

The Use of Lethal Autonomous Weapon Systems in an Electromagnetic Spectrum Contested Environment

Written for Dr. Sam Tangredi, Institute for Future War Studies, US Naval War College

William Rockwood
Frank Batten School of Leadership & Public Policy
University of Virginia
April 8, 2022

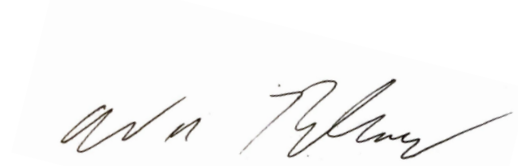
Acknowledgements:

As with any big project like this, there are a lot of people to thank. First, and most importantly, is my client, Dr. Sam Tangredi of the US Naval Warfare School who was willing to be my client and invited me to a virtual symposium in the autumn in artificial intelligence in warfare. I would also like to thank my APP class Professors, Professor Gelsdorf and Professor Stam, for giving me enough rope to hang myself with—thanks to Dr. Tangredi for this too—and a special thanks to Professor Gelsdorf for not making me redo my literature review the weekend I took my girlfriend to a cabin in the Shenandoah Valley for her birthday.

A thanks to my classmates—especially the ones in the group-chat Catten—who commiserated and advised me throughout this.

And a special thanks to my parents who are very supportive of everything I do—no matter how ridiculous it may seem—and my girlfriend for letting me talk to her about artificial intelligence and “killer robots” all year.

This, my second master’s thesis, was not nearly as much fun as the first (which was in Creative Writing), and I can safely say, this will be the last.

A handwritten signature in black ink, appearing to read 'Sam Tangredi', is centered on the page. The signature is fluid and cursive, with a large, sweeping flourish at the end.

Honor Pledge: On my honor as a student, I have neither given nor received aid on this report.

Disclaimer: The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

Executive Summary:

Lethal autonomous weapon systems (LAWS) are conventional weapons attached to a platform and controlled by an artificial intelligence enabled computer system. Once activated, they can select and engage targets without further intervention by a human operator. They have been used recently in Narbako-Karmaiv, Libya and Ukraine, and are likely to be used many times in the near future, including by the US Navy. The Department of Defense has issued guidelines for their use, stating that they must be under “reasonable control” of human commanders, but makes the bold assumption that a human will always be able to quickly and clearly communicate with a LAWS. This assumption is unlikely to hold in an electromagnetic spectrum contested environment, where communications are degraded. In order to address this policy hole, I provide background on the technology that makes up a LAWS, the twenty-first century battlefield, and contest in the electromagnetic spectrum.

I consider four possible policy alternatives for the use of LAWS in an electromagnetic spectrum contested environment: (1) recall them when communications are lost, (2) send US Navy sailors downrange with them in order to maintain light of sight communications, (3) operate LAWS within a mesh network of communications to maintain contact at all times and (4) assign LAWS targets that can only be military targets and allow them to operate independently in accordance with prior orders once communications are lost. I evaluate the alternatives across four criteria: lethality, chance of harming sailors, allies & civilians, cost, and control.

From those criteria I **recommend that the US Navy operate LAWS within a mesh network of communications to maintain contact at all times**, a recommendation already in line with the existing Defense Advanced Research Project Agency’s Mosaic Warfare Initiative. This alternative also takes advantage of the “centaur” method of using autonomous weapon systems, and provides a backstop for when—not ‘if,’ but ‘when’—LAWS malfunction or suffer a mishap.

(Word Count: 8,267)

<i>Section</i>	<i>Page</i>
Executive Summary	2
I. Introduction	4
II. Problem Statement	5
III. Background	6
a) The Weapon	6
i) Lethal Autonomous Weapon Systems	6
ii) Artificial Intelligence	7
iii) Complex Systems Theory	9
b) The Twenty-first Century Battlefield	11
i) Complexity	11
ii) Violence	12
iii) Opacity	13
c) Contested Electromagnetic spectrum	14
IV. Literature Review	16
V. Alternatives to be Evaluated	17
VI. Criteria for Evaluation	20
a) Criteria	20
b) Scale	21
VII. Findings & Recommendation	22
a) Findings	22
b) Outcomes Matrix	26
c) Recommendation	26
VIII. Implementation	27
Works Cited	29
Bibliography	33
Appendix 1: DoD Directive 3000.09	35
Appendix 2: Chaos Engineering	50

I. Introduction

For the first time in history, weapon systems that are able to distinguish and attack their targets without the direct intervention of human operators are in use on battlefields. In December of 2020, Israeli-made “loitering munitions” were used by the Azerbaijani military to attack Armenian radar sites in Narbako-Karmaiv (Atherton, 2021), in early 2021, Turkish-made drones enabled with facial recognition attacked Khalifa Haftar’s soldiers in Libya (Kallerborn, 2021), and in right now, are being used against Russian soldiers in Ukraine. (De Vynck, Verma, & Baran, 2021) These lethal autonomous weapon systems (LAWS) are another piece of the evolution of warfare in the 21st Century, but unlike data analysis or cyber-attacks, these weapon systems have a high and direct capacity for destructive harm. While the United States Department of Defense has not used these weapons systems yet, it is developing them, and has already written guidelines for their use. However, those guidelines say nothing about the use of LAWS in an electromagnetic spectrum contested environment, a likely scenario in the twenty-first century battlefield.

II. Problem Statement

At present, US Department of Defense Directive 3000.09 dictates that autonomous weapon systems (LAWS) shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force. However, this policy makes the bold assumption that a human will always be able to communicate clearly and quickly with a forward deployed weapon system. This is unlikely in an electromagnetic spectrum contested environment—where the vast majority of communications will be degraded if not entirely denied—putting members of the US Armed Forces, their equipment, and the mission, in tremendous danger. Given the complex nature of the technology, the US Navy needs to determine how it is going to use lethal autonomous weapon systems in the future, so as to build the weapons those capabilities now.

III. Background:

This problem does not exist in a vacuum, and in order to craft a solution it is important to understand both the technology of a lethal autonomous weapon, and the environment it will be operating in.

a) The Weapon

i) Lethal Autonomous Weapon Systems (LAWS)

LAWS are conventional weapons—such as missiles, rockets, guns, or explosives—attached to a transportation platform, and are controlled, or possess the ability to be controlled by, an artificial intelligence enabled computer system (Scharre, 44). The Department of Defense defines them as “a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.” (DoDD 3000.09, 13).

The big advantages that they will bring to the modern battlefield are speed, flexibility and protection for the operator. The speed at which these weapon systems will be able to collect, analyze, and act on information would be impossible for a human to match. They will also be able to collect more real time data than humans can, in ways that humans cannot—such as through the heat or electromagnetic spectrum—process it faster than any human would be able to, and once they have found them, attack their targets in ways humans would not even begin to think of. Finally, their biggest contribution will be the ability to protect sailors already on the battlefield. This may take the form of moving them farther from the physical battlefield, having fewer of them on the battlefield, or fighting other LAWS that will move too fast for humans to effectively defend themselves against. (Scharre, 6) (Payne, 173)

In Narbako-Karmaiv and Libya, LAWS took the form of small aircraft called loitering munitions that conducted “kamikaze attacks,” but it is not a stretch to imagining them as tanks, ships, submarines, land based “kamikaze vehicles”—like the ‘Mad-Max Fury Road’-esque vehicle borne improvised explosive devices (VBIED) used by the Islamic State in 2014—or artillery. The latter would be especially deadly because from 2014-2016, 85% of casualties in Ukraine came from artillery. Remotely piloted aircraft (RPA) played a large role in the deployment of artillery. A RPA would find the target, artillery would engage it, and the RPA would return to conduct a damage assessment (Karber, 18). It is extremely likely that in the futures a LAWS will take the form of a 155mm cannon and reconnaissance RPA—dozens of them—that could search for targets, attack them, and move itself in self-defense, all without the direction of a human.

This makes LAWS more than a weapon on the battlefield, this makes them an agent, actively shaping, and being shaped by the area of operations they are in. (Payne, 19)

Arms Controls on LAWS

Despite calls to ban the use of LAWS, they will still be used worldwide. They are just too useful. As Paul Scharre points out in his book, *Army of None*, Pope Innocent II banned the use of the crossbow against Christians in 1139, and no one stopped using them until the invention of the musket. At a recent meeting of the UN Convention on Certain Conventional Weapons, a consensus on what constitutes an autonomous weapon system could not be reached—largely thanks to the Russian delegation—and therefore no part of the treaty could move forward. (Cheng, 2022) (Scharre, 331) (Payne, 10) (Zeitchik, 2022) (Dawes, 2022)

ii) Artificial Intelligence

The most important component of a LAWS is not the physical weapon it will possess, but the artificial intelligence (AI) system that will be controlling it.

Artificial intelligence is a machine that responds to stimulation consistent with traditional responses from humans. Most importantly, unlike a graphing calculator or even a powerful personal computer, AI is capable of both *making a decision* with the data it collects and learning from its decisions. (Allen & West, pg. 3) The power and speed of AI systems makes it sometimes hard to believe that they are simply powerful computers processing enormous quantities of data based off of their instructions and updates, and not human—or magic. (O’Neil, 18) (Arbesman, 28) These instructions are known as algorithms, and they are based off of a mathematical model of the world.

Algorithms & Machine Learning

The foundation of AI, **algorithms** are sets of steps for a computer written by a human that translate inputs into repeatable outputs. **Machine learning** algorithms are a subset that consist of steps for improving upon imprecise results. They are the AI systems that are constantly updating based on the data they collect, and the results of their decisions. There are different varieties of machine learning too. Some are trained using real data, some are trained using simulations or training data, and some are written with the most basic code possible and given real world data to analyze on their own. (Kissinger et al., 57)

Artificial intelligence’s big advantage is its speed of processing. It can absorb more inputs and make a decision on them faster than a human ever could. (Kissinger et al., 14) This speed of processing power means it is capable of finding insights a human would never find, and making

decisions a human would never make. While playing against AlphaGo, an AI enabled computer system that could play the board game Go, professional human players were baffled by several of the moves the computer made. Not because they were wrong, but because they—the human who had been playing the game their entire life—had never conceived the move as possible. (Scharre, 126) (Kissinger et al., 7)

However, artificial intelligence systems have several glaring weaknesses.

The first, is that they are heavily reliant on clean data, or a data set without incorrect, duplicate, missing or corrupted data points. This weakness is often overlooked because at the moment, AI typically operates online, where colossal amounts of data are available in easy to access formats. (Clarke & Knake, 247) But companies attempting to make self-driving cars have already experienced the difficulty of turning the infinitely complex real world into clean data in real time. It's one of the reasons self-driving cars have been the “next big thing” for about a decade now. Even with all their computing power, their models still struggle to operate in the real world, especially in urban environments, and especially around humans. (Allen & West, 64) (Piper, 2020) (Payne, 89)

The second major weakness is that AI systems are brittle. They are very good at doing what they are programmed to do; nothing more. A powerful AI system can easily be reduced to nonsense when conditions change even slightly from the optimal. (Payne, 5)

The final weakness is its model. A model is merely an abstract representation of some process, codified into computer code. We make models in our heads every day for our daily activities, such as cooking, commuting, or interacting with other people, and those models can also be poorly written, outdated, or just wrong. (O'Neil, 18) Just because the AI system is processing data at enormous speeds does not mean it is doing so correctly. Models are based off of the past, but the future does not always look exactly like the past. (O'Neil, 2018) Further exacerbating this problem is the fact that most algorithms are written using previously effective models. The code is transferred over and altered for the new model, but the underlying calculations might not be as effective for the new model as they were for the old. (O'Neil, 23) (Allen & West, 128) Finally, models are, by their nature, an incomplete picture of reality. Alan Turing, one of the foundation thinkers of computer science, proved that no human or computer made model can fully encompass the real world, and that there will always be some unknown that exists outside of the model, or some ‘ghost in the machine.’ (Payne, pg. 41) (O'Neil, 20)

Artificial Intelligence is a powerful tool, but it has enough major flaws to make one wary of relying on it too much.

Other Planned Uses for Artificial Intelligence in Warfare:

Speed has been a long sought-after advantage in war, and the pace of calculations offered by artificial intelligence means that LAWS will not be the only AI the twenty-first century battlefield. Other initiatives include **precision targeting**, **predictive maintenance** for vehicles and aircraft, **nuclear weapon monitoring** and tracking, data analytics of **intelligence**, **cyber-attacks**, spreading or inhibiting the spread of **disinformation**, and **swarming technology**. One of the most talked about uses for it is in **command and control**. This is often imagined as AI enabled systems either advising commanders in their decision making, or making the decisions and sending out orders. This could conceptually mean that AI enabled command and control systems would send out AI enabled LAWS to attack targets. (Allen & West, 117), (Payne, 58), (Scharre, 55)

iii) Complex Systems Theory

A M4 semi-automatic rifle—the weapon I carried as a Marine—is a mechanical system. It uses eight cycles of sequential functioning—feeding, chambering, locking, firing, unloading, extracting, ejecting and cocking—to fire a 5.56mm bullet wherever its operator is aiming. There are only about a dozen ways that system can malfunction, and those malfunctions and their consequences are predictable, and can be avoided through preventative maintenance, or overcome through immediate and remedial actions.

LAWS are complex systems; or a system of systems. At a minimum, a LAWS will be made up of the weapon system used to deliver the munition, the sensors used to identify targets, the platform used to transport the weapon system, a communications system to its controller or overseer, and the AI enabled computer system that controls all of it. These different components will all be interacting with one another constantly, and sometimes in ways they were not designed to. Even though it is a machine, its complexity is more akin to that of a biological organism than that of a piece of technology. (Arbesman, 155)

This complexity has upsides. Complex systems are resilient, and sophisticated. It is through complex systems that we power and run our modern lives. (Arbesman, 16) The laptop I wrote this report on is a complex system, as was the power grid that supplied the power to its battery. The downside is that I cannot explain their entire systems to you. I can explain to you the broad strokes of high-tension wires and step downs, or Apple software updates, but one of the hallmarks of a complex system is that it cannot be fully understood, even by those who built it. The technology that runs the twenty-first century has gotten so complex we can neither fully understand it, nor fully control it. (Arbesman, 17) LAWS are not, and will not be an exception.

The results of this complexity are already on display in the civilian world. There was the so-called Flash Crash of May 2010, when trading algorithms interacted in a series of unexpected

ways and companies lost trillions of dollars in value instantly, only to regain them moments later. (Arbesman, 25) (Scharre, 206) There was also the June 2021 momentary crash of several major websites on the internet due to a cloud upgrade (Arbesman, 2021), and there was Facebook going offline for several hours in the fall of 2021 due to a maintenance mishap. (Conger, 2021) The complexity is amplified as systems get older because they are updated on top of existing software and hardware, and it is also impossible to predict how current operating systems will interact with older operating systems from many years earlier that are still in the machine. (Arbesman, 34)

This is not to say that these systems do not work, because they obviously do, it only means that they are so complex no one can predict when they will break, how they will break, or how they can be fixed when they do break. (Arbesman, 24) It is certainly possible for someone to understand one or two of the five main parts of a LAWS, but even if they understood all of them, they still would not be able to understand how they all worked together, and how they all worked together under duress.

And LAWS will be under duress. They will not be operating in the internet or the metaverse like Facebook's malfunctioning servers, they will be in the physical world, in one of the most violent, austere, hostile, chaotic, and unpredictable environments in the history of man on Earth: the twenty-first century battlefield.

b) The Twenty-first Century Battlefield

The environment that lethal autonomous weapon systems will be operating in will be notable for its complexity, its violence, and its opacity.

i) Complexity

People have been fighting for thousands of years, but never in as many domains, with as violent, deadly, and hyper-accurate weapons, as they are today.

In Gaul, Julius Caesar had to contend with one domain of war: land, Napoleon Bonaparte and Arthur Wellesley fought over two: land and sea, and in the Pacific Theater of the Second World War, General MacArthur had to contend with five: land, sea, undersea, air, and the electromagnetic spectrum. Today, on the twenty-first century battlefield, there are eight domains of war: land, sea, undersea, sea bed, air, space, the electromagnetic spectrum, and cyberspace. These eight domains are their own complex system of systems, as each affects the others in unpredictable ways with surprising effects.

Adding to this complexity are the actors in these eight domains. Caesar, Napoleon Bonaparte, the Duke of Wellington, General MacArthur all fought battles with reasonably clear lines. People were, for the most part, either Roman or barbarian, French or British, Allied or Axis. Today, those clear lines are fading as nation-states lost the monopoly on violence they have had since the Treaty of Westphalia in 1648. Non-state armed actors such as terrorist organizations, militias, mercenaries, religious groups, insurgents, organized crime, and even thrill-seekers are all eager participants across all spectrums of the twenty-first century battlefield, for by a kaleidoscope of motivations. (McFate, 30) (Kilcullen, 10) These groups frequently flip sides, do not listen to their suppliers, and turn on one another, prolonging and expanding conflicts. (Schneider, 2016)

The recent Russian invasion of Ukraine highlights this complexity. Russia hired the Wagner Group—a mercenary force that does not technically exist—to kill Ukrainian President Volodymyr Zelensky at the outset of the war, and since their invasion began, they have fought against the Ukrainian Army, auxiliary forces, self-organized local militias, foreign volunteers, and the Azov Battalion, a neo-Nazi group. (Colchester, 2022) (Katz, 2022) Meanwhile, in cyberspace, the international hacker group Anonymous declared war on Russia after their invasion of Ukraine and began to attack them online (Tidy, 2022), and in the space and electromagnetic domains, the tech billionaire Elon Musk redirected his Starlink internet satellites to Ukraine, and sent over more internet terminals after being directly asked for help by the Ukrainian Minister of Digital Transformation over Twitter. (Lerman & Zakrzewski, 2022)

This factional complexity is actually not unique to the battlefield. The Middle Ages were a time of armed groups representing Lords, Barons, Kings, religious groups such as the Knights Templar, mercenaries, bandits, and pirates all competing for the same resources and acclaim. The Treaty of Westphalia was meant to consolidate the use of force in the hands of the state, and it did so for a long time, but that is now coming undone. (McFate, 2014, pg. 6)

Will these non-state actors have LAWS and other AI-enabled weapons?

Yes, through of the black market or through state benefactors. The volume of trade in the twenty-first century means that enormous amounts of illicit goods travel through legal channels every single day, as a port that inspected every cargo container would soon be a non-functioning port. It is estimated that Illicit trade now accounts for as much as 20% of global GDP, and it safe to assume that weapons of all kinds will be making their ways into the hands of whoever can pay for them. (Glenny, xv)

ii) Violence

While the complexity in domains and combatants of war has changed, it remains just as chaotic, violent, bloody and awful as it did when Caesar's legions took the field against the Gauls, Napoleon's soldiers marched up the hill at Waterloo, and MacArthur's forces retook the Philippines.

In his harrowing account of the 2009 Battle of Combat Outpost (COP) Keating in Nuristan, Afghanistan, Clinton Romesha¹ recounts being thrown about by explosions, seeing others ripped to pieces by automatic weapons, and watching buildings crumble amid fire and thick smoke. The initial Taliban barrage is like if "someone had seized hold of a fold in the sky, ripped a hole in the thing, and was now dumping all the munitions in eastern Afghanistan down on his head." (Romesha, 108) When a B1 bomber attacks the ridgelines the Taliban are firing from, dropping five hundred pound bombs less two-hundred yards away from him, Romesha likens it to being "an especially tiny insect—a type of mite, say—huddled inside the bass drum of a heavy metal rock band." (Romesha, 288) While Romesha's experience was exceptional—in that he was in a valley, surrounded—its violence was not unique. In his book about the 2016 Battle of Mosul, *They Will Have to Die Now*, James Verini recounts the endless stream of Islamic State VBIEDs that attack the Iraqi Army as they enter the city—they are so frequent that tanks need to face down avenues of approach as Humvees cross streets—and how they are packed with so much explosive that they shake houses when they detonate, and a successful attack on an Iraqi Army Humvee leaves nothing left of the gunner, nicknamed Spongebob. (Verini, 38)

¹ Who won the Congressional Medal of Honor for his actions during this battle.

Notable from both of their accounts is the precision and the accuracy of the weapons. Verini recounts Islamic State snipers shooting the mirrors off of Iraqi Army Humvees when no soldiers present themselves as targets, while Romesha points to the Taliban shooting at and hitting—though not bringing down—US Army helicopters. (Verini, 35) (Romesha, 256) This accuracy is a reflection of the dispersion of both military technology and small unit tactics. (Blanken, Thaxton, & Alexander, 2018) During Russia’s 2014 invasion of Ukraine, both sides found that lightly armored vehicles did not protect the men inside from laser guided munitions and precision artillery, so soldiers from both sides preferred to ride on the vehicles rather than in them. (Karber, 38)

iii) Opacity

For all this violence, the twenty-first century battlefield largely exists in a nebulous space of conflict, but not quite open war. This is often referred to as “the Gray Zone,” and the Australian counter-insurgency expert David Kilcullen defines it as:

“Neither fully overt nor truly clandestine; rather, it rides the edge, surfing the threshold of detectability, sometimes subliminal (literally “below” the threshold of perception), at other times breaking fully into the open to seize an advantage or consolidate gains before adversaries can react.” (Kilcullen, 119)

This definition is reflected in both Romesha and Verini’s accounts of their battles, with Romesha recounting how the Taliban reconnoitered COP Keating from beneath burkas—one soldier in a tower even shouted to apathetic Afghan Security Guards “Hey, search that lady, she’s got the hairiest damn feet I’ve ever seeing in my life!” (Romesha, pg. 77)—and Verini recounting the ambiguity that was the Iraqi Army lived in as it assessed who was a member of the Islamic State, who was a supporter, who had been forced to work for them, and where the next VBIED might be hidden. (Verini, 122).

While not new to war by any means, gray zone operations have become the *modus operandi* for many, especially non-western or non-democratic factions, in the twenty-first century.² It is reflected in Russia’s use of the Wagner Group in Syria and Ukraine, (Kofman, 2017) its “Little Green Men” in Crimea in 2014, and China’s maritime militia (Erickson & Kennedy, 2016).

² Obviously, the current conflict in Ukraine contradicts this assessment, but I would argue that Russian President Vladimir Putin only opted for a conventional assault of Ukraine *after* his gray zone operation—a mercenary backed coup—was foiled in November of 2021 (Stern, 2021), and that the lack of success of this conventional operation will push future conflicts back into the gray zone, but that is outside the scope of this paper.

Strangely, or perhaps because of, this gray zone mode of warfare is rising to prominence in a hyperconnected world. Writing in the New York Times, Tom Friedman notes that 3-4 billion people have smartphones worldwide. He has called Russia's conventional invasion of Ukraine World War Wired because people everywhere are able to watch missile strikes, speeches, and even live videos of combat from their phones, and then share their opinions on what they've seen instantly. (Friedman, 2022) Unlike brutality, or factional complexity, this is unique to the twenty-first century battlefield, and has demonstrated the potential to make battlefield mistakes, or outright war crimes, into strategic level errors in a matter of hours.

c) The Electromagnetic Spectrum

Wartime communications have been contested since they were carried by runners, and the electromagnetic spectrum is no different. The electromagnetic spectrum is the medium through which all radio, radar, cellular, wireless data, visual, and communications signals pass. It was first contested in the Second World War as the Axis and Allied Powers attempted to intercept and track one another's communications. Today it is far more crowded and complex, with dozens of satellites, towers, radios, and the contest can occur either at the infrastructure, or in the spectrum itself. (Tourangeau, 2018)

Attacking communications infrastructure can take the form of either a physical attack, or a hack of software. A physical attack is straightforward and involves destroying the communications towers, satellites, or undersea cables that connect one person to another.³ Hacking attacks are much more common though because they do not involve destroying physical infrastructure—which the attacker might want to use at some point—and have the deniability so sought after in the gray zone. When overt (as opposed to intelligence gathering), these attacks almost always take the form of a distributed denial of service, either through spoofing, ransomware, or malware that shuts down the network. Russia has used them to great effect on its near neighbors in the past decade. They overwhelmed and made inoperable the internet in Estonia through coordinated requests for data, increased traffic, and overloading servers. (Cyberlaw, 2022) They also crashed the Ukrainian energy grid in 2016 (Perloth, 293), and as they launched their conventional invasion of Ukraine in February of this year, they attacked the modems of the US satellite firm, Viasat, which was used by the Ukrainian military, government agencies, and many civilians to disrupt Ukrainian communications. (Schaffer, 2022) (Corera, 2022)

However, regardless of their form, these attacks all are labor intensive, intricate, and fragile. Despite Hollywood depictions of hackers being a single person typing furiously on a keyboard, most hacks are conducted by teams with powerful computers who have managed to make every single step in a delicate process. The so-called kill chain for hacking is reconnaissance,

³ The Russian Navy does this in James Stavridis and Elliot Ackerman's future war novel *2034*, and kills a bunch of sharks in the process.

weaponization, delivery, exploitation, installation, command and control, and actions on. If a defender disrupts just one of those steps, then the hacker team is back to square one. (Clarke & Knake, 51)

Attacking the spectrum itself is more complicated, but the effects are similar. The weapons include particle beam weapons, high powered microwaves, electromagnetic bombs, and rail guns. (Globe News Wire, 2021) The most powerful of these is an electromagnetic bomb, which is a massive burst of electromagnetic energy, and destroys communications by surging power through communications equipment. (Gent, 2021) They have not been used so far, but smaller, more focused attacks have been successful. Russia jammed GPSes during a NATO exercise in 2018 (Schneier & Wheeler, n.d.), knocked out Latvian cellular communication twice in 2017, and briefly jammed Norwegian GPS at the same time.⁴ (Trevithick, n.d.) (Gelzis & Emmott, 2017)

⁴ This despite the fact they were apparently aiming for Sweden, who claimed to have suffered no denial of any kind.

IV. Literature Review

Believe it or not, I am not the first person in the world to write about the use of LAWS in an electromagnetic spectrum contested environment. Dr. Paul Scharre of the Center for New American Security, devoted four whole pages near the end of his book, *Army of None*, to it. Throughout his book, he maintains that humans should both choose targets for LAWS and supervise them while they attack. Within an electromagnetic spectrum contested environment, he advocates for the use of Defense Advanced Research Projects Agency (DARPA) Collaborative Operations in Denied Environment (CODE) program to maintain communications. He notes that the communications available from the CODE program will be very low bandwidth—about equivalent to that of 56K modem from the 1990s—but still adequate for a trained human to confirm targets. (Scharre, 327)

In a completely denied environment, Dr. Scharre thinks it would only be practical—in terms of targeting responsibility—for LAWS to attack pre-authorized fixed targets, and goes on to question the military value of a LAWS attacking mobile targets while operating outside of human control and supervision, given the risks of the weapon failing, being hacked, or attacking the wrong target. (Scharre, 329)

V. Alternatives to be Evaluated

The US Navy has several policy alternatives for the use of LAWS in an electromagnetic spectrum contested environment.

(1) Recall LAWS when communications are lost.

This alternative is the most basic, and most applicable across all weapon systems. It is based off of most of the No Communications Plans I used in training in the Marine Corps, which was to return to a point of last known communication when communications went down. These points could be easily preprogrammed into the weapon systems, and be theater or situation dependent. Recall also does not mean complete removal from the battlefield, just moving to a rendezvous point to reestablish communications. This plan will be complicated further by the nature of the communications on the LAWS, and the available communications structure as LAWS will likely communicate via data, which requires more bandwidth than voice, and therefore need to likely withdraw farther from the battlefield.

What about the DARPA CODE Program?

While DARPA is developing jam proof communication frequencies, those are limited in terms of both resources and spectrum, and it is in the interest of the US Navy to assume that it will not have access to those spectrums when it operates LAWS in an electromagnetic spectrum contested environment. (Scharre, 329)

(2) Send US Servicemembers downrange with LAWS to maintain line of sight communication.

This alternative is based off of the “centaur” approach advocated by Paul Scharre and Kenneth Payne in their books on LAWS. (Scharre, 321) (Payne, 181) It combines the speed and accuracy of LAWS with the creativity and understanding of the human mind; a potent combination in the infinitely complex space that is the twenty-first century battlefield. Line of sight communications could be maintained with ultra-high frequency radio waves—the same ones that are currently used to talk with aircraft from the ground and make 5G possible—which are extremely hard to jam over a wide area, and can be amplified with repeaters. In this way, commanders will, through the humans who are also in the electromagnetic spectrum contested environment, maintain reasonable control over the LAWS as they operate.

Centaurs in Action

In November of 2020, Israeli intelligence agents assassinated Mohsen Fakhrizadeh, an Iranian Nuclear scientist, using a remote controlled, AI assisted machine gun. The Israeli agents smuggled the weapon into Iran in pieces, and assembled it on a pickup truck meant to look like a construction vehicle hill overlooking the highway leading to Mr. Fakhrizadeh's vacation home on the Caspian Sea. After confirming Mr. Fakhrizadeh's identity at a hairpin turn, the Mossad agent fired while the AI weapon adjusted the shots to compensate for the 1.6 second delay between the cameras sending the image of Mr. Fakhrizadeh to the Mossad triggerman and his command to fire. Mr. Fakhrizadeh died on the road. Fifteen shots were fired, seven hit Mr. Fakhrizadeh, none hit his wife who was sitting right beside him in the car. (Bergman & Fassihi, 2021)

(3) Operate LAWS within a mesh network of communications to maintain contact at all times.

This alternative builds upon the concept of mosaic warfare, but adds a layer of complexity to the already complex system that is a LAWS. In this scenario, every weapon in the US Navy's arsenal is also a communications device. Therefore, if a single LAWS, human, aircraft, or drone, is able to receive a communication from outside the contested zone, they would be able to relay said message to everyone on the network using alternate communications. This plan is akin to the modern cellular network, where a device communicates with the network, not necessarily one particular tower or receiver. Key to this alternative too is redundancy, meaning that the communications network needs to be built so that there is more than one way to communicate with a LAWS, and more than one way to confirm its target.

Mosaic Warfare

Mosaic Warfare is a DARPA initiative that places a premium on seeing battle as an emergent, complex system, and aims to use large amounts of low-cost units and weapon systems alongside other electronic and cyber capabilities to overwhelm adversaries, and force their military system to collapse.

The central idea is to be cheap, fast, lethal, flexible, and scalable. It's called mosaic warfare because the same pieces of a mosaic can be rearranged to create any picture, as opposed to now, where most military weapon systems are more like puzzle pieces, designed for, and only fitting into, a specific picture. Key to mosaic warfare is the ability for all the pieces to be able to talk to one another. (Jensen & Paschkewitz, 2019)

(4) Assign LAWS targets that can only be military targets and allow them to operate independently in accordance with prior orders once communications are lost.

LAWS programmed to attack only military targets—such as the Harpy, which is designed only to attack radar sites—means it is unlikely to attack civilians or civilian infrastructure. Therefore,

giving LAWS narrow missions will ensure that key military targets such as radar, and aircraft can be attacked using the most effective weapons in the US Navy's arsenal. By narrowing the mission so much, commanders will also be exerting reasonable control over the LAWS they send into an electromagnetic spectrum contested environment.

VI. Criteria for Evaluation

a) Criteria

In *Section VII: Findings*, the alternatives from Section V will be evaluated on the following criteria:

Lethality:

Will the LAWS help the US Navy win the battle they are fighting? This is the most important question of any new weapon system. The alternatives described will be evaluated on the presence of the LAWS on the battlefield, the redundancy of communication, and the complexity of the LAWS themselves, with more complexity making them less effective because they will be more likely to break down or malfunction, and more communication making them more effective because they will be able to receive orders and respond in real time to changes in the battlefield situation.

Chance for Harm to US Service Members & Non-combatants:

This potential exists in all weapons systems, however LAWS are a special kind of threat in this regard, as they are so complex that no one person will be able to understand every part of how they work, nor will a person, or even another computer system be able to predict how they might malfunction or break down. This criterion will be evaluated through the complexity of the proposed systems, the presence of the LAWS on the battlefield, and the redundancy of communications.

Cost:

The three most important things one needs to fight a war are money, money, and money. Even as the technology that underwrites them matures, becomes more widespread, and becomes cheaper, LAWS will not be cheap weapon systems. Any plan that will obviously attrite LAWS at a high rate will be considered cost ineffective, as will a plan that makes them overly complicated and in need of constant maintenance cycles, repair, and upgrades.

But how much will this actually cost?

These weapons are being developed right now, and most information about their development is highly classified, incomplete, or unknown. The National Security Commission on Artificial Intelligence spoke to the implications of LAWS, but did not put a price tag on their development—though they did recommend **\$8 billion go towards AI R&D** at the Department of Defense (however this includes all AI enabled systems, not just LAWS). (Schmidt, et al, 732)

Meanwhile, costs for LAWS already in use are as follows:

Weapon	Country of Origin	Cost per unit
Harpy	Israel	\$70,000
KUB-BLA	Russia	Less than \$70,000
Switchblade	USA	\$6,000

(I could find no information about the cost of the Turkish-made Kargu-2)

However, given that the cost of Reaper drones have more than doubled since they were first introduced in 2008—from \$14 million to \$32 million—it is only reasonable to expect that the costs will not remain where they are now. (Axe, 2021) (Aitken, 2022) (Hambling, 2020)

Control:

Just as commanders of today want to know that their subordinates are making decisions and taking actions in accordance with their intent, the commanders of tomorrow will want to know that their LAWS are acting in accordance with their orders, and that, in accordance with DoDD 3000.09, they have reasonable control over their weapons system. This criterion will be evaluated on communications systems redundancy and complexity of the weapon system.

b) Scale

All criteria will be evaluated on a 1–5 point scale to the tenth place with 5 being preferable to 1, all criteria will be weighted evenly, and the total of those evaluations displayed on the Outcomes Matrix. The alternative with the highest total evaluation will be recommended.

For criterion (2) *Potential for harm to US Service Members & Non-combatants*, a 5 will mean less potential for harm to US service members and non-combatants than a 1, and for criterion (3) *Cost*, a 5 will mean lower costs than a 1.

VII. Findings & Recommendation

The alternatives from *Section V* will now be evaluated with the criteria from *Section VI*.

Alternative 1: Recall LAWS when communications are lost.

Lethality: 3.5

This alternative would make LAWS effective weapon systems only under certain conditions on the battlefield. Communications can be lost due to any number of circumstances—weather, enemy interference, human error, or equipment breakdown—and in those moments LAWS would remove themselves from the battlefield in order to reestablish communications. This does not mean that they need to be completely removed from the battlefield—after all, helicopters, drones, and fixed wing aircraft are more than capable of hitting targets from their holding areas—but it does mean that they might leave areas of operation unexpectedly, or be forced by targeted enemy interference to leave.

Potential for harm to US Service Members & Non-combatants: 4.4

If every part of a LAWS operation—searching for, identifying, choosing to attack, and attacking targets—are all taking place under the supervision of a human, then the potential for harm will be about what it was in Iraq, Afghanistan, Libya and other places where the US was identifying targets using satellite and drone imagery.

Cost: 3.2

This alternative has a moderate cost because adding these instructions to the LAWS as they are being built will not be a great change from the cost of building them already. Additional costs might come from commanders demanding additional communications assets to keep their LAWS closer to the battlefield, but that has less to do with the LAWS themselves.

Control: 3.5

This alternative will keep the LAWS under strict human control at all times, and ensure they are never operating outside of the direction of their commander. While they will still be able to pursue their own attack patterns, and discern targets, there will always be a human looking at what they are looking at, ready to pull them off the attack if need be. However, there will be times when the LAWS are out of communications with their human commanders—traveling to their reconnection points—leaving them vulnerable to unsupervised mishap.

Alternative 2: Send US Navy Sailors downrange with LAWS to maintain line of sight communication

Lethality: 4.9

This “centaur” combination of the unique abilities of artificial intelligence systems and the complex reasoning that only the human mind is capable of. This combination of human reasoning and machine speed will be decisive more often than not when it is employed on a battlefield, and will be able to navigate the ever-shifting complexities of the gray zone and modern warfare better than either a LAWS or a human combatant would individually.

Potential for harm to US Service Members & Non-combatants: 2.1

The potential for harm to US service members will remain high because they will still be in harm’s way on the battlefield, however, they will fighting alongside LAWS so they will have an advantage over unsupported humans, and not be in critical danger from those adversaries who also have LAWS. It is likely though that the US servicemembers operating with the LAWS in an electromagnetic spectrum contested environment will also be cut off from long distance communications.

Cost: 1.9

This will be an expensive alternative because not only will the LAWS have to be developed, but the humans will have to be trained to fight with the LAWS, and the LAWS will have to be trained to fight with the humans.

Control: 4.9

Humans having eyes on, and almost constant contact with LAWS substantially reduces the risk of the LAWS ‘going rogue’ and adversely affecting the mission.

Alternative 3: Operate LAWS within a mesh network of communications to maintain contact at all times.

Lethality: 4.6

Under this alternative, LAWS will be able to operate in any environment, and there will always be some form of communication back to their command, even if it is hundreds of miles away—much like the control of RPAs in Iraq and Afghanistan. They will be fully able to fight in their creative, unorthodox ways, while still operating under the supervision of their human commander. Finally, LAWS will not only be controlled by humans in the rear, but those on the front lines with them as well creating the effective human-machine “centaur.”

Potential for harm to US Service Members & Non-combatants: 4.1

While some US servicemembers will still be on the battlefield and in harm's way, fewer of them will be needed, and those that are there will be in tight control over the LAWS.

Cost: 1.2

It will be expensive to build, maintain, protect, upgrade, and merge new weapon systems into this network.

Control: 4.7

With so much redundancy built into the system, it will take great deal of disruption to remove the LAWS from commander's control and human oversight.

Alternative 4: Assign LAWS targets that can only be military targets and allow them to operate independently in accordance with prior orders once communications are lost.

Lethality: 4.0

Assuming that LAWS are given clear instructions, allowing them to operate independently should enable them to accomplish their mission when communications back to a human commander are degraded. Furthermore, if sailors operating in the same area of operations are briefed on the mission of LAWS, then they will be able to deconflict. This will give a small dose of predictability to an otherwise fairly unpredictable technology.

Potential for harm to US Service Members & Non-combatants: 2.0

The afore mentioned predictability will make it easier for US servicemembers who are both aware of the mission of LAWS in their area of operations, and able to avoid them, to avoid being attacked by them. However, given the inherent complexity of both LAWS and the modern battlefield, if a LAWS suffers a malfunction, there will be no way to retake control over the weapon system. Finally, giving them only military targets might seem like a fool proof way to reduce the chances of serious harm, but on a modern battlefield, where so much is obfuscated and unclear, LAWS will be more likely to mistake civilians for military and vice versa because they lack the complex reasoning of the human mind, and will be unable to communicate with a human to help them discern otherwise.

Cost: 2.5

This would mean no serious changes to the ways that LAWS are being produced at the moment, and while still expensive, would keep costs somewhat reasonable.

Control: 2.5

Conditions on the battlefield—especially on a modern battlefield—often change rapidly. LAWS who are “set loose” will not be able to respond meaningfully to changes in weather, enemy

action, friendly action, civilian action, or political action in an electromagnetic spectrum contested environment. In today's hyperconnected world, this inability to adjust to sudden changes in the military or political situation could have disastrous effects.

Outcomes Matrix:

Alternatives	Criteria (1 – 5)				
	<i>Lethality</i>	<i>Harm to US Personnel</i>	<i>Cost</i>	<i>Control</i>	<i>Total Score</i>
<i>Recall</i>	3.5	4.4	3.2	3.5	14.6
<i>Go With</i>	4.9	2.1	1.9	4.9	13.8
<i>Mesh Network</i>	4.6	4.2	1.2	4.7	14.7
<i>Only Military Targets</i>	4.0	2.0	2.5	2.5	11.0

Recommendation: *Alternative 3: Operate LAWS within a mesh network of communications to maintain contact at all times*

Despite being the most expensive option, the mesh network offers the lethality of the human-machine centaur with the control necessary in the modern battlefield, while still reducing the risk to sailors. It also reduces the chance of such brittle technology suffering a mishap—either a forced error due to an attack or a malfunction—while it has lost communication with its commander. What is given about all military technology is that it will break. What is not given about LAWS is how, when, or under what circumstances they will break. There need to be backstops on these weapon systems. Besides, it is extremely difficult to knock out all communications across the entire spectrum for a long period of time. So much redundancy will be able to overcome an attack.

VIII: Implementation

This recommendation will be neither simple nor straightforward to implement. The Navy does not own the electromagnetic spectrum, so it will have to work within the frequencies given to it by the Federal Communications Commission. As it does not manufacture LAWS, computers, or communications equipment, it will have to coordinate with manufacturers who are also supplying to different customers, both within the DoD and internationally, and it will have to demand certain capabilities and be prepared to not pay or accept equipment that will be obsolete on a twenty-first century battlefield. Finally, the rapid rate of innovation, and invention in the fields of computer science, artificial intelligence, and communications means that the solutions of today quickly become the liabilities of tomorrow. It will take constant investment, reinvention, and buy-in to maintain the robust communications network that is able to successfully maintain control over LAWS in an electromagnetic spectrum contested environment.

The obvious stakeholders in this are the sailors who will be operating on a twenty-first century battlefield with LAWS. If LAWS are able to be controlled in an electromagnetic spectrum contested environment then they will benefit either by not having to go onto the aforementioned battlefield—because fewer fighters are needed—or being able to utilize the LAWS they have trained to fight with even though most communications are down. Additional stakeholders include the people they will be protecting by fighting, and finally, the reputation of the Navy. This is a completely foreseeable problem. Military communications have been getting disrupted since the dawn of war, but for the first time in history, the receiver of those communications will not be another human being who can infer, calculate, and understand the situation the way only a human can. It will be a machine that is extremely good at doing only what it has been programmed to do. “We couldn’t talk to it, so it just did what it was programmed,” will not be an acceptable answer when one of the Navy’s LAWS attacks the wrong target or commits a war crime.

I imagine that the afore-mentioned stakeholders will be accepting of this implementation in theory, but not in practice. The various military specialties take pride in being who they are. While they all coordinate constantly, this will be one of those initiatives where everyone has to feel like it is their idea. This is where you, Dr. Sam Tangredi, come in. As a Professor at the Naval War College you can educate not only your students, but others across the service on the coming problem, and how to fix it. This is not a small problem, and the solution will not be easy or cheap, but before it can begin there needs to be buy in from across the entire Department of the Navy.

The list of things that could go wrong is borderline infinite. As I have stated many times, one of the biggest concerns about LAWS is that they are so complex it is impossible to predict when and how they will break. It is a given that they will break, and it is a certainty that communications

on a twenty-first century battlefield will be disrupted. Worst-case scenarios in this regard mean that a malfunction of the LAWS causes them to attack the wrong targets—civilians, or US military personnel or allies—or choose not to attack the correct targets. Either way, this means that constant oversight of their operations—even when communications are being disrupted—is essential to ensure that by their actions and inactions they are working towards the mission of their commander.

In conclusion, implementing the above recommendation will not be easy, straightforward, or simple, but it remains essential. The positive potential for LAWS on the modern battlefield is enormous, but the negative potential is comparably sized. It is necessary that the US Navy plan for how it will maintain positive control over LAWS in an electromagnetic spectrum contested environment now, so it will be able to employ them effectively when the time comes.

What this might actually look like...

Is rather than having two US Navy aviators fly one aircraft, they flew one hundred... And instead of having a US Navy Captain command one ship, what if they commanded twenty, plus ten submarines, plus thirty more aircraft...

That's what this could be. A collection of autonomous weapons—aircraft, ships, submarines—commanded by a human who is there on the front line with them. Human identifies target, human orders LAWS to attack target, target is destroyed. That's one, or only several humans, doing the fighting that hundreds, or even thousands of humans used to do, with weapons more powerful and accurate than those previous generations of sailors could dream of.

Works Cited:

Atherton, K. (2021, August 4). Loitering munitions preview the autonomous future of warfare. *Brookings*. <https://www.brookings.edu/techstream/loitering-munitions-preview-the-autonomous-future-of-warfare/>

Axe, D. (2021, November 9). *Take a Look at Russia's New "Suicide Drones"* [Text]. The National Interest; The Center for the National Interest. <https://nationalinterest.org/blog/reboot/take-look-russias-new-suicide-drones-195929>

Bergman, R., & Fassihi, F. (2021, September 18). The Scientist and the A.I.-Assisted, Remote-Control Killing Machine. *The New York Times*. <https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html>

Blanken, Thaxton, & Alexander. (2018, February 27). *Shock of the Mundane: The Dangerous Diffusion of Basic Infantry Tactics*. War on the Rocks. <https://warontherocks.com/2018/02/shock-of-the-mundane-the-dangerous-diffusion-of-basic-infantry-tactics/>

Brose, C. (2020). *The kill chain: Defending America in the future of high-tech warfare* (First edition). Hachette Books.

Cheng, A. (n.d.). 'Killer robots' may be coming. New Zealand wants to stop them. *Washington Post*. Retrieved April 7, 2022, from <https://www.washingtonpost.com/world/2021/12/01/new-zealand-killer-robots-autonomous-weapons-law/>

Carey, S. (2020, May 13). *What is Chaos Monkey? Chaos engineering explained*. InfoWorld. <https://www.infoworld.com/article/3543233/what-is-chaos-monkey-chaos-engineering-explained.html>

Clay, M. (2021, January 22). *To Rule the Invisible Battlefield: The Electromagnetic Spectrum and Chinese Military Power*. War on the Rocks. <http://warontherocks.com/2021/01/to-rule-the-invisible-battlefield-the-electromagnetic-spectrum-and-chinese-military-power/>

Colchester, M. (n.d.). *U.K. Says Russian Mercenary Group Aims to Assassinate Ukraine's President*—WSJ. Retrieved April 4, 2022, from <https://www.wsj.com/articles/u-k-says-russian-mercenary-group-aims-to-assassinate-ukraines-president-11648137870>

Conger, K. (2021, October 5). Facebook says its outage was caused by a cascade of errors. *The New York Times*. <https://www.nytimes.com/2021/10/05/technology/facebook-outage-cause.html>

Corera, G. (2022, March 25). Russia hacked Ukrainian satellite communications, officials believe. *BBC News*. <https://www.bbc.com/news/technology-60796079>

Cyberlaw. (2021, September 17). *Cyber attacks against Estonia (2007)*. International Cyber Law: Interactive Toolkit. [https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_\(2007\)](https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007))

Dawes, J. (n.d.). *UN fails to agree on "killer robot" ban as nations pour billions into autonomous weapons research*. The Conversation. Retrieved April 7, 2022, from

<http://theconversation.com/un-fails-to-agree-on-killer-robot-ban-as-nations-pour-billions-into-autonomous-weapons-research-173616>

De Vynck, Verma, & Baran. (n.d.). Exploding ‘kamikaze’ drones are ushering in a new era of warfare in Ukraine. *Washington Post*. Retrieved April 2, 2022, from

<https://www.washingtonpost.com/technology/2022/03/24/loitering-drone-ukraine/>

Erickson, A. S., & Kennedy, C. M. (2022, March 23). *China’s Maritime Militia*.

<https://www.foreignaffairs.com/articles/china/2016-06-23/chinas-maritime-militia>

Friedman, T. L. (2022, April 3). Opinion | Putin Had No Clue How Many of Us Would Be Watching. *The New York Times*. <https://www.nytimes.com/2022/04/03/opinion/ukraine-russia-wired.html>

Gelzis & Emmott. (2017, October 5). Russia may have tested cyber warfare on Latvia, Western officials say. *Reuters*. <https://www.reuters.com/article/us-russia-nato-idUSKBN1CA142>

Gent, E. (2021, March 11). *US Air Force is guarding against electromagnetic pulse attacks. Should we worry?* Livescience.Com. <https://www.livescience.com/air-force-emp-attacks-protection.html>

Glenny, M. (2008). *McMafia: A journey through the global underworld*. Anansi.

Hambling, D. (2020, June 12). News: Why The Air Force Needs A Cheaper Reaper. *Navmar Applied Sciences Corporation*. <https://www.nasc.com/why-the-air-force-needs-a-cheaper-reaper/>

Jensen, B., & Paschkewitz, J. (2019, December 23). *Mosaic Warfare: Small and Scalable are Beautiful*. War on the Rocks. <https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/>

Jewkes & Vukmanovic. (2017, May 11). Suspected Russia-backed hackers target Baltic energy networks. *Reuters*. <https://www.reuters.com/article/us-baltics-cyber-insight-idUSKBN1871W5>

Karber, P. (2015, July 8). *Karber RUS-UKR War Lessons Learned*.

Katz, R. (n.d.). *Neo-Nazis are exploiting Russia’s war in Ukraine for their own purposes—The Washington Post*. Retrieved April 4, 2022, from <https://www.washingtonpost.com/outlook/2022/03/14/neo-nazi-ukraine-war/>

Kilcullen, D. (2020). *The dragons and the snakes: How the rest learned to fight the West*. Hurst & Company.

Kofman, M. (2017, February 16). *A Comparative Guide to Russia’s Use of Force: Measure Twice, Invade Once*. War on the Rocks. <https://warontherocks.com/2017/02/a-comparative-guide-to-russias-use-of-force-measure-twice-invade-once/>

Lerman, R., & Zakrzewski, Cat. (n.d.). Elon Musk’s Starlink is keeping Ukrainians online when traditional Internet fails. *Washington Post*. Retrieved April 4, 2022, from <https://www.washingtonpost.com/technology/2022/03/19/elon-musk-ukraine-starlink/>

McFate, S. (2017). *The Modern Mercenary: Private Armies and What They Mean for World Order*. Oxford University Press, Incorporated. <https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5045694>

McFate, S. (2019). *The new rules of war: How America can win- against Russia, China and other threats*.

The Truth About Algorithms | Cathy O’Neil—YouTube. (2018, October 17).
<https://www.youtube.com/watch?v=heQzqX35c9A&t=31s>

O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy* (First edition). Crown.

Payne, K. (2021). *I, warbot: The dawn of artificially intelligent conflict*. Hurst & Company.

Piper, K. (2020, February 14). *It’s 2020. Where are our self-driving cars?* Vox.
<https://www.vox.com/future-perfect/2020/2/14/21063487/self-driving-cars-autonomous-vehicles-waymo-cruise-uber>

Roche, C. (2016, November 30). *Assad Regime Militias and Shi’ite Jihadis in the Syrian Civil War*. Bellingcat. <https://www.bellingcat.com/news/mena/2016/11/30/assad-regime-militias-and-shiite-jihadis-in-the-syrian-civil-war/>

Romesha, C. (2016). *Red Platoon: A true story of American valor*. Dutton.

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war* (First edition). W. W. Norton & Company.

Schneider, T. (n.d.). *The Decay of the Syrian Regime is Much Worse Than You Think*. Retrieved April 4, 2022, from <https://warontherocks.com/2016/08/the-decay-of-the-syrian-regime-is-much-worse-than-you-think/>

Schmidt, E. (n.d.). *2021 Final Report: National Commission on Artificial Intelligence*. NSCAI. <https://www.nscai.gov/2021-final-report/>

Schneier, B., & Wheeler, T. (n.d.). *Hacked drones and busted logistics are the cyber future of warfare*. Retrieved December 10, 2021, from <https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>

Shapiro, A. (2018, April 23). *Autonomous Weapons Would Take Warfare To A New Domain, Without Humans*. NPR.
<https://www.npr.org/sections/alltechconsidered/2018/04/23/604438311/autonomous-weapons-would-take-warfare-to-a-new-domain-without-humans>

Stern, D. (n.d.). *Zelensky accuses Russia of plotting a coup against him; Kremlin denies claim—The Washington Post*. Retrieved April 4, 2022, from https://www.washingtonpost.com/world/europe/ukraine-zelensky-russia-coup/2021/11/26/16e51c80-4e0d-11ec-a7b8-9ed28bf23929_story.html

Tidy, J. (2022, March 20). *Anonymous: How hackers are trying to undermine Putin*. BBC News. <https://www.bbc.com/news/technology-60784526>

Tourangeau, S. (n.d.). *Denial of Spectrum Denial: The EW Gap That Should Worry Us All—Association of Old Crows*. Retrieved November 4, 2021, from <https://www.crows.org/news/389518/Denial-of-Spectrum-Denial-The-EW-Gap-That-Should-Worry-Us-All.htm>

Tourangeau, S., & Smith, D. (n.d.). *Denial of Spectrum Denial: NATO's EW Worry*. Joint Air Power Competence Centre. Retrieved November 4, 2021, from <https://www.japcc.org/denial-of-spectrum-denial-natos-ew-worry/>

Trevithick, J. (n.d.). *Russia Jammed Phones and GPS in Northern Europe During Massive Military Drills*. The Drive. Retrieved October 13, 2021, from <https://www.thedrive.com/the-war-zone/15194/russia-jammed-phones-and-gps-in-northern-europe-during-massive-military-drills>

Verini, J. (2019). *They Will Have to Die Now: Mosul and the Fall of the Caliphate*.

West, D. M., & Allen, J. R. (2020). *Turning point: Policymaking in the era of artificial intelligence*. Brookings Institution Press.

Zeitchik, S. (n.d.). The future of warfare could be a lot more grisly than Ukraine. *Washington Post*. Retrieved April 7, 2022, from <https://www.washingtonpost.com/technology/2022/03/11/autonomous-weapons-geneva-un/>

Bibliography:

A French Opinion on the Ethics of Autonomous Weapons. (2021, June 2). War on the Rocks. <https://warontherocks.com/2021/06/the-french-defense-ethics-committees-opinion-on-autonomous-weapons/>

A State Department for the Digital Age. (2021, June 21). War on the Rocks. <https://warontherocks.com/2021/06/a-state-department-for-the-digital-age/>

AI and Irregular Warfare: An Evolution, Not a Revolution. (2019, October 31). War on the Rocks. <https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/>

AI for Peace. (2019, December 13). War on the Rocks. <https://warontherocks.com/2019/12/ai-for-peace/>

AI Principles. (n.d.). Future of Life Institute. Retrieved July 22, 2021, from <https://futureoflife.org/ai-principles/>

Allen, D. M. W. and J. R. (2018, April 24). How artificial intelligence is transforming the world. *Brookings*. <https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/>

America's Counterterrorism Wars. (n.d.). New America. Retrieved October 26, 2021, from <http://newamerica.org/international-security/reports/americas-counterterrorism-wars/>

An Enduring Impasse on Autonomous Weapons. (2020, September 28). Just Security. <https://www.justsecurity.org/72610/an-enduring-impasse-on-autonomous-weapons/>

Battlefield Singularity. (n.d.). Retrieved October 13, 2021, from <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>

Comment: Artificial intelligence not ready for prime time. (2021, October 6). HeraldNet.Com. <https://www.heraldnet.com/opinion/comment-artificial-intelligence-not-ready-for-prime-time/>

DARPA Tiles Together a Vision of Mosaic Warfare. (2020, June 16). *Joint Air Power Competence Centre*. <https://www.japcc.org/darpa-tiles-together-a-vision-of-mosaic-warfare/>

Data Cleaning: Definition, Benefits, And How-To | Tableau. (n.d.). Retrieved April 2, 2022, from <https://www.tableau.com/learn/articles/what-is-data-cleaning>

Debunking the AI Arms Race Theory. (2021, June 28). Texas National Security Review. <https://tnsr.org/2021/06/debunking-the-ai-arms-race-theory/>

Drone Warfare. (n.d.). The Bureau of Investigative Journalism (En-GB). Retrieved October 26, 2021, from <https://www.thebureauinvestigates.com/projects/drone-war>

Engler, A. (2021, January 21). 6 developments that will define AI governance in 2021. *Brookings*. <https://www.brookings.edu/research/6-developments-that-will-define-ai-governance-in-2021/>

From Deception to Attrition: AI and the Changing Face of Warfare. (2020, February 18). War on the Rocks. <https://warontherocks.com/2020/02/from-deception-to-attrition-ai-and-the-changing-face-of-warfare/>

Homepage. (2021, October 20). *Lethal Autonomous Weapons*.
<https://autonomousweapons.org/>

Kallenborn, Z. (2021, October 5). Applying arms-control frameworks to autonomous weapons. *Brookings*. <https://www.brookings.edu/techstream/applying-arms-control-frameworks-to-autonomous-weapons/>

Opinion | In warfare, the future is now. (n.d.). *Washington Post*. Retrieved July 29, 2021, from <https://www.washingtonpost.com/opinions/2021/05/27/warfare-future-is-now/>

Policy Roundtable: Artificial Intelligence and International Security. (n.d.). Texas National Security Review. Retrieved July 21, 2021, from <https://tnsr.org/roundtable/policy-roundtable-artificial-intelligence-and-international-security/>

Russia may have used a killer robot in Ukraine. Now what? - Bulletin of the Atomic Scientists. (n.d.). Retrieved April 2, 2022, from <https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/>

Sacasas, L. M. (n.d.). *The Convivial Society*. Retrieved August 12, 2021, from <https://theconvivialsociety.substack.com/>

Sacasas, L. M. (2021, June 4). The Questions Concerning Technology [Substack newsletter]. *The Convivial Society*. <https://theconvivialsociety.substack.com/p/the-questions-concerning-technology>

Strategic Technology Office. (n.d.). Retrieved April 7, 2022, from <https://www.darpa.mil/about-us/offices/sto/more>

Tech Leaders Justify Project To Create Army Of AI-Controlled Bulletproof Grizzly Bears As Inevitable Part Of Progress. (n.d.). *The Onion*. Retrieved February 16, 2022, from <https://www.theonion.com/tech-leaders-justify-project-to-create-army-of-ai-contr-1848402815>

The Unplanned Costs of an Unmanned Fleet. (2021, December 28). *War on the Rocks*. <https://warontherocks.com/2021/12/the-unplanned-costs-of-an-unmanned-fleet/>

The U.S. says humans will always be in control of AI weapons. But the age of autonomous war is already here. (n.d.). *Washington Post*. Retrieved July 14, 2021, from <https://www.washingtonpost.com/technology/2021/07/07/ai-weapons-us-military/>

Types Of Machine Learning. (n.d.). Retrieved October 12, 2021, from <https://book.mlcompendium.com/types-of-machine-learning>

Was a flying killer robot used in Libya? Quite possibly. (2021, May 20). *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2021/05/was-a-flying-killer-robot-used-in-libya-quite-possibly/>

What is Mosaic Warfare? (n.d.). BAE Systems | United States. Retrieved April 7, 2022, from <https://www.baesystems.com/en-us/definition/mosaic-warfare>



Department of Defense **DIRECTIVE**

NUMBER 3000.09

November 21, 2012

Incorporating Change 1, May 8, 2017

USD(P)

SUBJECT: Autonomy in Weapon Systems

References: See Enclosure 1

1. **PURPOSE.** This Directive:

- a. Establishes DoD policy and assigns responsibilities for the development and use of autonomous and semi-autonomous functions in weapon systems, including manned and unmanned platforms.
- b. Establishes guidelines designed to minimize the probability and consequences of failures in autonomous and semi-autonomous weapon systems that could lead to unintended engagements.

2. **APPLICABILITY.** This Directive:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff (CJCS), the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).

(2) The design, development, acquisition, testing, fielding, and employment of autonomous and semi-autonomous weapon systems, including guided munitions that can independently select and discriminate targets.

(3) The application of lethal or non-lethal, kinetic or non-kinetic, force by autonomous or semi-autonomous weapon systems.

b. Does not apply to autonomous or semi-autonomous cyberspace systems for cyberspace operations; unarmed, unmanned platforms; unguided munitions; munitions manually guided by the operator (e.g., laser- or wire-guided munitions); mines; or unexploded explosive ordnance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.

(1) Systems will go through rigorous hardware and software verification and validation (V&V) and realistic system developmental and operational test and evaluation (T&E) in accordance with the guidelines in Enclosure 2. Training, doctrine, and tactics, techniques, and procedures (TTPs) will be established. These measures will ensure that autonomous and semi-autonomous weapon systems:

(a) Function as anticipated in realistic operational environments against adaptive adversaries.

(b) Complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement.

(c) Are sufficiently robust to minimize failures that could lead to unintended engagements or to loss of control of the system to unauthorized parties.

(2) Consistent with the potential consequences of an unintended engagement or loss of control of the system to unauthorized parties, physical hardware and software will be designed with appropriate:

(a) Safeties, anti-tamper mechanisms, and information assurance in accordance with DoD Instruction 8500.01 (Reference (a)).

(b) Human-machine interfaces and controls.

(3) In order for operators to make informed and appropriate decisions in engaging targets, the interface between people and machines for autonomous and semi-autonomous weapon systems shall:

(a) Be readily understandable to trained operators.

(b) Provide traceable feedback on system status.

(c) Provide clear procedures for trained operators to activate and deactivate system functions.

b. Persons who authorize the use of, direct the use of, or operate autonomous and semi-autonomous weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement (ROE).

c. Autonomous and semi-autonomous weapon systems intended to be used in a manner that falls within the policies in subparagraphs 4.c.(1) through 4.c.(3) will be considered for approval in accordance with the approval procedures in DoD Directive 5000.01 (Reference (b)), DoD Instruction 5000.02 (Reference (c)), and other applicable policies and issuances.

(1) Semi-autonomous weapon systems (including manned or unmanned platforms, munitions, or sub-munitions that function as semi-autonomous weapon systems or as subcomponents of semi-autonomous weapon systems) may be used to apply lethal or non-lethal, kinetic or non-kinetic force. Semi-autonomous weapon systems that are onboard or integrated with unmanned platforms must be designed such that, in the event of degraded or lost communications, the system does not autonomously select and engage individual targets or specific target groups that have not been previously selected by an authorized human operator.

(2) Human-supervised autonomous weapon systems may be used to select and engage targets, with the exception of selecting humans as targets, for local defense to intercept attempted time-critical or saturation attacks for:

(a) Static defense of manned installations.

(b) Onboard defense of manned platforms.

(3) Autonomous weapon systems may be used to apply non-lethal, non-kinetic force, such as some forms of electronic attack, against materiel targets in accordance with DoD Directive 3000.03E (Reference (d)).

d. Autonomous or semi-autonomous weapon systems intended to be used in a manner that falls outside the policies in subparagraphs 4.c.(1) through 4.c.(3) must be approved by the Under Secretary of Defense for Policy (USD(P)); the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); and the CJCS before formal development and again before fielding in accordance with the guidelines in Enclosure 3, References (b) and (c), and other applicable policies and issuances.


e. International sales or transfers of autonomous and semi-autonomous weapon systems will be approved in accordance with existing technology security and foreign disclosure requirements and processes, in accordance with DoD Directive 5111.21 (Reference (e)).

5. RESPONSIBILITIES. See Enclosure 4.

6. RELEASABILITY. Cleared for public release. This Directive is available on the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update organizational titles and references for accuracy.

8. EFFECTIVE DATE. This Directive is effective November 21, 2012.



Ashton B. Carter
Deputy Secretary of Defense

Enclosures

1. References
2. V&V and T&E of Autonomous and Semi-Autonomous Weapon Systems
3. Guidelines for Review of Certain Autonomous or Semi-Autonomous Weapon Systems
4. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
- (b) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003, as amended
- (c) DoD Instruction 5000.02, "Operation of the Defense Acquisition System,"
January 7, 2015, as amended
- (d) DoD Directive 3000.03E, "DoD Executive Agent for Non-Lethal Weapons (NLW), and
NLW Policy," April 25, 2013, as amended
- (e) DoD Directive 5111.21, "Arms Transfer and Technology Release Senior Steering Group
and Technology Security and Foreign Disclosure Office," October 14, 2014
- (f) DoD Directive 2311.01E, "DoD Law of War Program," May 9, 2006, as amended
- (g) DoD Directive 1322.18, "Military Training," January 13, 2009, as amended

ENCLOSURE 2

V&V AND T&E OF AUTONOMOUS AND SEMI-AUTONOMOUS WEAPON SYSTEMS

To ensure autonomous and semi-autonomous weapon systems function as anticipated in realistic operational environments against adaptive adversaries and are sufficiently robust to minimize failures that could lead to unintended engagements or to loss of control of the system, in accordance with subparagraph 4.a.(1) above the signature of this Directive:

a. Systems will go through rigorous hardware and software V&V and realistic system developmental and operational T&E, including analysis of unanticipated emergent behavior resulting from the effects of complex operational environments on autonomous or semi-autonomous systems.

b. After initial operational test and evaluation (IOT&E), any further changes to the system will undergo V&V and T&E in order to ensure that critical safety features have not been degraded.

(1) A regression test of the software shall be applied to validate critical safety features have not been degraded. Automated regression testing tools will be used whenever feasible. The regression testing shall identify any new operating states and changes in the state transition matrix of the autonomous or semi-autonomous weapon system.

(2) Each new or revised operating state shall undergo integrated T&E to characterize the system behavior in that new operating state. Changes to the state transition matrix may require whole system follow-on operational T&E, as directed by the Director of Operational Test and Evaluation (DOT&E).

ENCLOSURE 3

GUIDELINES FOR REVIEW OF CERTAIN AUTONOMOUS OR SEMI-AUTONOMOUS
WEAPON SYSTEMS

1. Autonomous or semi-autonomous weapon systems intended to be used in a manner that falls outside the policies in subparagraphs 4.c.(1) through 4.c.(3) above the signature of this Directive must be approved by the USD(P), USD(AT&L), and CJCS before formal development and again before fielding.

a. Before a decision to enter into formal development, the USD(P), USD(AT&L), and CJCS shall ensure:

(1) The system design incorporates the necessary capabilities to allow commanders and operators to exercise appropriate levels of human judgment in the use of force.

(2) The system is designed to complete engagements in a timeframe consistent with commander and operator intentions and, if unable to do so, to terminate engagements or seek additional human operator input before continuing the engagement.

(3) The system design, including safeties, anti-tamper mechanisms, and information assurance in accordance with Reference (a), addresses and minimizes the probability or consequences of failures that could lead to unintended engagements or to loss of control of the system.

(4) Plans are in place for V&V and T&E to establish system reliability, effectiveness, and suitability under realistic conditions, including possible adversary actions, to a sufficient standard consistent with the potential consequences of an unintended engagement or loss of control of the system.

(5) A preliminary legal review of the weapon system has been completed, in coordination with the General Counsel of the Department of Defense (GC, DoD) and in accordance with References (b) and (c), DoD Directive 2311.01E (Reference (f)), and, where applicable, Reference (d).

b. Before fielding, the USD(P), USD(AT&L), and CJCS shall ensure:

(1) System capabilities, human-machine interfaces, doctrine, TTPs, and training have demonstrated the capability to allow commanders and operators to exercise appropriate levels of human judgment in the use of force and to employ systems with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable ROE.

(2) Sufficient safeties, anti-tamper mechanisms, and information assurance in accordance with Reference (a) have been implemented to minimize the probability or consequences of failures that could lead to unintended engagements or to loss of control of the system.

(3) V&V and T&E assess system performance, capability, reliability, effectiveness, and suitability under realistic conditions, including possible adversary actions, consistent with the potential consequences of an unintended engagement or loss of control of the system.

(4) Adequate training, TTPs, and doctrine are available, periodically reviewed, and used by system operators and commanders to understand the functioning, capabilities, and limitations of the system's autonomy in realistic operational conditions.

(5) System design and human-machine interfaces are readily understandable to trained operators, provide traceable feedback on system status, and provide clear procedures for trained operators to activate and deactivate system functions.

(6) A legal review of the weapon system has been completed, in coordination with the GC, DoD, and in accordance with References (b), (c), (f), and, where applicable, Reference (d).

2. The USD(P), USD(AT&L), and CJCS may request a Deputy Secretary of Defense waiver for the requirements outlined in section 1 of this enclosure, with the exception of the requirement for a legal review, in cases of urgent military operational need.

ENCLOSURE 4
RESPONSIBILITIES

1. USD(P). The USD(P) shall:

- a. Provide policy oversight for the development and employment of autonomous and semi-autonomous weapon systems.
- b. In coordination with the USD(AT&L) and CJCS, review and consider for approval weapon systems submitted in accordance with paragraph 4.d. above the signature of this Directive.
- c. Review, as necessary, the appropriateness of guidance established in accordance with this Directive given the continual advancement of new technologies and changing warfighter needs.
- d. Approve the DoD position on international sales or transfers of autonomous and semi-autonomous weapon systems in accordance with existing technology security and foreign disclosure requirements and processes.

2. USD(AT&L). The USD(AT&L) shall:

- a. Provide principal oversight responsibility for the establishment and enforcement of standards for testing, safety and reliability, hardware and software V&V, anti-tamper mechanisms, and information assurance in accordance with Reference (a), for autonomous and semi-autonomous weapon systems in order to minimize the probability and consequences of failures that could lead to unintended engagements or to loss of control of the system.
- b. Provide principal oversight responsibility for the establishment of science and technology and research and development priorities for autonomy in weapon systems, including the development of new methods of V&V and T&E.
- c. Oversee adequate developmental testing of autonomous and semi-autonomous weapon systems to assess the risk of failures that could lead to unintended engagements or to loss of control of the system.
- d. In coordination with the USD(P) and CJCS, review and consider for approval weapon systems submitted in accordance with paragraph 4.d. above the signature of this Directive.

3. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) shall, consistent with DoD Directive 1322.18 (Reference (g)), oversee and provide policy for:

a. Individual military training programs for the Total Force relating to autonomous and semi-autonomous weapon systems.

b. Individual and functional training programs for military personnel and the collective training programs of military units and staffs relating to autonomous and semi-autonomous weapon systems.

4. DOT&E. The DOT&E shall:

a. Provide principal oversight responsibility for the development of realistic operational T&E standards for semi-autonomous and autonomous weapon systems, including standards for T&E of any changes to the system following IOT&E, in accordance with subparagraph 4.a.(1) above the signature of this Directive and Enclosure 2.

b. Evaluate whether semi-autonomous and autonomous weapon systems under DOT&E oversight have met sufficient V&V and T&E in realistic operational conditions, including potential adversary action, in order to minimize the probability and consequences of failures that could lead to unintended engagements or to loss of control of the system to unauthorized parties.

5. GC, DoD. The GC, DoD, shall, in accordance with References (b), (c), (f), and, where applicable, Reference (d), provide for guidance in and coordination of legal reviews of weapon systems submitted in accordance with paragraph 4.d. above the signature of this Directive.

6. DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO, shall monitor, evaluate, and provide advice to the Secretary of Defense regarding information assurance for autonomous and semi-autonomous weapon systems, in accordance with subparagraph 4.a.(2)(a) above the signature of this Directive and Reference (a).

7. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS (ATSD(PA)). The ATSD(PA) shall coordinate and approve guidance on public affairs matters concerning autonomous and semi-autonomous weapon systems and their use.

8. SECRETARIES OF THE MILITARY DEPARTMENTS; COMMANDER, U.S. SPECIAL OPERATIONS COMMAND (USSOCOM); AND THE HEADS OF THE DEFENSE AGENCIES AND DoD FIELD ACTIVITIES. The Secretaries of the Military Departments; the Commander, USSOCOM; and the Heads of the Defense Agencies and DoD Field Activities shall:

a. Develop and implement employment concepts, doctrine, experimentation strategies, TTPs, training, logistics support, V&V, anti-tamper mechanisms, physical hardware and software-level safeties, information assurance in accordance with Reference (a), and

developmental and operational T&E appropriate for autonomous and semi-autonomous weapon systems.

(1) Design autonomous and semi-autonomous weapon systems in such a manner as to minimize the probability and consequences of failures that could lead to unintended engagements or to loss of control of the system.

(2) Perform rigorous and realistic developmental and operational T&E and V&V, including T&E of any changes to the system following IOT&E, in accordance with subparagraph 4.a.(1) above the signature of this Directive and Enclosure 2.

(3) Design autonomous and semi-autonomous weapon systems with sufficient safeties, anti-tamper mechanisms, and information assurance in accordance with subparagraph 4.a.(2) above the signature of this Directive and Reference (a).

(4) Design human-machine interfaces for autonomous and semi-autonomous weapon systems to be readily understandable to trained operators, provide traceable feedback on system status, and provide clear procedures for trained operators to activate and deactivate system functions, in accordance with subparagraph 4.a.(3) above the signature of this Directive.

(5) Certify that operators of autonomous and semi-autonomous weapon systems have been trained in system capabilities, doctrine, and TTPs in order to exercise appropriate levels of human judgment in the use of force and employ systems with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable ROE.

(6) Establish and periodically review training, TTPs, and doctrine for autonomous and semi-autonomous weapon systems to ensure operators and commanders understand the functioning, capabilities, and limitations of a system's autonomy in realistic operational conditions, including as a result of possible adversary actions.

b. Ensure that legal reviews of autonomous and semi-autonomous weapon systems are conducted in accordance with References (b), (c), (f) and, where applicable, Reference (d). Legal reviews should ensure consistency with all applicable domestic and international law and, in particular, the law of war.

c. Consider for support only those autonomous and semi-autonomous weapon systems that are technically feasible and that conform to this Directive. Submit to the USD(P), USD(AT&L), and CJCS for review, in accordance with paragraph 4.d. above the signature of this Directive, any autonomous or semi-autonomous weapon system intended to be used in a manner that falls outside the policies in subparagraphs 4.c.(1) through 4.c.(3) above the signature of this Directive before a decision to enter into formal development and again before fielding of any such system.

9. CJCS. The CJCS shall:

- a. Advise the Secretary of Defense on the capability needs and employment of autonomous and semi-autonomous weapon systems.
- b. Assess military requirements for autonomous and semi-autonomous weapon systems, including applicable key performance parameters and key system attributes.
- c. Develop and publish joint doctrine, as appropriate, to incorporate emerging capabilities of autonomous and semi-autonomous weapon systems.
- d. In coordination with the USD(P) and USD(AT&L), review and consider for approval autonomous weapon systems submitted in accordance with paragraph 4.d. above the signature of this Directive.

10. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands shall:

- a. Use autonomous and semi-autonomous weapon systems in accordance with this Directive and in a manner consistent with their design, testing, certification, operator training, doctrine, TTPs, and approval as autonomous or semi-autonomous systems.
- b. Employ autonomous and semi-autonomous weapon systems with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable ROE, in accordance with paragraph 4.b. above the signature of this Directive.
- c. Ensure that weapon systems are not employed or modified to operate in a manner that falls outside the policies in subparagraphs 4.c.(1) through 4.c.(3) above the signature of this Directive without specific approval in accordance with paragraph 4.d. above the signature of this Directive.
- d. Integrate autonomous and semi-autonomous weapon systems into operational mission planning.
- e. Through the CJCS, identify warfighter priorities and operational needs that may be met by autonomous and semi-autonomous weapon systems.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ATSD(PA)	Assistant to the Secretary of Defense for Public Affairs
CJCS	Chairman of the Joint Chiefs of Staff
DoD CIO	Department of Defense Chief Information Officer
DOT&E	Director of Operational Test and Evaluation
GC, DoD	General Counsel of the Department of Defense
IOT&E	initial operational test and evaluation
ROE	rules of engagement
T&E	test and evaluation
TTP	tactics, techniques, and procedures
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSOCOM	U.S. Special Operations Command
V&V	verification and validation

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this Directive.

automated regression testing. A type of regression testing that uses testing tools and repeatable test scripts.

autonomous weapon system. A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of

the weapon system, but can select and engage targets without further human input after activation.

electronic attack. Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

failures. An actual or perceived degradation or loss of intended functionality or inability of the system to perform as intended or designed. Failures can result from a number of causes, including, but not limited to, human error, human-machine interaction failures, malfunctions, communications degradation, software coding errors, enemy cyber attacks or infiltration into the industrial supply chain, jamming, spoofing, decoys, other enemy countermeasures or actions, or unanticipated situations on the battlefield.

human-supervised autonomous weapon system. An autonomous weapon system that is designed to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur.

operating state. A variable or vector reflecting the status of the system.

operator. A person who operates a weapon system.

regression testing. A type of software testing that seeks to uncover new deficiencies (i.e., regressions) in the existing functional and non-functional areas of a system created by changes to the software, including enhancements, patches, emergency transports, or configuration changes.

semi-autonomous weapon system. A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator. This includes:

Semi-autonomous weapon systems that employ autonomy for engagement-related functions including, but not limited to, acquiring, tracking, and identifying potential targets; cueing potential targets to human operators; prioritizing selected targets; timing of when to fire; or providing terminal guidance to home in on selected targets, provided that human control is retained over the decision to select individual targets and specific target groups for engagement.

“Fire and forget” or lock-on-after-launch homing munitions that rely on TTPs to maximize the probability that the only targets within the seeker’s acquisition basket when the seeker activates are those individual targets or specific target groups that have been selected by a human operator.

state transition matrix. A matrix that characterizes the ability of a system to transition from one operating state to another.

target selection. The determination that an individual target or a specific group of targets is to be engaged.

unintended engagement. The use of force resulting in damage to persons or objects that human operators did not intend to be the targets of U.S. military operations, including unacceptable levels of collateral damage beyond those consistent with the law of war, ROE, and commander's intent.

unmanned platform. An air, land, surface, subsurface, or space platform that does not have the human operator physically onboard the platform.

Appendix II: Chaos Engineering

Chaos engineering is the proactive way to contend with some of the problems that arise from complex systems. It is the discipline of experimenting on a system in order to build confidence in the system's capability to withstand turbulent conditions in operation. In essence, it is deliberately breaking different parts of the system (in a simulation) to see what sort of effects it will have on the rest of it, and building resiliency into the system from there. It began in 2010 with Netflix's program Chaos Monkey, and is generally used on software, but the principles are the same for all complex systems, and should be used to build resiliency in all US Navy and DoD software, and artificial intelligence enabled systems. (Carey, 2020)