Additional Protocols further demand to distinguish, respect and protect specifically protected persons and objects<sup>74</sup> as long as they do not directly participate in hostilities.<sup>75</sup> Amongst others, this includes

- Medical personnel, units and transports,
- Hospital and safety zones,
- Religious personnel,
- Persons hors de combat,<sup>76</sup>
- Personnel displaying the ICRC's distinctive emblem,
- Humanitarian relief personnel and objects,
- Journalists.

Furthermore, state practice treats peacekeeping forces involved in a peacekeeping mission in accordance with the Charter of the United Nations as civilians because they are not members of a party to the conflict and are deemed to be entitled to the same protection against attack as that accorded to civilians, as long as they are not taking a direct part in hostilities.<sup>77</sup>

Although many of the aforementioned rules regarding specifically protected persons and objects are codified in treaty law, state practice, including that of states not, or not at the time, party to the respective

treaties, establishes this principle as a norm of customary international law.<sup>78</sup> Therefore, AWS have to meet the requirements for distinguishing, respecting and protecting these persons and objects to be compliant with the law.

### 5.2.2 Requirements for the Distinction of Civilians and Protected Persons from Combatants

Protecting civilians from the effects of war is one of the primary principles of IHL and has been agreed state practice since the foundation of the ICRC and the first Geneva Convention.<sup>79</sup> However, applying this principle turned out to be more and more complex as the methods of warfare have evolved. Today's conflicts are no longer fought between two armies confronting each other on a dedicated battlefield. Participants in a contemporary armed conflict may not respect the rules of IHL and not wear uniforms or any distinctive emblem at all, making them almost indistinguishable from the civilian population. In some cases, the civilian population itself may take part in hostilities, in consequence losing their protection against attack.

So, the distinction between civilians, protected persons and combatants can no longer be exercised only by visual means, e.g., uniforms or emblems. The person's behaviour and actions on the battlefield, often referred to as 'pattern of life,' have become a highly important distinctive factor as well.

**Combatant Uniforms and Emblems.** The AWS must be capable of positively identifying uniform patterns

74. ICRC, *supra* note 71, Customary IHL, Rules 25, 27, 31-35, 47, 59.

75. To discuss whether a person is directly participating in hostilities or not would exceed the scope of this document. A dedicated study addressing this issue can be found at ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Dr. Nils Melzer, Legal Adviser, ICRC, Geneva, May 2009); available from <https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>.

76. Attacking persons who are recognized as hors de combat is prohibited. A person hors de combat is anyone who is in the power of an adverse party; anyone who is defenceless because of unconsciousness, shipwreck, wounds or sickness; or anyone who clearly expresses an intention to surrender; provided he or she abstains from any hostile act and does not attempt to escape. ICRC, *supra* note 71, Customary IHL, Rule 47. Attacks against Persons Hors de Combat.

77. ICRC, *supra* note 71, Customary IHL, Rule 33. Personnel and Objects Involved in a Peacekeeping Mission.

78. The Statute of the International Court of Justice describes customary international law as "a general practice accepted as law". It is generally agreed that the existence of a rule of customary international law requires the presence of two elements, namely state practice (*usus*) and a belief that such practice is required, prohibited or allowed, depending on the nature of the rule, as a matter of law (*opinio juris sive necessitatis*). Following this principle, the ICRC deems any of the rules regarding protected persons and objects mentioned as customary law. Jean-Marie Henckaerts, 'Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict', *International Review of the Red Cross*, vol. 87, no. 857, pp. 175–212, 2005.

79. International humanitarian law has its origins in the customary practices of armies as they developed over the ages and on all continents. The "laws and customs of war", as this branch of international law has traditionally been called, was not applied by all armies, and not necessarily vis-à-vis all enemies, nor were all the rules the same. However, the pattern that could typically be found was restraint of behaviour vis-à-vis combatants and civilians, primarily based on the concept of the soldier's honour. The content of the rules generally included the prohibition of behaviour that was considered unnecessarily cruel or dishonourable, and was not only developed by the armies themselves, but was also influenced by the writings of religious leaders. ICRC, *supra* note 71, Customary IHL, Introduction.

and national emblems of parties to the conflict. The vicinity of combat equipment, such as military vehicles or weapons of parties to the conflict may support the identification process. However, if positive identification is not possible, the AWS must not rely on this visual type of identification only and has to further assess the individual's behaviour and actions in order to determine if they qualify for direct participation in hostilities. With regard to the positive identification of a lawful target IHL states that 'in case of doubt whether a person is a civilian, that person shall be considered to be a civilian.'<sup>80</sup>

### **Internationally Established Distinctive Emblems.**

The AWS must be capable of identifying protected persons such as medical and religious personnel, humanitarian relief personnel and objects, peacekeeping forces, and journalists.<sup>81</sup> These groups typically wear either the ICRC's distinctive emblems<sup>82</sup> or the United Nations' light blue colours.<sup>83</sup> For journalists or war correspondents there is no formally agreed protective emblem yet, but a dedicated distinctive emblem showing 'Press' in black capital letters on a circular orange background may be incorporated into IHL in the near future.<sup>84</sup> If in doubt whether a person is showing a distinctive emblem or not, the AWS must treat them as protected persons, unless their behaviour qualifies them for direct participation in hostilities.

**Direct Participation in Hostilities.** The AWS must be capable of recognizing and analysing a person's behaviour and determining if it qualifies as direct partici-

pation in hostilities. Obviously, a person actively takes part in hostilities if he/she attacks the AWS or the forces it belongs to. In doing so, the person loses his/her protection against attack and becomes a lawful target in combat, regardless of his/her previous status. However, whether a person is directly participating in hostilities or not is not always that clear, especially in a non-international armed conflict. The ICRC issued an 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' addressing the complexity of that issue.<sup>85</sup> Hence, if the AWS cannot clearly attribute a person's behaviour to direct participation in hostilities, it must refrain from attack. This is also true in cases of persons hors de combat and persons who have surrendered or aborted their offensive actions.

### **5.2.3 Assessment**

In theory, the requirements to comply with the principle of distinction can be formulated quite easily. In practice, and depending on the environment, these requirement can be quite hard to codify into a software application.

Current AWS such as Phalanx<sup>86</sup> or Skyshield<sup>87</sup> have a very narrow and defensive use-case in which it is absolutely certain that hostile adversary action is present, because rockets, grenades or projectiles moving on a ballistic trajectory towards their protected area can be clearly identified. To prevent civilian casualties, the physical engagement zone of

80. The issue of how to classify a person in case of doubt is complex and difficult. In the case of international armed conflicts, Additional Protocol I has sought to resolve this issue by stating that "in case of doubt whether a person is a civilian, that person shall be considered to be a civilian". [...] In the light of the foregoing, it is fair to conclude that when there is a situation of doubt, a careful assessment has to be made under the conditions and restraints governing a particular situation as to whether there are sufficient indications to warrant an attack. One cannot automatically attack anyone who might appear dubious. ICRC, *supra* note 71, Customary IHL, Rule 6. Civilians' Loss of Protection from Attack.

81. ICRC, *supra* note 71, Customary IHL, Rules 25, 27, 31–35, 47, 59.

82. The use and misuse of the Red Cross, Red Crescent and Red Crystal emblems is clearly defined in law. In armed conflicts, the protective emblem must be in red on a white background with no additions. It must be clearly displayed in a large format on protected buildings, such as hospitals, and vehicles. Emblems on armbands and vests for protected personnel must also be clear and stand alone. A deliberate attack on a person, equipment or a building carrying a protective emblem is a war crime under international law. ICRC, *The Emblems* (accessed 10 Oct. 2016); available from <https://www.icrc.org/eng/war-and-law/emblem/overview-emblem.htm>.

83. Article 3(1) of the 'Convention on the Safety of United Nations and Associated Personnel' states that 'The military and police components of a United Nations operation and their vehicles, vessels and aircraft shall bear distinctive identification. Other personnel, vehicles, vessels and aircraft involved in the United Nations operation shall be appropriately identified unless otherwise decided by the Secretary-General of the United Nations'. United Nations Office of Legal Affairs Codification Division, *Convention on the Safety of United Nations and Associated Personnel* (accessed 10 Oct. 2016); available from <http://www.un.org/law/cod/safety.htm>.

84. Emily Crawford and Kayt Davies, 'The International Protection of Journalists in Times of Armed Conflict: The Campaign for a Press Emblem', *Wisconsin International Law Journal* (2014); available from [http://hosted.law.wisc.edu/wordpress/wilj/files/2015/03/Crawford\\_final.pdf](http://hosted.law.wisc.edu/wordpress/wilj/files/2015/03/Crawford_final.pdf).

85. ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Dr. Nils Melzer, Legal Adviser, ICRC, Geneva, May 2009); available from <https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>.

86. Phalanx, *supra* note 2.

87. Skyshield, *supra* note 1.

the AWS is strictly limited to a pre-defined sector and it is operating under the rights of self-defence, hence superseding the principle of distinction and avoiding the aforementioned legal and technical challenges.

In an offensive role, the application of the principle of distinction may be more difficult, but still reliably feasible, to ascertain. Specifically, distinction may be attained if the use-case can be narrowed down enough to match the current capabilities of sensors and software algorithms and where the presence of civilian population and objects can be ruled out to the maximum extent possible. One example could be an air-to-air combat scenario where the enemy combat aircraft is clearly identifiable and its actions can be clearly attributed to hostile intent. Advancing main battle tanks towards friendly troops in a symmetric

conflict scenario is also clearly a hostile act and confers combatant status. However, in this case a civilian population may still be present and need to be protected, potentially making this generic scenario too challenging for a software algorithm to cope with.

Air-to-ground combat and precision strike missions by AWS are likely to require the most advanced technology, as they are typically conducted in an environment with a lot of uncertainties regarding the behaviour and activities of the target itself. An AWS will have to prove that it can reliably distinguish combatants from civilians and other protected personnel to meet the requirement for positive identification of a lawful target. However, even humans are not without error and it has to be further assessed how much, if any, probability of error would also be acceptable for an AWS.





**Figure 9 – Wesel, Germany, was intensely bombed and 97% destroyed in February and March 1945.**

### 5.3 Principle of Proportionality

***‘[...] an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated’***

The principle of proportionality in attack is codified in Article 51(5)(b) and repeated in Article 57 of AP I as well as in Protocol II and Amended Protocol II to the Convention on Certain Conventional Weapons (CCW). As with the principle of distinction, the principle of proportionality was first formally codified in treaty law and not every state is a party to the respective protocol. However, numerous states, including the United States, have adopted legislation making it an offence to carry out an attack which violates the principle of

proportionality. In addition, under the Statute of the ICC, ‘intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects [...] which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated’ constitutes a war crime in international armed conflicts.<sup>88</sup> Therefore, the ICRC also characterizes the principle of proportionality as a norm of international customary law.<sup>89</sup> Conclusively, AWS have to meet the requirements of the principle of proportionality to be compliant with international law.

#### 5.3.1 Requirements for Adhering to the Principle of Proportionality

International law dictates that the use of military force should always be proportionate to the anticipated mili-

88. Rome Statute, *supra* note 73, Article 8(2)(b)(iv).

89. The principle of proportionality in attack is codified in Article 51(5)(b) of Additional Protocol I, and repeated in Article 57. At the Diplomatic Conference leading to the adoption of the Additional Protocols, Mexico stated that Article 51 was so essential that it ‘cannot be the subject of any reservations whatsoever since these would be inconsistent with the aim and purpose of Protocol I and undermine its basis.’ Also at the Diplomatic Conference, several states expressed the view that the principle of proportionality contained a danger for the protection of the civilian population but did not indicate an alternative solution to deal with the issue of incidental damage from attacks on lawful targets. The United Kingdom stated that Article 51(5)(b) was ‘a useful codification of a concept that was rapidly becoming accepted by all states as an important principle of international law relating to armed conflict.’ The principle of proportionality in attack is also contained in Protocol II and Amended Protocol II to the Convention on Certain Conventional Weapons. ICRC, *supra* note 71, Customary IHL, Rule 14. Proportionality in Attack.

tary advantage.<sup>90</sup> This principle evolved alongside the technological capabilities of the time. For example, carpet bombing of cities inhabited by civilians was a common military practice in World War II, which would be considered completely disproportionate today.<sup>91</sup> Modern Laser Guided Bombs (LGB) are capable of hitting their targets with so called 'surgical' precision whereas advanced software is used in preparation of the attack to calculate the weapon's blast and fragmentation radius and anticipated collateral damage. Especially for the latter, it can be argued that an AWS could potentially apply military force more proportionately than humans because they are capable of calculating highly complex weapon effects in an instant and therefore reducing the probability, type and severity of collateral damage. However, this requires an AWS which has a sophisticated set of capabilities as outlined below.

**Real-time Situational Awareness.** To accurately calculate the effects of a military weapon and to assess whether its use is proportionate, the AWS must have sufficient situational awareness of the target area and its environment. Depending on the weapon's capabilities, the area where situational awareness is required may be quite large. The more range, time to impact and effect radius, the more area has to be covered to reliably react on uncertain events, e.g., civilians entering the predicted target zone. This area has to be surveyed and assessed – as a human would do – continuously and in real-time. If the situational picture is unclear or intolerable collateral damage is anticipated, weapon employment has to be suspended or aborted. The capability to conduct these calculations is already possible and available in such applications as weaponeering and collateral damage estimation software tools for target development.<sup>92</sup> However, an AWS' sensor suite would have to provide these tools real-time data to allow for appropriate calculations which, in turn, would have to satisfy the principles of 'Distinction' and 'Anticipation' as outlined below.

**Distinction.** The AWS could only provide a clear situational picture if it is capable of reliably identifying and distinguishing every person and object in the respective area. Ultimately, this refers to the application of the principle of distinction and entails all the legal and technical challenges as discussed in Section 5.2.2.

**Anticipation.** In addition to the ability to reliably distinguish every person and object, the AWS must also be capable of anticipating their movements and behaviours within a certain timeframe, which could be defined by the range and time to impact of the respective weapon. Modern fire control software of main battle tanks or artillery guns is already capable of calculating an enemy vessel's speed and adjusting the aim point accordingly, assuming their direction and speed to be constant. In the same way, an AWS could sufficiently anticipate the location of every person and object at the time of weapon impact, potentially better than any human would do.

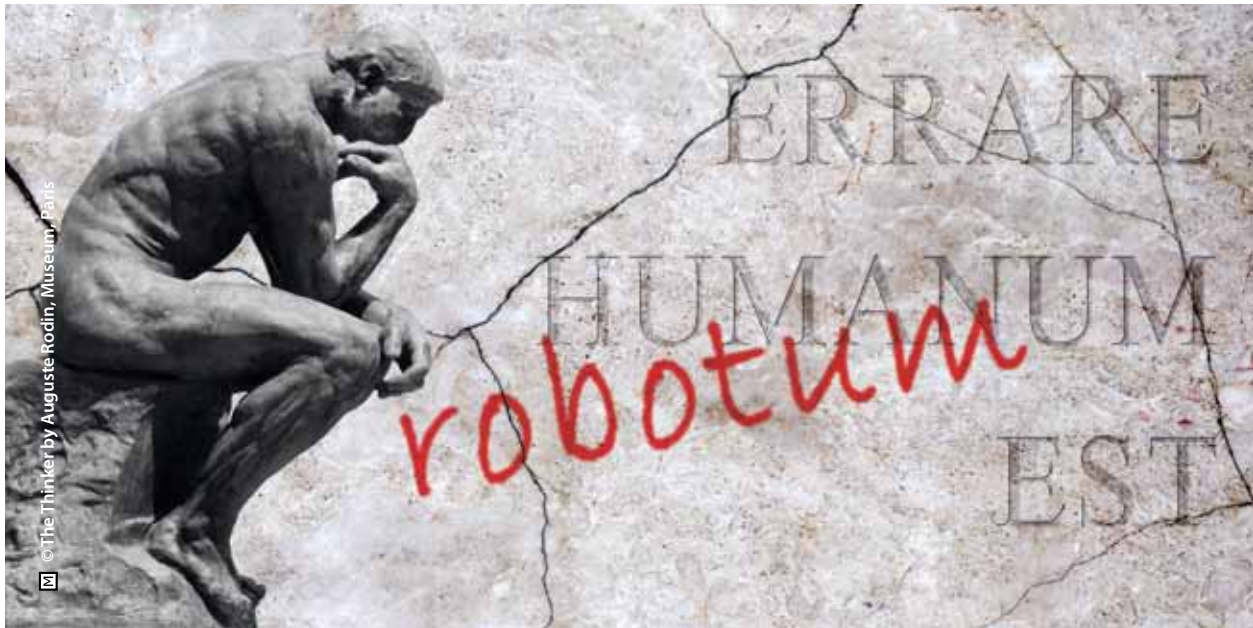
### 5.3.2 Assessment

Assuming that appropriate and timely data is given, any computer, and hence any AWS, is capable of calculating weapon effects such as blast and fragmentation potentially more quickly and precisely than any human. It can also be anticipated that an AWS would be superior to the human in processing and predicting movements of persons and objects in relation to the weapon's effect radius and estimating collateral damage. The sophisticated sensors required to provide the respective situational awareness may not be as challenging to develop, or may be already in service. However, adhering to the principle of proportionality is completely dependent on reliably incorporating the principle of distinction.

90. The principle of proportionality in attack is codified in Article 51(5)(b) of Additional Protocol I, and repeated in Article 57. The principle of proportionality in attack is also contained in Protocol II and Amended Protocol II to the Convention on Certain Conventional Weapons. In addition, under the Statute of the International Criminal Court, 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects [...] which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated' constitutes a war crime in international armed conflicts. ICRC, *supra* note 71, Customary IHL, Rule 14. Proportionality in Attack.

91. Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Routledge, Taylor & Francis Group, 17. Jul. 2009)

92. According to U.S. targeting doctrine, there are numerous systems in service, e.g., the Joint Weaponeering System which provides the standard automated methodology for estimating the employment effectiveness of kinetic weapons, or the Digital Precision Strike Suite Collateral Damage Estimation tool for collateral damage analysis of kinetic weapons. Curtis E. Lemay Center for Doctrine Development and Education, Annex 3-60 Targeting - Dynamic Targeting and the Tasking Process (accessed 11 Oct. 2016); available from <https://www.doctrine.af.mil/download.jsp?filename=3-60-D17-Target-Dynamic-Task.pdf>.



## 5.4 Principle of Precaution

The principle of precautions in attack was first set out in the 1907 Hague Convention (IX), which provides that 'if for military reasons immediate action is necessary [...] the commander shall take all due measures in order that the town may suffer as little harm as possible.' It is now more clearly codified in Article 57(1) of Additional Protocol I, which states that

***'In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.'***

It further dictates that all feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects.<sup>93</sup> State practice including that of states not, or not at the time, party to AP I establishes this principle as a norm of customary international law applicable in both international and non-international

armed conflicts.<sup>94</sup> Conclusively, AWS have to meet the requirements of the principle of precaution to be compliant with international law.

### 5.4.1 Requirements for Adhering to the Principle of Precaution

The obligation of states to take all feasible precautions to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects<sup>95</sup> inherently requires respect for the principles of distinction and proportionality. Therefore the principle of precaution can be seen as an overarching rule, once more emphasizing the importance of protecting civilians from the effects of war.<sup>96</sup>

**Precautions while Planning, Deciding on or Conducting an Attack.** In detail, states are obliged to take these precautions in advance while planning or deciding upon an attack, as well as during the immediate conduct of the attack if unforeseen events make it be-

93. AP I, supra note 54, Article 57(2)(a)(ii).

94. The principle of precautions in attack was first set out in Article 2(3) of the 1907 Hague Convention (IX), which provides that if for military reasons immediate action against naval or military objectives located within an undefended town or port is necessary, and no delay can be allowed the enemy, the commander of a naval force "shall take all due measures in order that the town may suffer as little harm as possible". It is now more clearly codified in Article 57(1) of Additional Protocol I, to which no reservations have been made. ICRC, supra note 71, Customary IHL, Rule 15. Precautions in Attack.

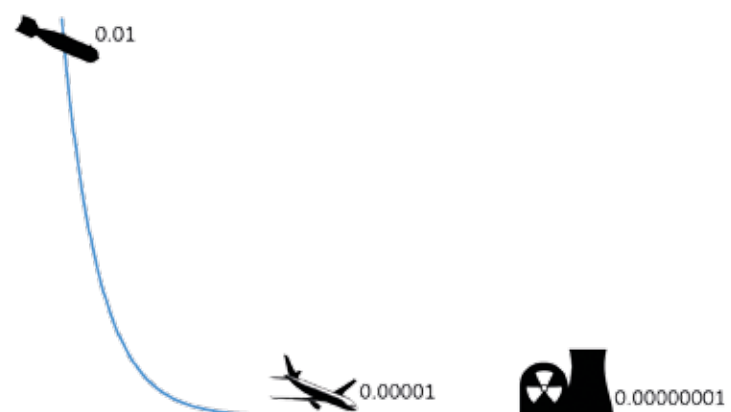
95. ICRC, supra note 71, Customary IHL, Rule 15. Precautions in Attack.

96. The principles of proportionality and precaution follow a different approach to protect civilians during armed conflicts. The principle of proportionality reaches this aim through prohibitions while the principle of precaution does the same but through obligations.



come apparent that civilian life or property will be affected.<sup>97</sup> An AWS capable of processing higher level intent and generating its own mission tasks to achieve its specified objective must incorporate the principle of precaution during this ‘planning’ stage; i.e., the AWS must verify that the object to be attacked is a lawful military target and select the proper means and methods of attack to avoid incidental loss or injury of civilians and civilian objects. To adhere to this principle during the immediate conduct of an attack, the AWS has to meet the requirements of situational awareness, distinction and anticipation as outlined in Section 5.3.1.

**Precautions while Developing and Testing AWS.** Deriving from the aforementioned requirements and from the obligation to review new weapons according to Article 36 of AP I, the principle of precaution should be respected far in advance of employing an AWS, potentially during the initial development of the system itself. Any type of weapon, to include AWS, has to demonstrate if it can reliably stay within the limits of an acceptable failure rate as no current technology is perfectly free of errors. For example, the US Congress defined the acceptable failure rate for their cluster munitions as less than one percent.<sup>98</sup> The recent general aviation accident rates in the United States are only a fraction compared to that<sup>99</sup> and even nuclear power plants cannot guarantee 100 percent reliability.<sup>100</sup> It is doubtful that any type of future technology would ever accomplish an error level of zero, which is also true for any AWS. Therefore, an acceptable failure rate for AWS has to be determined.



**Figure 10 – Failure Rates in Modern Technology.**<sup>98,99,100</sup>

## 5.4.2 Assessment

The more complex a system is the more probable errors will occur.<sup>101,102</sup> It can be anticipated that AWS will never be perfectly free of errors. So the question is therefore ‘how good is good enough?’ One approach to answer this question could be a comparison with human errors in a comparable combat scenario. If an AWS could narrow down its probability for errors to that of the human, this may be considered ‘good enough.’

Finally, a military commander having AWS under his command must have sufficient trust in the AWS to reasonably predict its behaviour and effects on the battlefield, comparable to the confidence in his human soldiers after they passed a combat readiness test. Weapon development and experimentation should therefore provide documented evidence to support commanders with guidance for responsibly employing AWS.

97. The obligation to take all ‘feasible’ precautions has been interpreted by many states as being limited to those precautions which are practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations. Protocols II and III and Amended Protocol II to the Convention on Certain Conventional Weapons define feasible precautions in the same terms. Numerous states have expressed the view that military commanders and others responsible for planning, deciding upon or executing attacks necessarily have to reach decisions on the basis of their assessment of the information from all sources which is available to them at the relevant time. At the same time, many military manuals stress that the commander must obtain the best possible intelligence, including information on concentrations of civilian persons, important civilian objects, specifically protected objects, the natural environment and the civilian environment of military objectives. ICRC, *supra* note 71, Customary IHL, Rule 15. Precautions in Attack.

98. The central directive in the Pentagon’s new policy is the unwaiverable requirement that cluster munitions used after 2018 must leave less than 1% of unexploded submunitions on the battlefield. Prior to 2018, U.S. use of cluster munitions with a greater than 1% unexploded ordnance rate must be approved by Combatant Commanders. Congressional Research Service (CRS), *Cluster Munitions: Background and Issues for Congress* (Andrew Feickert, Paul K. Kerr, CRS, 2014); available from <https://www.fas.org/sgp/crs/weapons/RS22907.pdf>.

99. In 2012, the fatal accident rate was 1.09 fatal accidents per 100,000 hours flown, [...]. In 2011, the fatal accident rate was 1.12 fatal accidents per 100,000 hours flown, [...]. In 2010, the fatal accident rate was 1.10 fatal accidents per 100,000 hours flown, [...]. Federal Aviation Administration, *Fact Sheet – General Aviation Safety* (accessed 11 Oct. 2016); available from [http://www.faa.gov/news/fact\\_sheets/news\\_story.cfm?newsId=16774](http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=16774).

100. There have been three major reactor accidents in the history of civil nuclear power – Three Mile Island, Chernobyl and Fukushima. These are the only major accidents to have occurred in over 16,000 cumulative reactor-years of commercial nuclear power operation in 33 countries. World Nuclear Association, *Safety of Nuclear Power Reactors* (accessed 11 Oct. 2016); available from <http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx>.

101. There have been numerous cases in recent years where software malfunctions caused substantial damage, financially as well as physically, e.g., the divert of an Air India Boeing 787 in Feb. 2014, the recall of 2.6 million Toyota Prius vehicles in Feb. and Jul. 2014, the outage of emergency services in Washington and 6 other US states in Apr. 2014, the collapse of the UK’s National Air Traffic Services on 12 Dec. 2014, or the outage of stock exchange services in Bloomberg’s London Office in Apr. 2015. An overview of the most severe software failures is available from <http://www.computerworlduk.com/galleries/infrastructure/top-10-software-failures-of-2014-3599618>.

102. Amruta Kudale, *Case study: The Ariane 5 explosion due to software error* (accessed 11 Oct. 2016); available from [https://www.academia.edu/11818474/Case\\_study\\_on\\_Ariane\\_5\\_launch\\_failure](https://www.academia.edu/11818474/Case_study_on_Ariane_5_launch_failure).



## CHAPTER VI

### Responsibilities with Regard to AWS

The higher the degree of automation, and the lower the level of human interaction, the more the question arises as to who is actually responsible for actions conducted by an AWS. This question is most relevant if lethal capabilities cause civilian harm, be it incidentally or intentionally. Who will be held liable for a criminal act if IHL has been violated and who will have to compensate for the damage caused? Chapter 3 recommended four different levels of automation, i.e., manually controlled, automated, autonomic and autonomous. Will responsibility change if predictability of AWS behaviour is limited with higher levels of automation? This chapter discusses the potential individual responsibilities if an AWS is employed.

### 6.1 Responsibility of the Automated Weapon System

Holding the AWS itself accountable for its actions would be obviously nonsensical given the current stage of technology, nor is there any legal framework which would allow for that. In current law, any crime consists of three elements, an act, a mental state and a causal link between the two first ones.<sup>103</sup> So if an AWS would violate IHL (the act) it currently lacks the mental state to make these actions prosecutable crimes.

However, if an AWS ever achieves this mental state as a prerequisite for true autonomy, robots might be given a legal personality. In fact, non-human entities like corporations are already attributed personhood and can be made legally responsible. The European Parliament's Committee on Legal Affairs recently stated in a draft report that 'it becomes more and more

<sup>103.</sup> In general, every crime involves three elements: first, the act or conduct ('actus reus'); second, the individual's mental state at the time of the act ('mens rea'); and third, the causal link between the act and the offense. In a criminal prosecution, the government has the burden of proof to establish every element of a crime beyond a reasonable doubt; and third, the individual's conduct must be the cause of the crime. Cornell University Law School, Criminal Law (accessed 11 Oct. 2016); available from [https://www.law.cornell.edu/wex/criminal\\_law](https://www.law.cornell.edu/wex/criminal_law).

urgent to address the fundamental question of whether robots should possess a legal status' and 'if they should be regarded as natural persons, legal persons, animals or objects [...] regarding the attribution of rights and duties, including liability for damage.'<sup>104</sup> However, it is questionable if machines could ever be subject to punishment, imprisonment or other legal means of accountability.

But even if we consider this very hypothetical possibility of granting legal personality and legal accountability to fully autonomous weapon systems in the distant future, it would not change a commander's responsibility for deploying them, as he would be held responsible for actions conducted by his human subordinates in the same manner.

## 6.2 Responsibility of the Military Commander

Military commanders have the responsibility to ensure that members of the armed forces under their command are aware of their obligations under IHL.<sup>105</sup> They are also obliged to prevent and, where necessary, to take disciplinary or judicial action, if they are aware that subordinates or other persons under their control are going to commit or have committed a breach of IHL.<sup>106</sup> Military commanders are, of course, also responsible for unlawful orders given to their subordinates.<sup>107</sup>

This responsibility does not change when authorizing the use of an AWS. Section 5.4 outlined the issue of reliability and trust in the AWS as a prerequisite for its reasonable deployment. This has also a direct impact on the commander's responsibility. If a commander was aware in advance of the potential for unlawful actions by an AWS and still wilfully deployed it, he would likely be held liable. In contrast, if weapon experimen-

tation and testing provided sufficient (documented) evidence that an AWS can be trusted to respect IHL, a commander would likely not be accountable and the liability of either the developer or manufacturer has to be taken into account.

## 6.3 Responsibility of the Operator

Depending on the level of human interaction, if still required, the individual responsibility of the system's operator may vary. For example, at the current stage of aviation technology pilots already rely on a high degree of automation and there is usually sufficient evidence that these automated functions are reliable and can be trusted. If an accident can be solely attributed to a malfunction of a trusted automated system and the aircrew cannot affect the error chain, the pilot would not be liable. If the automated system indicated a problem before take-off and the pilot disregarded it, or if he incorrectly responded to the error during flight, he would be responsible. The same principle can be applied to the use of AWS.

However, some already fielded AWS such as Phalanx or Skyshield can operate in a mode where the human operator has only a short timeframe to stop the system from automatically releasing its weapons if a potential threat has been detected. Attributing liability to the operator is doubtful if the timeframe between alert and weapon release is not sufficient to manually verify if the detected threat is real and if engagement of the computed target would be lawful under IHL.

## 6.4 Responsibility of the Manufacturer

Civil law in most states holds corporations legally responsible if their products cause harm through poor design or substandard manufacturing. In the military

104. The European Parliament calls on the Commission, [...] to explore the implications of all possible legal solutions, such as creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations, including that of making good any damage they may cause, and applying electronic personality to cases where robots make smart autonomous decisions or otherwise interact with third parties independently. European Parliament, Committee on Legal Affairs, Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (accessed 11 Oct. 2016); available from <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>.

105. AP I, supra note 54, Article 87(2).

106. Rome Statute, supra note 73, Article 28(a); AP I, supra note 54, Article 86, 87(1).

107. Article 49 of the 1949 Geneva Convention I, Article 50 of the 1949 Geneva Convention II, Article 129 of the 1949 Geneva Convention III and Article 146 of the 1949 Geneva Convention IV, Article 28 of the 1954 Hague Convention for the Protection of Cultural Property, Article 25(3) of the 1998 ICC Statute. Article 15 of the 1999 Second Protocol to the Hague Convention for the Protection of Cultural Property.

domain there is now also a rising tendency to sue manufacturers if products do not perform as promised or if deadlines for delivery have passed. It is probable that any undocumented behaviour of the AWS causing unexpected harm could be interpreted as poor design and may be attributed to the manufacturer, resulting in some form of punishment. This could mean cancellation of the contract, penalties or compensation for damages. For severe breaches of the law, managers or engineers could individually be held responsible for their products if they knew about their limitations and potential errors and did not inform the user.

In contrast, if the company meets all the given quality standards, typically defined by the military within the arms acquisition process, they are not to be held liable for any outcome of an AWS operation.

## 6.5 Responsibility of the Programmer

Software has a key role not only while operating AWS but already in many of today's automated and autonomous systems. Usually, the source code of the software used is not displayed to the user, i.e., with regard to AWS, the military commander and the operator. But even if this were the case they could not be expected to verify the code as they're simply not educated to do so. Furthermore, source code is only used during software development and the final application is usually compiled into machine code, which even experts cannot easily translate back into a human readable format.

Hence, the programmer may be predominantly attributed responsibility for the AWS' behaviour and actions. However, modern software applications show clearly that the more complex the program the higher

the potential of software 'bugs.' For example, the software for the F-35 fighter jet comprises roughly 24 million lines of source code (cf. Figure 11) whereas the most recent Microsoft Windows operating system contains approximately 50-60 million, forcing the company to regularly release bug fixes and security updates. Such large software undertakings, and this would be especially true for any AWS, are typically developed and modified by a large team of programmers and each individual has only limited understanding of the software in its entirety. Furthermore, it is doubtful if the individual programmer could predict in detail any potential interaction between his portion of the source code and the rest of the software. So, holding an individual person liable for software weaknesses is probably not feasible unless intentionally erroneous programming may be evidenced.

## 6.6 Responsibility of the Deploying Nation

According to the system of international law, states are held responsible for wrongful acts with regard to their foreign relations and their obligations under IHL and the Charter of the United Nations. Like any other obligation under international law, this is also applicable to any AWS operated by a state's armed forces. Furthermore, a state would also be held responsible if it uses an AWS that has not, or has inadequately, been tested or reviewed prior to deployment and, in consequence, committed a breach of IHL.

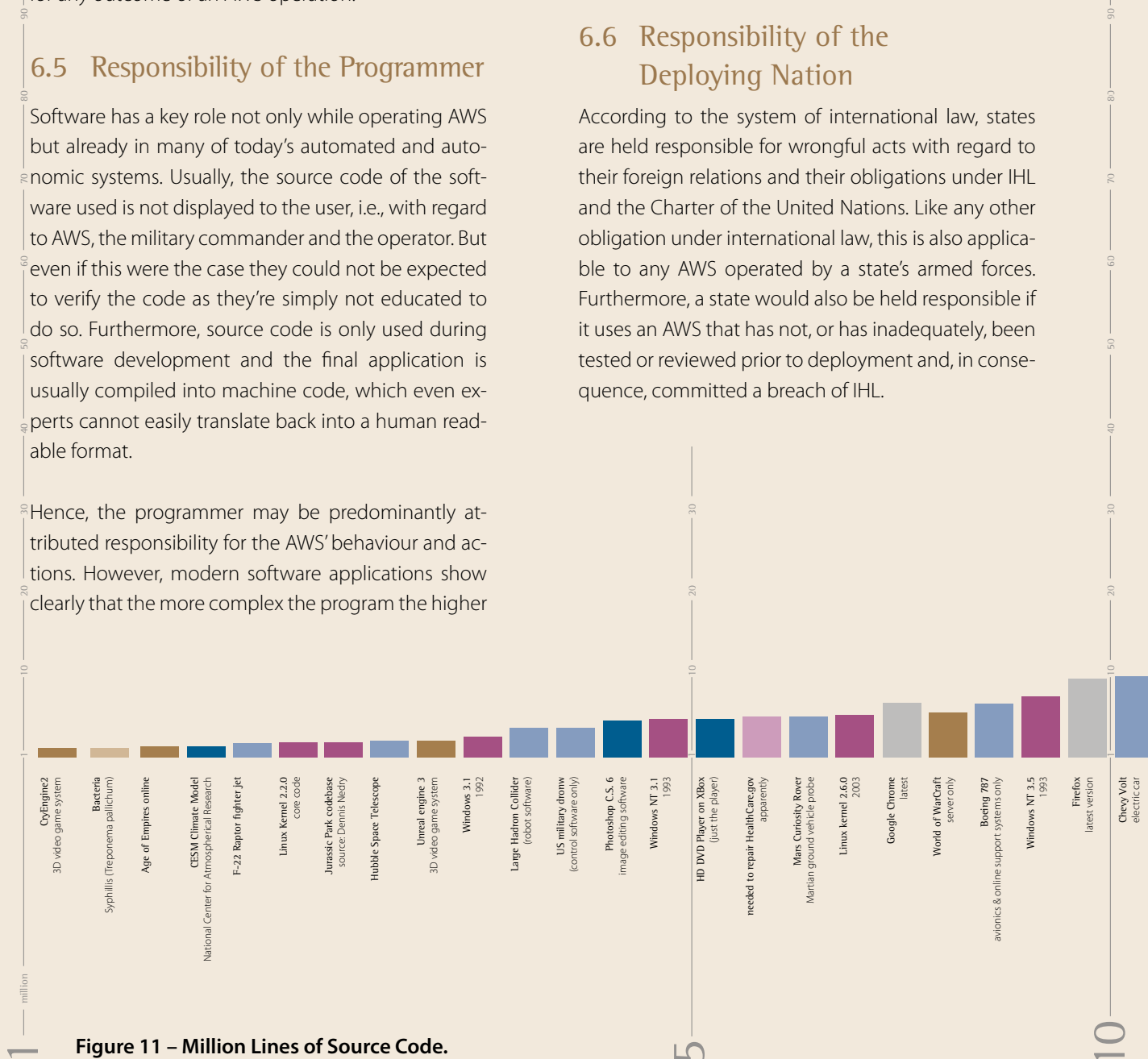


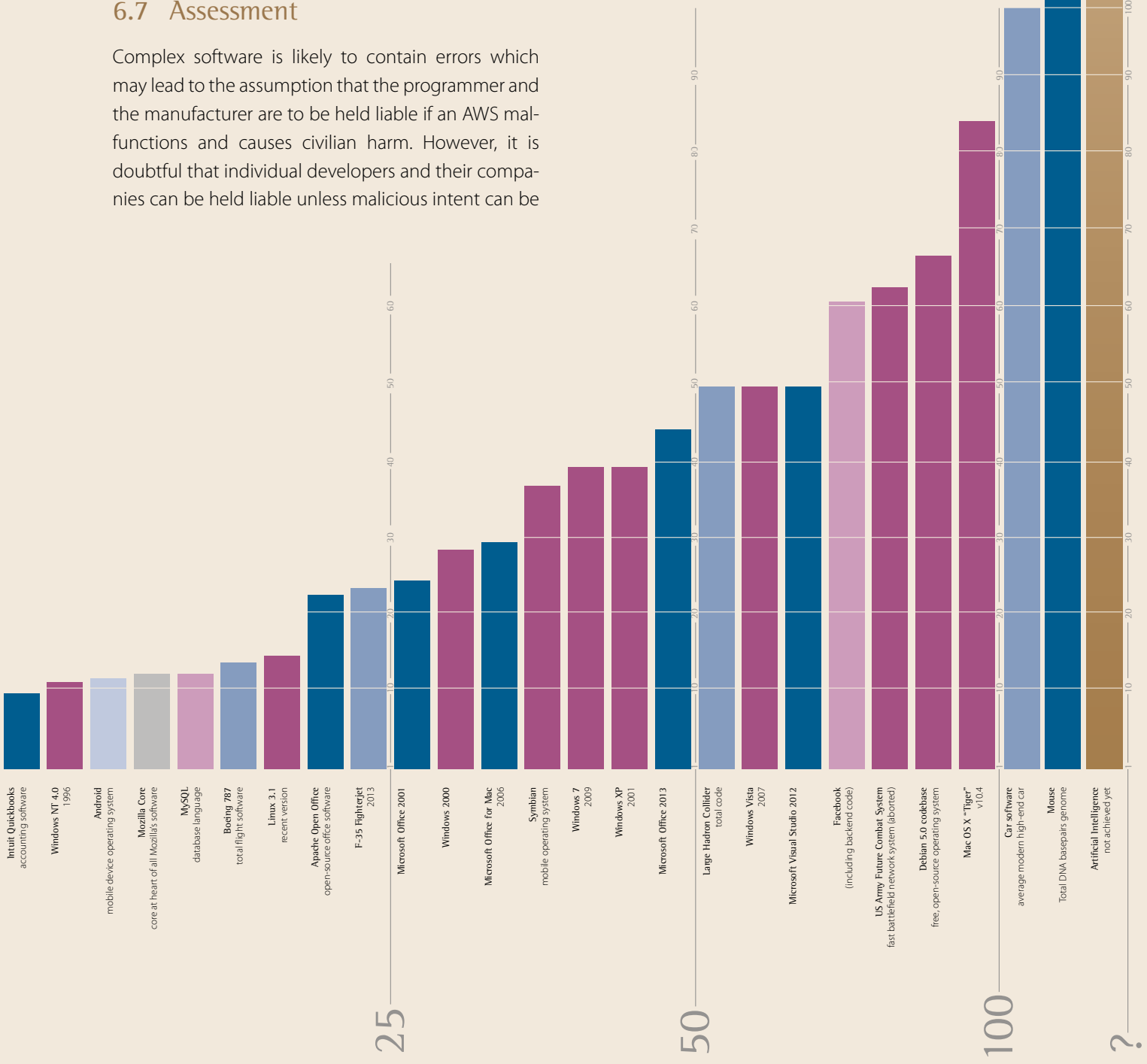
Figure 11 – Million Lines of Source Code.

To hold a state accountable for violations of international law, it is sufficient that the breach can be objectively attributed to the state, i.e., it was committed by a weapon system operated by the state's armed forces. The state in question would be responsible unless it could invoke 'force majeure.' However, the threshold of force majeure is very high. An ordinary malfunction of an AWS would not suffice, although a completely unexpected incident against which no reasonable precautions could have been taken would qualify. Regardless, the burden of proof rests with the state which again emphasizes the need for appropriate testing and documentation of the AWS' performance before deploying it.

### 6.7 Assessment

Complex software is likely to contain errors which may lead to the assumption that the programmer and the manufacturer are to be held liable if an AWS malfunctions and causes civilian harm. However, it is doubtful that individual developers and their companies can be held liable unless malicious intent can be

proven, given they comply with proper manufacturing standards. Similarly, military commanders and system operators could also only be held liable if they act recklessly or intentionally against the given Rules of Engagement, to include IHL. So in the end, the overall responsibility for the AWS' actions lies always with the state who employs it.







## CHAPTER VII

### Ethical Issues

#### 7.1 The Public Perception of an Autonomous Weapon

*'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.'*

The above quote was taken from the movie 'Terminator 2 – Judgment Day' which basically shaped the predominant public's vision of an autonomous robot as

that of a self-thinking killing machine. This common understanding mainly drives the tabloid press' discussion, and, as a result, the public willingness to accept AWS is very low. The respective main arguments are typically that the decision on life and death must not be delegated to a machine, and that human judgment is essential in order to make such decisions, and that AWS would be out of human control.

#### 7.2 Arguments Against AWS

**Decision on Life and Death.** The first and foremost argument is that the decision on the life and death of humans must not be delegated to a machine and to do so is considered ethically unacceptable. This argument is supported by the fact that machines do not live and die, thus cannot show respect to the value of human life.<sup>108</sup>

**Necessity for Human Judgement.** The second argument is that human judgment is essential in order to as-

<sup>108</sup>. Krishnan, *supra* note 91.

sess the fundamental principles of proportionality, distinction and precautions in attack as outlined in Chapter 5. It is questionable if legal assessments could be codified into a machine, enabling it to reliably distinguish between lawful and unlawful targets. This argument is supported by the fact that machines are currently incapable of executing legal judgements in complex and cluttered environments and are therefore indiscriminate.<sup>109, 110</sup>

**Necessity for Human Control.** The third argument is that a fully autonomous system would be inherently unpredictable and it would be reckless to operate such a system that is 'out of control.' This argument is supported by the definition of 'autonomy' in its philosophical sense as outlined in Section 3.2. However, this argument may be challenged by the fact that unpredictability is also present in human behaviour.

### 7.3 Arguments in Favour of AWS

In contrast to the aforementioned arguments, there are also potential benefits when employing AWS, once the required level of technology has been achieved.

**Immunity to Emotions.** Emotions play a critical role in human reasoning and decision-making and therefore decisions taken by humans are qualitatively different than those taken by a machine. AWS will be resistant to adverse psychological effects, like fear, anger or revenge that underlie the perpetration of some unlawful acts by human actors.<sup>111</sup> This may be a significant advantage over human combatants, potentially making the conduct of hostilities more humane by respecting legal rules better than humans. However, the absence of emotions may also prevent acts of compassion and mercy.<sup>112</sup>

**No Instinct of Self-preservation.** If calculated in plain numbers, the preservation of a soldier's own life may cause disproportionate collateral damage. While

the soldier might be forced to make a lethal defensive decision, an AWS may not prioritize its own existence, could assess the situation completely dispassionately and sacrifice itself if necessary.<sup>113</sup>

### 7.4 Asimov's Three Laws of Robotics

The Three Laws of Robotics are a set of rules devised by the science fiction author Isaac Asimov in his 1942 short story 'Runaround'. In his fictional universe, the following laws were embedded into the software that governs robot behaviour and the rules could not be bypassed, over-written, or revised.

**1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.**

**2. A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.**

**3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.**

Actually, these Laws were meant as a literary device. But as late as 1981, Asimov himself believed that they could actually work and he stated that his three Laws are the only way in which rational human beings can deal with robots.<sup>114</sup> In fact, the applicability and necessity of Asimov's Laws is discussed within the robot and AI community quite controversially.

From an ethical as well as a legal perspective, Asimov's Laws look very appealing as they seem to provide the solution for preventing robots from getting out of human control. However, it is obvious that Asimov's Laws are not applicable in a military context as they inherently forbid a robot to harm any human being. To resolve this contradiction, the First Law could

109. Krishnan, *supra* note 91.

110. European Parliament, Directorate-General for External Policies of the Union, Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare (Dr. Nils Melzer, 2013), p. 28.

111. Ronald Arkin, *Governing Lethal Behaviour in Autonomous Robots* (Chapman & Hall/CRC, Boca Raton, 2009).

112. Krishnan, *supra* note 91.

113. P. Lin et al., *Autonomous Military Robotics: Risks, Ethics and Design* (US Office of Naval Research, 2008).

114. Isaac Asimov, 'The Three Laws', *Computel*, Issue 18 (1981): 18; available from . [https://archive.org/stream/1981-11-compute-magazine/Compute\\_Issue\\_018\\_1981\\_Nov/page/n19/mode/2up](https://archive.org/stream/1981-11-compute-magazine/Compute_Issue_018_1981_Nov/page/n19/mode/2up).

be amended to also recognize the lawfulness of potentially harmful actions to human beings. After this slight change, the First Law would read as follows:

*A robot may not **unlawfully** injure a human being or, through inaction, allow a human being to come to harm **unlawfully**.*

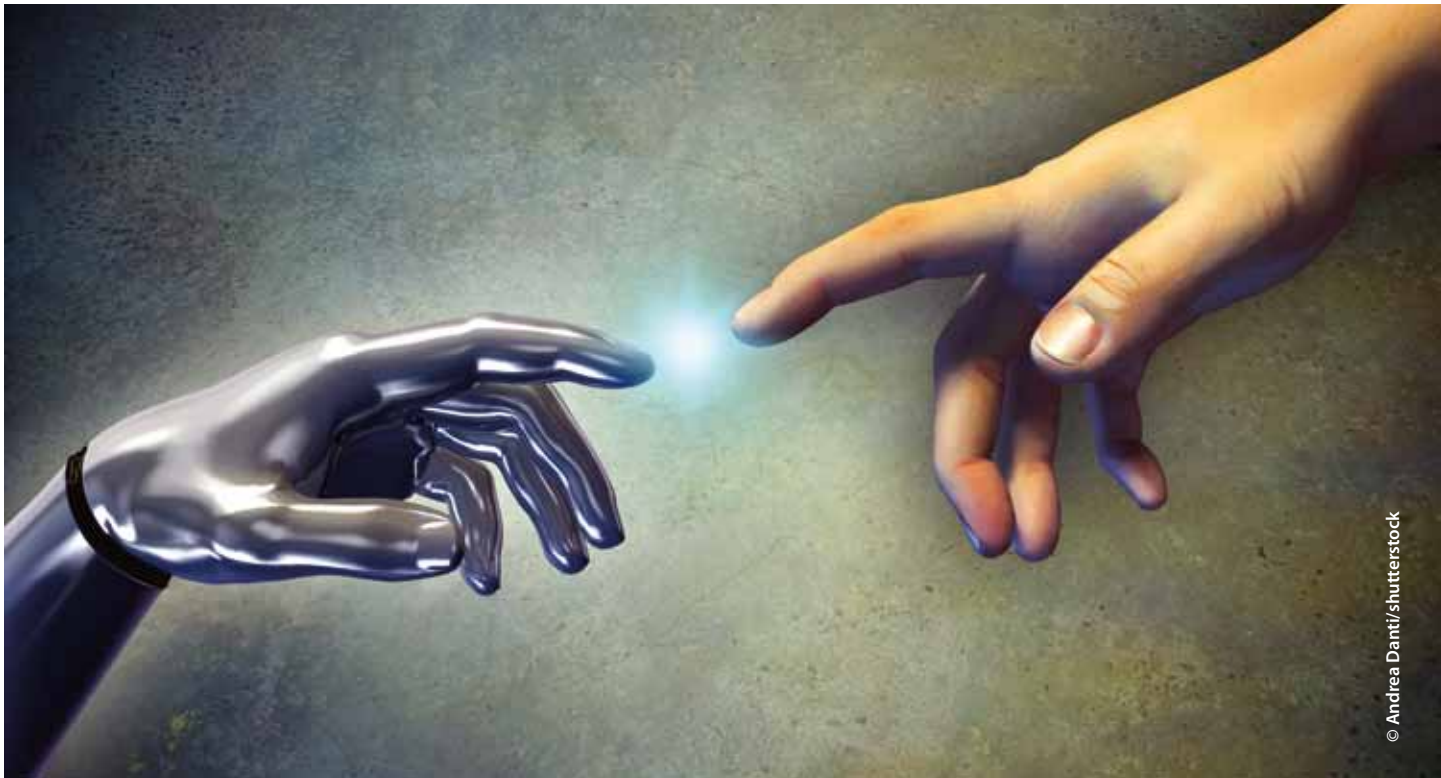
## 7.5 Assessment

What is ethically acceptable has always been defined by the society of the time. All previously discussed legal principles of international law have their foundations in this development of ethical guidelines. It is doubtful that AWS will be able to act perfectly ethically in the conduct of hostilities, but they may perform more ethically than humans, whose behaviour during war is often questionable at best.

The aforementioned arguments focus on the assumed coincidence of two capabilities, i.e., an AWS would be autonomous in its literal meaning and it would provide or support lethal weapon employment. If only one of these capabilities is present, either a human controlled weapon or an unarmed autonomous system, the aforementioned ethical issues do not apply, as the AWS in question is not able to autonomously employ lethal force.

Conclusively, 'meaningful human control' should always be involved in the application of force. Defining meaningful human control, however, is difficult. The Martens Clause (cf. Chapter 4) could be used as a guiding concept here by utilizing the principles of humanity and public conscience. Furthermore, Asimov's robotic laws may serve as a guiding principle if slightly adjusted.





## CHAPTER VIII

### Conclusions

Automated weapon systems are not new and have been in service since the 1970s. Due to increasing computerization, which allowed for more and more complex control software, these systems evolved to a stage where they give the impression that they behave autonomously. But, in fact, there are no autonomous systems developed yet nor will there be an artificially intelligent, self-aware robot in the near future, if ever. The term 'autonomy' is commonly and wrongly used as a buzzword and does not reflect the current (and likely future) stage of technology. Admittedly, simple automation has been surpassed already and therefore current and future sophisticated unmanned systems should more accurately be labelled as 'highly automated' or, as proposed by this study, 'autonomic.'

International law does not explicitly address automated, autonomic or even autonomous weapons. Conclusively, there is no legal difference between these

weapons. What they all have in common is the absence of human control, although with varying degrees. But regardless of the different levels of human control, any weapon and its use in an armed conflict has to comply with the principles and rules of IHL. Therefore, AWS cannot simply be labelled unlawful or illegal. In fact, they may be perfectly legal if they are capable of adhering to the principles and rules of IHL or if their 'modus operandi' is restricted in a way that they cannot cause, or can sufficiently minimize, civilian harm.

International law consists of customary law and treaty law. Customary law derives from long established practices between states and is obligatory for any state, regardless of their ratification of a specific international treaty. In contrast, treaty law only applies to states which are party to a treaty, agreement or convention. It is noteworthy, that within NATO different Nations signed and ratified dissimilar international treaties. However, the principles and rules of international law discussed in this study are commonly recognised as customary IHL. Consequently, there are no

legal dissimilarities within the Alliance in this regard and any NATO Nation is obliged to follow these principles and rules when developing, fielding and operating AWS.

The principles of international humanitarian law to be followed are predominantly the ones of distinction, proportionality and precaution. None of them can be looked at in isolation as they are all interwoven and require each other to protect civilians and civilian objects during the conduct of hostilities. The requirements for an AWS to adhere to these principles are technically extremely high, especially if the AWS is intended to operate in a complex environment. However, considering the current speed of technological advances in computer and sensor technology it appears not unlikely that these requirements may be fulfilled in the not so distant future. Deriving from the obligation to follow the aforementioned principles, every country has to ensure that AWS are thoroughly tested and reviewed before using them. In this regard, Asimov's robotic laws may serve as a guiding principle if slightly adjusted.

**1. A robot may not unlawfully injure a human being or, through inaction, allow a human being to come to harm unlawfully.**

**2. A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.**

**3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.**

Nevertheless, not even the most sophisticated computer system can be expected to be perfectly flawless.

Consequently, potential erroneous system behaviour has to be an integral part of the review process, and, most importantly, the probability of error should be at least equal if not lower than that of humans confronted with a similar task and environment.

If an AWS violates international law the overall responsibility lies with the sending Nation. This is not at all different from any human originated breaches of international law and entails the same consequences, e.g., commitments to pay damages to the victims or other sanctions of the international community against the sending state. The individual responsibility of the military commander, system operator, manufacturer or programmer may be judged, firstly, by their national jurisdiction or, in a subsidiary way, by the International Criminal Court if certain conditions are met, such as a ratified treaty by the defendant's state. However, individual responsibility may only be applicable if severe negligence or intent can be evidenced.

With regard to the ethical issues discussed, the three predominant concerns about the use of AWS should be taken seriously. These concerns are:

**Machines must not decide on life and death of humans,**

**Machines cannot substitute human judgement,**

**Machines must always be predictable.**

Finally, this emphasizes the necessity for a meaningful level of human control with regard to any use of AWS at present or in the future and this should be based on the principle of humanity and public conscience.

# ANNEX A

## Bibliography

**Asimov, Isaac**, 'The Three Laws', *Computel*, Issue 18 (1981): 18; available from [https://archive.org/stream/1981-11-compute-magazine/Compute\\_Issue\\_018\\_1981\\_Nov#page/n19/mode/2up](https://archive.org/stream/1981-11-compute-magazine/Compute_Issue_018_1981_Nov#page/n19/mode/2up).

**Computer History Museum**, *Where to? A History of Autonomous Vehicles* (accessed 6 Oct. 2016); available from <http://www.computerhistory.org/atchm/where-to-a-history-of-autonomous-vehicles>.

**Computerworld UK**, *Top software failures 2015/2016: Amazon, RBS, Starbucks – the worst software glitches this year* (accessed 11 Oct. 2016); available from <http://www.computerworlduk.com/galleries/infrastructure/top-10-software-failures-of-2014-3599618>.

**Cornell University Law School**, *Criminal Law* (accessed 11 Oct. 2016); available from [https://www.law.cornell.edu/wex/criminal\\_law](https://www.law.cornell.edu/wex/criminal_law).

**Crawford, Emily and Davies, Kayt**, 'The International Protection of Journalists in Times of Armed Conflict: The Campaign for a Press Emblem', *Wisconsin International Law Journal* (2014); available from [http://hosted.law.wisc.edu/wordpress/wilj/files/2015/03/Crawford\\_final.pdf](http://hosted.law.wisc.edu/wordpress/wilj/files/2015/03/Crawford_final.pdf).

**Curtis E. Lemay Center for Doctrine Development and Education**, Annex 3-60 Targeting – Dynamic Targeting and the Tasking Process (accessed 11 Oct 2016); available from <https://www.doctrine.af.mil/download.jsp?filename=3-60-D17-Target-Dynamic-Task.pdf>.

**Defense Systems**, *Navy extends UAV range with first in-flight refueling* (accessed 6 Oct 2016); available from <https://defensesystems.com/articles/2015/04/27/navair-x47b-uas-midair-refueling.aspx>.

**European Parliament, Committee on Legal Affairs**, *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))* (accessed 11 Oct. 2016); available from <http://www.euro>

[parl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN](http://parl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN).

**European Parliament, Directorate-General for External Policies of the Union**, *Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare* (Dr. Nils Melzer, 2013).

**Federal Aviation Administration**, *Fact Sheet – General Aviation Safety* (accessed 11 Oct. 2016); available from [http://www.faa.gov/news/fact\\_sheets/news\\_story.cfm?newsId=16774](http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=16774).

**Google**, *Google Photos* (accessed 6 Oct. 2016); available from <https://www.google.com/photos/about>.

**Henckaerts, Jean-Marie**, 'Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict', *International Review of the Red Cross*, vol. 87, no. 857, pp. 175–212, 2005.

**Human Rights Watch, International Human Rights Clinic (IHRC) at Harvard Law School**, *Losing Humanity – The Case against Killer Robots* (accessed 6 Oct. 2016); available from <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>.

**IBM Corporation**, *An architectural blueprint for autonomic computing* (accessed 6 Oct. 2016); available from <http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf>.

**International Committee of the Red Cross (ICRC)**, *Commentary of 1987 – New Weapons* (accessed 10 Oct 2016); available from <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=F095453E41336B76C12563CD00432AA1>.

**International Committee of the Red Cross (ICRC)**, *Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (Geneva, 2006).

**International Committee of the Red Cross (ICRC),** *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Dr. Nils Melzer, Legal Adviser, ICRC, Geneva, May 2009); available from <https://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf>.

**International Committee of the Red Cross (ICRC),** *The Emblems* (accessed 10 Oct 2016); available from <https://www.icrc.org/eng/war-and-law/emblem/overview-emblem.htm>.

**International Committee of the Red Cross (ICRC),** *Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land* (The Hague, 29 Jul. 1899).

**International Committee of the Red Cross (ICRC),** *Customary IHL*, (accessed 10 Oct. 2016); available from <https://ihl-databases.icrc.org/customary-ihl/>.

**International Committee of the Red Cross (ICRC),** *The Geneva Conventions of 1949 and their Additional Protocols* (accessed 10 Oct 2016); available from <https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols>.

**International Court of Justice (ICJ),** *Statute of the International Court of Justice* (accessed 10 Oct. 2016); available from <http://www.icj-cij.org/documents/?p1=4&p2=2>.

**Israel Aerospace Industries (IAI),** *Heron* (accessed 6 Oct 2016); available from [http://www.iai.co.il/2013/18900-16382-en/BusinessAreas\\_UnmannedAirSystems\\_HeronFamily.aspx](http://www.iai.co.il/2013/18900-16382-en/BusinessAreas_UnmannedAirSystems_HeronFamily.aspx).

**Jacobsson, Marie,** 'Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments', *International Law Studies*, vol. 82, pp. 183–191.

**Joint Air Power Competence Centre (JAPCC),** *Machines Do Not Think! The Contradiction with Autonomous Systems* (accessed 11 Oct. 2016); available from: <https://www.japcc.org/portfolio/flyer-9>.

**Kant, Immanuel,** *Fundamental Principles of the Metaphysics of Morals* (accessed 6 Oct. 2016); available from <http://www.gutenberg.org/ebooks/5682>.

**Krishnan, Armin,** *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Routledge, Taylor & Francis Group, 17. Jul. 2009).

**Kudale, Amruta,** *Case study: The Ariane 5 explosion due to software error* (accessed 11 Oct. 2016); available from [https://www.academia.edu/11818474/Case\\_study\\_on\\_Ariane\\_5\\_launch\\_failure](https://www.academia.edu/11818474/Case_study_on_Ariane_5_launch_failure).

**Lin, P. et al.,** *Autonomous Military Robotics: Risks, Ethics and Design* (US Office of Naval Research, 2008).

**Lockheed Martin,** *Autonomic Logistics Information System* (accessed 6 Oct. 2016); available from <http://www.lockheedmartin.com/us/products/ALIS.html>.

**Lockheed Martin,** *F-35 Capabilities – Multi-Mission Capability for Emerging Global Threats* (accessed 6 Oct. 2016); available from: <https://www.f35.com/about/capabilities>.

**McClelland, Justin,** 'The review of weapons in accordance with Article 36 of Additional Protocol I' *International Review of the Red Cross*, vol. 85, no. 850, pp. 397–415, 2003.

**Microsoft Corporation,** *Windows Live Photo Gallery and Movie Maker* (accessed 6 Oct. 2016); available from <https://www.microsoft.com/en-US/download/details.aspx?id=26689>.

**North Atlantic Treaty Organization (NATO),** Allied Command Transformation, Multinational Capability Development Campaign (MCDC) 2013-2014, *Role of Autonomous Systems in Gaining Operational Access, Policy Guidance, Autonomy in Defence Systems* (Artur Kuptel and Andrew Williams, MCDC, 2014).

**North Atlantic Treaty Organization (NATO),** Allied Command Transformation, Innovation Hub, *How to Counter Unmanned Autonomous Systems?* (accessed 6 Oct. 2016); available from <http://innovationhub-act.org/AxSCountermeasures>.

**North Atlantic Treaty Organization (NATO),** *NATO Glossary of Terms and Definitions (AAP-06)* (NATO, 2015)

**Northrop Grumman,** *RQ-4 Global Hawk Factsheet* (accessed 6 Oct. 2016); available from [http://www.northropgrumman.com/capabilities/rq4block20globalhawk/documents/hale\\_factsheet.pdf](http://www.northropgrumman.com/capabilities/rq4block20globalhawk/documents/hale_factsheet.pdf).

**Psibernetix Inc,** *Flagship Defense AI: ALPHA* (accessed 6 Oct. 2016); available from <http://www.psibernetix.com/projects/defense>.

**Raytheon,** *Phalanx Close-In Weapon System - Last Line of Defense for air, land and sea*, (accessed 6 Oct. 2016); available from <http://www.raytheon.com/capabilities/products/phalanx/>.

**Rheinmetall Defence,** *Fresh success for Rheinmetall in air defence: MENA nation places new €83 million order* (accessed 6 Oct. 2016); available from [http://www.rheinmetall-defence.com/en/rheinmetall\\_defence/public\\_relations/news/archive\\_2014/details\\_5120.php](http://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/news/archive_2014/details_5120.php).

**Rifkin, Jeremy,** *The End of Work: The Decline of the Global Labor Force and the Dawn of the Post-Market Era* (New York, Putnam Publishing Group, 1995).

**SentientVision Pty Ltd,** *KESTREL LAND MTI* (accessed 6 Oct. 2016); available from <http://www.sentientvision.com/products/kestrel-land-mti>.

**Shen, S., Michael, N., Kumar, V.,** University of Pennsylvania, *Autonomous Aerial Navigation in Confined Indoor Environments* (accessed 6 Oct. 2016); available from <https://www.youtube.com/watch?v=IMSozUpFFkU>.

**Society of Automotive Engineers (SAE),** *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems* (SAE International, 2014).

**United Nations General Assembly,** *Universal Declaration of Human Rights (UDHR)* (Paris, 10 Dec. 1948); available from <http://www.un.org/en/universal-declaration-human-rights>.

**United Nations Human Rights Office of the High Commissioner,** *International Legal Protection of Human Rights in Armed Conflict* (New York and Geneva, 2011).

**United Nations Office at Geneva (UNOG),** *Background – Lethal Autonomous Weapons Systems* (accessed 6 Oct. 2016); available from [http://www.unog.ch/80256EE600585943/\(httpPages\)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument).

**United Nations Office at Geneva (UNOG),** *Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS)* (accessed 6 Oct. 2016); available from [http://www.unog.ch/80256EDD006B8954/\(httpAssets\)/DDC13B243BA863E6C1257FDB00380A88/\\$file/ReportLAWS\\_2016\\_AdvancedVersion.pdf](http://www.unog.ch/80256EDD006B8954/(httpAssets)/DDC13B243BA863E6C1257FDB00380A88/$file/ReportLAWS_2016_AdvancedVersion.pdf).

**United Nations Office at Geneva (UNOG),** *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW)* (21 Dec. 2001).

**United Nations Office of Legal Affairs Codification Division,** *Convention on the Safety of United Nations and Associated Personnel* (accessed 10 Oct. 2016); available from <http://www.un.org/law/cod/safety.htm>.

**United Nations,** *Rome Statute of the International Criminal Court (ICC), circulated as document A/CONF.183/9 of 17 Jul. 1998 and corrected by process-verbaux of 10 Nov. 1998, 12 Jul. 1999, 30 Nov. 1999, 8 May 2000, 17 Jan. 2001 and 16 Jan. 2002.* (accessed 10 Oct. 2016); available from <http://legal.un.org/icc/statute/romefra.htm>.

**United States Congressional Research Service (CRS),** *Cluster Munitions: Background and Issues for Congress* (Andrew Feickert, Paul K. Kerr, CRS, 2014); available from <https://www.fas.org/srgp/crs/weapons/RS22907.pdf>.

**United States National Institute of Standards and Technology,** *Autonomy Levels for Unmanned Systems (ALFUS) Framework* (accessed 6 Oct. 2016); available from [https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP\\_1011-I-2-0.pdf](https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP_1011-I-2-0.pdf).

**United States Navy**, *X-47B Makes First Arrested Landing at Sea* (Brandon Vinson, USS George H.W. Bush Public Affairs, 2013); available from [http://www.navy.mil/submit/display.asp?story\\_id=75298](http://www.navy.mil/submit/display.asp?story_id=75298).

**Watson, David P. and Scheidt, David H.**, 'Autonomous Systems', *Johns Hopkins APL Technical Digest*, vol. 26, no. 4 (2005): 368; available from <http://www.jhuapl.edu/techdigest/TD/td2604/Watson.pdf>.

**World Nuclear Association**, *Safety of Nuclear Power Reactors* (accessed 11 Oct. 2016); available from <http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx>.



# ANNEX B

## Acronyms and Abbreviations

<b>A3R</b>	Autonomous Air-to-Air Refuelling	<b>IAI</b>	Israel Aerospace Industries
<b>ACT</b>	Allied Command Transformation	<b>ICC</b>	International Criminal Court
<b>AI</b>	Artificial Intelligence	<b>ICJ</b>	International Court of Justice
<b>ALIS</b>	Autonomic Logistics Information System	<b>ICRC</b>	International Committee of the Red Cross
<b>AP I</b>	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts	<b>IHL</b>	International Humanitarian Law
<b>AWS</b>	Autonomic, or Autonomous Weapon System	<b>IHRC</b>	International Human Rights Clinic
<b>BTWC</b>	Biological and Toxin Weapons Convention	<b>IHRL</b>	International Human Rights Law
<b>CCW</b>	Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects	<b>ISR</b>	Intelligence, Surveillance, and Reconnaissance
<b>CIWS</b>	Close-In Weapon Systems	<b>LAWS</b>	Lethal Autonomous Weapon Systems
<b>CRS</b>	Congressional Research Service	<b>LGB</b>	Laser Guided Bomb
<b>EO/IR</b>	Electro-optical / Infrared	<b>LOAC</b>	Law of Armed Conflict
<b>F2T2EA</b>	Find, Fix, Track, Target, Engage, Assess	<b>MCDC</b>	Multinational Capability Development Campaign
<b>FMV</b>	Full-motion Video	<b>NATO</b>	North Atlantic Treaty Organization
<b>GMTI</b>	Ground Moving Target Indication	<b>RPA</b>	Remotely Piloted Aircraft
<b>HC II</b>	Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land	<b>SAE</b>	Society of Automotive Engineers
		<b>UAS</b>	Unmanned Aircraft System
		<b>UDHR</b>	Universal Declaration of Human Rights
		<b>UN</b>	United Nations
		<b>UNOG</b>	The United Nations Office at Geneva



# NOTES

## NOTES





## **Joint Air Power Competence Centre**

von-Seydlitz-Kaserne

Römerstraße 140 | 47546 Kalkar (Germany) | [www.japcc.org](http://www.japcc.org)