REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
24-03-2021	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
Future Kill Chains: Harnessing Emerging Technology to Improve Marine Corps Warfighting

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Jesse T. Knight (Major)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
USMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The past eighteen years of counterterrorism and counter-insurgency operations have created a kill chain that is effective in low-intensity conflicts where the US Military enjoys a strategic overmatch against our adversaries. However, in a high-intensity, great power conflict against a peer competitor, this current paradigm would likely be too fragile and slow. Success in deterring or fighting a peer competitor in the INDOPACOM region will hinge upon forward-positioned commanders acting in a denied and degraded environment while rapidly employing fires in support of an overall naval campaign. To achieve this vision, technological improvements will be needed to facilitate the decentralized and rapid employment of the kill-chain cycle. Improvements must be made to each portion of the targeting cycle as well as our communications architecture to ensure the Marine Corps is prepared to make an impactful contribution to the overarching naval strategy.

15. SUBJECT TERMS
Kill-Chain, Technology, EABO, Fires.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	46	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Future Kill Chains: Harnessing Emerging
Technology to Improve Marine Corps Warfighting

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Jesse T. Knight

AY 2020-21

Mentor and Oral Defense Committee Member: Dr. Alex Heckmann
Approved: [signature]
Date: 24 MAR 2021
Oral Defense Committee Member: LtCol John Nash
Approved: [signature]
Date: 24 MAR 2021

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Future Kill Chains: Harnessing Emerging Technology to Improve Marine Corps Warfighting

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Major Jesse T. Knight

AY 2020-21

Mentor and Oral Defense Committee Member: _____
Approved: _____
Date: _____
Oral Defense Committee Member: _____
Approved: _____
Date: _____

DISCLAIMER

Executive Summary

Title: Future Kill Chains: Harnessing Emerging Technology to Improve Marine Corps Warfighting

Author: Major Jesse Knight, United States Marine Corps

Thesis: If the Marine Corps hopes to deter or fight a peer competitor, it must harness the power of emerging technologies to enhance the lethality and speed of its kill chain.

Discussion: The past eighteen years of counterterrorism and counter-insurgency operations have created a kill chain that is effective in low-intensity conflicts where the US Military enjoys a strategic overmatch against our adversaries. However, in a high-intensity, great power conflict against a peer competitor, this current paradigm would likely be too fragile and slow. Success in deterring or fighting a peer competitor in the INDOPACOM region will hinge upon forward-positioned commanders acting in a denied and degraded environment while rapidly employing fires in support of an overall naval campaign. To achieve this vision, technological improvements will be needed to facilitate the decentralized and rapid employment of the kill-chain cycle. Improvements must be made to each portion of the targeting cycle as well as our communications architecture to ensure the Marine Corps is prepared to make an impactful contribution to the overarching naval strategy.

Conclusion: The Marine Corps must not only aggressively seek new technologies that will aid the kill chain process, but also develop new and disruptive methods for technologies that already exist. Innovation must enable commanders to better decide target allocations, detect potential targets, deliver the appropriate munition, and assess their effects faster and more effectively than the enemy. To achieve this end, technology must be developed in a comprehensive and networked manner to ensure the greatest efficiency and adaptability to the future fight.

Table of Contents

Preface

The impetus for this paper began while I served as a Platoon Commander for 5th Air Naval Gunfire Liaison Company (5th ANGLICO) from 2017 to 2020 as we dissected the problem of conducting operations against a peer competitor in the South China Sea. During this period, it became obvious that our current system was not adequately equipped or designed for the future. Through my research, I have found a wealth of information concerning issues with the US military's kill chain process, technological developments, and potential solutions. However, room remains for assessments that attempt to tie all these things together into cogent work. Although the scope of this paper is necessarily limited by its writing in a brief, mid-career professional military education setting, it aims to complement the body of existing research by framing the issues in a structured and comprehensive approach. This effort endeavors less in contending to discover new technologies or implementation processes, but more as providing additional context for how emerging technologies might be integrated as a comprehensive whole, with a specific focus on a specific aspect of modern warfare—the kill chain.

I also find it important to bound my premise. Although I use a conflict in the South China Sea against the Chinese People's Liberation Army (PLA) as a framework, the venue is solely a vehicle to draw out key aspects of the chain process in a potential high-end conflict. Therefore, I have omitted certain aspects of the intelligence/counterintelligence fight which occur before kinetic conflict, do not fully address the US military's acquisitions process, and bypass certain logistic concerns. Although these aspects will be critical when fighting a peer adversary, this paper isolates these variables to distill and isolate analysis of the critical aspects of the kill chain. Additionally, among the many different US military targeting methodologies, this study uses the

D3A model outlined in Joint Publication 3-60, *Joint Targeting.* This method, broken down into its four distinct elements; Decide, Detect, Deliver, and Assess (D3A), is the most recognizable and simple way to illustrate the synergistic aspects of intelligence, maneuver, and fires in the prosecution of targets.

This paper also utilizes a "vignette" approach to vividly illustrate how the somewhat dry doctrinal and systems issues might play out in the real world. Vignettes, or notional scenarios, are useful "thought experiments" that translate the academic world into the actual operating environment and offer a simulated environment to play out alternative concepts. In particular, this paper first presents a vignette on how the existing kill chain might perform in a crisis today, and then, following the paper's development of concepts for how new technologies and practices might improve the US kill chain, concludes with a vignette on how those concepts would offer future forces a competitive advantage.

Lastly, it is important to thank those that helped me accomplish this work. I want to thank my wife and daughter for supporting me through the endless hours in my office required to research and write this paper. Also, LtCol Chad Grimmett, my Company Commander at 5th ANGLICO, who prompted me to begin thinking about a better kill chain process and provided me the latitude to explore many of these aspects during my time as his Operations Officer. Finally, my thesis advisor Dr. Richard Hegmann for providing much-needed structure to my process, and the valuable feedback required to shape and hone my prose.

Introduction

> *…after our victory in Operation Desert Storm. As victors, we made the classic error, learning the wrong lessons from our experience. We used victory to validate doctrine, tactics, and weapons that have prevailed against a particularly inept foe. We ignored the fact that nations from China to Serbia have been studying the conduct of war for a decade solely in order to devise counter strategies.*
>
> *-Admiral (Ret) Bill Owens*[1]

In 1999, a retired Marine general testified before Congress that "the days of armed conflict between nation-states are ending."[2] The following decades appeared to confirm this sentiment as America was drawn into "the long war" of counterterrorism and counterinsurgency operations against non-state actors. During this time, the US military enjoyed the advantages of maneuvering with relative impunity and operating with virtual superiority in all domains. Technological developments enabled US forces to exponentially increase their ability to gather situational awareness and maintain effective communications with all echelons of the battlefield. Continuously operating in the information environment while uncontested from a peer competitor has left the American military over-reliant on fragile communications pathways and an overabundance of information. In a high-intensity, great power conflict against a peer competitor, the current paradigm would likely be too fragile and slow.

The 2018 *National Defense Strategy* refocused American priorities toward great power competition.[3] Accordingly, the 38th Commandant of the Marine Corps published his *Commandant's Planning Guidance* wherein he affirms the challenges of the new security environment and outlines how the Marine Corps must conduct institutional change to become a

naval expeditionary force-in-readiness in support of fleet operations.[4] To effect this change, the Marine Corps has developed the Expeditionary Advanced Based Operations (EABO) service concept as an approach for conducting military operations against a peer competitor who employs significant Anti-Access Area Denial (A2AD) capabilities. While EABO does not provide detailed concepts of how a conflict will play out against a peer competitor, it establishes the framework by which expeditionary forces must be prepared to operate.

To deter or fight in the contested spaces of the Indo-Pacific region, the Marine Corps must be prepared to conduct actions inside the adversary's weapons engagement zone (WEZ). "Inside forces" like Marine EABs reassure allies and partners while contesting the space against China's coercion or influence. The byproduct of these actions likely means US forces will be contested in domains where they once enjoyed supremacy and dominance. Accordingly, the process of acquiring and prosecuting targets, referred to as the "kill chain," must be examined if the Marine Corps seeks to effectively contribute to an overall naval strategy. Current means to conduct this kill chain are outdated, susceptible to enemy electronic warfare (EW), and too slow. Emerging technology can aid our ability to **decide** what targets to engage, **detect** where these targets are located, **deliver** the appropriate munition on time, and properly **assess** the effects and impacts of these actions. Known as the D3A targeting process, this methodology will be utilized to describe and assess current and potential future kill chain effectiveness.[5]

Part I: The Pacing Threat and A2AD

> *[The People's Liberation Army] Active defense from Jiang to Xi has evolved to include a mix of offensive, defensive, and deterrent concepts encompassing operations further from China's periphery and also in the space and cyber domains. It is defensive at the strategic level of war but often offensive at the operational and tactical levels.*
>
> - PLA Operational Concepts[6]

Adversaries of the United State watched the Post-World War II era with concern as the American military built impressive financial, diplomatic, and military mechanisms enabling it to project power across the globe. In response to this paradigm shift, many countries developed multi-layered defensive systems designed to contest American supremacy of the air and sea domains.[7] This method is often referred to as Anti-Access/Area Denial or A2AD. While many actors employ this type of multi-layered maritime defense, "China has by far the greatest economic and technological capacity" to present a challenge to American military capabilities.[8] As such, both the US Secretary of Defense and the Commandant of the Marine Corps have identified China as the DOD's pacing threat, and have directed military personnel to study and eventually counter the People's Liberation Army's (PLA) A2AD capabilities.[9] For the remainder of this paper, Chinese A2AD

Figure 1: Chinese A2AD layered defenses

capabilities will act as the benchmark against which US current and future kill chains will be measured.

The Chinese A2AD threat consists of an integrated, multi-layer, and multi-domain system designed to engage adversary assets at the greatest distance from China possible. Its goal is to create standoff from the Chinese mainland and prevent enemy forces from rapidly projecting power toward the homeland. One of the key elements of this effort is the PLA's KJ-2000 early warning radar system fitted on the Y-9 electronic intelligence/anti-submarine aircraft. By providing early warning of potential enemy threats, this system can provide long-range warning and targeting info to mainland assets. Another major pillar in the Chinese A2AD threat is the anti-ship ballistic missile (ASBM) threat posed by both the DF-21 and DF-26 systems; although possessing varying ranges, each poses a great risk to even the most substantial US warship.[10] The PLA also employs Russian-influenced S-300 anti-air capabilities, while the People's Liberation Army Navy (PLAN) employs capable Type 52 and Type 55 cruiser and destroyer surface vessels with organic radars, anti-air/anti-surface missiles, and anti-ship cruise missiles (ASCMs).[11] Lastly, the PLA has invested heavily in their Strategic Support Force which employs space, counter-space, and electronic warfare (EW) capabilities to further supplement their kinetic assets to establish local or temporal dominance in space, electromagnetic, and information domains.[12] These elements combine to create a formidable force, but one that also relies heavily on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) dominance and a centralized kill chain process. [13] If the Navy-Marine Corps team is to implement an effective naval strategy that begins inside the enemy WEZ and gradually generates local pockets of domain superiority, the Services must develop weapons and tactics that both counter Chinese A2AD threats and execute a quicker and more lethal kill chain.

Part II: Understanding the Problem—A Vignette of the Current Kill Chain

> *Although the U.S. has spent far more on standing military forces than other countries, for far longer, this accumulated advantage is also a vulnerability. It presents an opportunity for Washington's international adversaries and competitors to reap the advantage of their backwardness and leapfrog the U.S. with emerging technology.*
>
> - Leo Blanken[14]

In recent years, the Sino-American relationship has been strained for several different reasons, but few points of contention are as flammable as the question of Taiwan's independence. Similar to the Taiwan Straits Crisis of 1996, overt military attempts from Beijing to unite the island with the Chinese mainland would likely precipitate a strong response from Washington.[15] If this scenario were to play out, this vignette's notional actions illuminate how the conflict may unfold; particularly in the South China Sea, with a focus on how the Navy-Marine Corps team's kill chain process would perform. The vignette has four basic assumptions: deterrence efforts have failed and a crisis has escalated to large-scale conflict; high-intensity conventional warfare will fall short of actions escalating to nuclear war; the US naval services' conduct of a naval campaign is occurring in the context of an overall US Joint Force campaign; and the techniques and technology employed are readily available within the next two years.

As a crisis moves to large-scale conflict, each side would likely initially engage in rapid actions seeking to gain as much targeting information as possible. Next, they would degrade adversary C4I systems and conduct operational maneuvers culminating in strikes aimed at high payoff targets.[16] For the PLA, this would mean utilizing primarily space-based assets to gain

intelligence on the status of the US Navy's surface fleet and Marine lodgements while degrading US satellite communications and satellite intelligence collection assets. The PLA would simultaneously start selectively striking US bases and potential staging locations. US forces would similarly use space assets to acquire targets and conduct electronic warfare while conducting kinetic strikes to pare down PLA A2AD capabilities.

In the early stages of this scenario, therefore, US commanders and military forces would have limited access to space-based surveillance and communications assets. In the decision portion of the D3A targeting methodology, Navy and Marine Corps personnel likely would try to compensate by shifting target allocation away from satellite assets to remaining aviation platforms and ground-based surveillance assets – resulting in increased complexity in the decision cycle and strain on remaining assets. Additionally, the loss of sensing capabilities would result in a reduction in the capability to identify and track targets. Thus, targeting personnel would be forced to conduct a manual reshuffling of the collections plan to compensate for the reduction in the capability to collect. This would have cascading effects impacting the High Payoff Target List (HPTL) as fewer targets would be identified for prosecution.[17]

To continue the vignette, as forward-positioned Marine Corps elements begin employing organic sensing capabilities, an RQ-21 Blackjack (US Marine Corps unmanned aviation vehicle) spots three PLA Navy *Luyang*-class destroyers. Despite the RQ-21's limited dwell time, it acquires the enemy ships' coordinates and relays them to its ground station before being struck by a PLA S-300 missile after being identified by the PLAN surface action group's integrated air defense system. Due to the degradation of the electromagnetic spectrum (EMS), Marine Corps EABs are forced to pass the coordinates verbally to their higher headquarters for processing. PLA signals intelligence assets would likely be cued to bursts on the EMS and begin further

investigation into friendly force locations. As the MEF coordination center receives this information, it manually inputs the coordinates into an operating system, referred to as a Common Operational Picture (COP). Due to separate COPs between the Navy-Marine Corps team, Marine Forces again verbally pass this data to the Navy coordination center for synchronization. At this point targeting personnel from both the Marine Corps and Navy will coordinate to determine the best possible targeting solution and select the course of action. As these verbal communications continue to take place, PLA sensors can increase the targeting fidelity of US forces involved in the communications kill chain. The Fire Support Coordination Center determines mission requirements and tasks nearby F-35s to locate the PLAN ships.

Marine Corps F-35B's launch from a Forward Arming and Refuelling Point (FARP) and regain contact with the Chinese destroyers. As the aircraft locates the ships, it transmits this target information to the artillery unit established on an EAB in the vicinity. At this point, the PLA signals intelligence assets pinpoint the communications signals between the F-35 and artillery EAB, and the PLAN maneuvers additional assets into the area to launch missile strikes against the EAB. The US artillery unit manually inputs targeting data received from the F-35s and computes the ballistic solution. The EAB transmits this data to the F-35s and coordinates appropriate deconfliction measures. The artillery EAB can launch a single volley of naval strike missiles (NSM) before the launchers are destroyed by a coordinated missile attack from both PLA and PLAN assets. As the EAB's NSMs reach the PLAN ships, most are defeated by active and passive internal defensive measures before reaching their target. The effort results in minimal effects on PLAN targets and fails to achieve desired effects.

As a result, additional PLAN assets pulse into the surrounding seas while the few remaining EABs not yet located through signals intelligence assets are forced to remain hidden

which are bypassed and isolated by PLAN ships. The Chinese Navy now can extend its A2AD threat range and maintain local naval superiority in the vicinity of Taiwan. This enables the PLA to conduct a virtually unharried amphibious landing on Taiwan to establish a foothold for further PLA forces to conduct operations.

Part III: Identifying the Problems in Our Current Kill Chain

If we do not change our trajectory, we will lose our qualitative and quantitative edge.

- General (Ret) Joseph Dunford[18]

The failures outlined in the preceding scenario are not ones where technology failed the military, but instead, one where the military failed to adopt technological advancements to the current paradigm. Years of unquestioned supremacy in the information domain have left our communications pathways susceptible to degradation by more capable adversaries. Moreover, our ability to dominate operations while accumulating almost omniscient situational awareness has left us willing to sacrifice speed for process and confirmation. Because US forces were typically not at risk, delays could be afforded to limit the risk of collateral damage, for example. Meanwhile, the constellation of US imagery satellites, although exquisitely produced, are too few and susceptible to enemy interference. Similarly, our UAV fleet provides persistent ISR but lacks stealth capability and is likely to be quickly located and destroyed by enemy air defenses. Additionally, the lack of system synchronicity amongst US services creates a logjam of information flow where human interaction is required to manually transfer data. Similarly, several nodes in the kill chain process require human acknowledgment or confirmation before executing actions. These manual inputs or touchpoints are often unnecessary and can add time to a critically sensitive process. The US military is also drastically underutilizing autonomous systems and swarm technology.

In sum, the kill chain process employed by the US military is outmoded and not equipped to fight against a peer competitor capable of contesting dominance in all domains. The US must embrace advancements made in communications, computing, nanotechnology, artificial intelligence (AI), autonomous systems, and data fusion. Moreover, US planners must rapidly fuse this technology into a seamless and efficient loop that minimizes disruption in data processing while maximizing the

exploitation of fleeting targets. With limited friendly assets available, each potential target engagement will be critical, and rewards must be maximized. As the paradigm shifts to high-intensity combat, new technologies must be adapted if US forces are to prevail in the new paradigm.

Part IV: Potential Improvements to the Kill Chain

> *[We] must prioritize research, development, and fielding of emerging and advanced technologies that are applicable within the seaward and landward portions of the littorals. Technologies such as artificial intelligence, robotics, additive manufacturing, quantum computing, and nanotechnology will continue to change the world – we must be positioned to capture the returns on investment.*
>
> - General David Berger[19]

To best develop future systems and capabilities, the US Department of Defense (DOD) must not only look to its own weaknesses but also take a holistic look at the adversary. Only a dispassionate and empirical analysis will enable acquisitions and development to generate an effective roadmap forward. The goal should be to develop a kill chain that not only takes advantage of emerging technology but also maximizes friendly strengths and exploits potential gaps in the enemy system. A phase-by-phase examination of the kill chain can foster discovery and potential application of technologies, undergirded by an overall philosophy that facilitates American ingenuity and exploits PLA, centralized planning models.

The first phase in the kill chain targeting methodology, the decision phase, is designed to develop target conditions, allocate detection assets, and assign engagement criteria. Here, AI can be harnessed to its greatest effect. Due to advances in sensor technology, in a single day, one space-based sensor can collect the equivalent data imagery contained in every play of every game of three complete NFL seasons.[20] The DOD has neither the capability nor capacity to conduct the human analysis of this much information. AI can use reinforcement learning techniques to sort through massive amounts of information to detect patterns. Through continued processing of captured images, AI algorithms can help determine baseline locations and habits of

enemy assets. This baseline information can assist leaders in determining changes in adversary behavior measured against friendly activity. These scenarios can help develop targeting packages that are most effective based on potential courses of action.

While AI and machine learning can take large steps toward making sense of the mountains of data that will be gathered, many of the systems the DOD operates are drastically underpowered to process them. The most powerful core processor the military operationally deploys is contained in the F-35 aircraft. While it is capable of computing 400 billion operations per second, Tesla employs processors in their self-driving vehicles capable of 320 trillion operations per second - and at a much cheaper price tag.[21] This comparison not only demonstrates the military employs inferior computing systems compared to the civilian sector, but it also represents a willingness to trade power for processes. Much of the information gathered throughout the battlefield often requires processing in centralized locations separated from the zone of action. This information must then be transferred across the military network. In most cases, sending targeting or map data wirelessly through military radio networks can take anywhere from minutes to hours. This is not feasible in potential conflict against a peer competitor in the future. This takes precious time and may also expose the transmitting agent to enemy communications direction finding and targeting. The DOD can overcome this obstacle by embracing the concept of Edge Computing. By placing more capable computers in forward locations, at the "edge" of the network, deployed units can store and process much more of the data they gather without having to reach back to centralized nodes.[22] This speeds the process, facilitates decentralized decision-making, and reduces the strain on cloud-based or wireless networks.

In the second phase of the targeting cycle, emerging technology can assist with the detection and processing of targeting information. Currently, the US's most prodigious sensing capability is conducted through a limited number of exquisitely capable satellite systems. This information is then processed through centralized nodes and disseminated through various networks and systems to targeting elements for prosecution. This portion of the kill chain is the most fragile and susceptible for disruption as both military and commercial imagery satellites are likely early targets for PLA forces.[23]

One of the simplest methods to counter this threat is to disperse sensing capabilities among several assets. This must be done across multiple domains to include space, surface, and sub-surface. As in much of technological innovation, the commercial sector leads the way in this regard. Commercial developments in nanosatellite technology provide a cheap and disposable solution by decreasing the size and cost of satellite payloads. Although these smaller assets may provide less fidelity than current military versions, their ubiquity can provide cueing for more capable assets that more than offsets this loss. Additional research has demonstrated the capability to "crowdsource" images from multiple satellites to create near real-time seamless theater assessments.[24] This capability can compensate for the potential loss of assets and additionally help ties military capabilities into allied or commercial partners. The small size and sheer

Figure 2: Networked constellations of nanosatellites could ensure constant access to space-based sensors and nodes.

numbers would decrease targeting payoff by enemy forces and secure more continual access to space-based sensors. [25]

Space should not be the only domain where the military looks to increase its sensor capability. Autonomous systems have had limited use in the US military, but as systems become more capable and less expensive, they will likely become much more effectively utilized as sensors on the future battlefield.[26] The Air Force's experimental XQ-58A Valkyrie provides an excellent example of a UAV system that provides a persistent sensing platform with increased stealth capability to reduce the threat of enemy disruption to access.[27] Similarly, autonomous underwater systems provide surveillance capabilities with superhuman persistence. One such system, Boeing's ORCA, can subsist for up to six months and travel a distance of 6,500 nautical miles while providing sub-surface reconnaissance. [28] Space-based and terrestrial autonomous systems can help provide a more robust and capable collection network, but this increased information will do little good unless there are better methods to process and integrate it all.

The first step toward better integration will be a synchronized network between the Joint Force at the strategic level. The DOD has taken steps in this direction with their concept for a Combined Joint All Domain Command and Control (CJADC2) network. This will provide the appropriate network architecture to assimilate individual services, and potentially allied partners, operational pictures together. [29] This could be a critical piece in gaining shared command and control (C2). At the operational

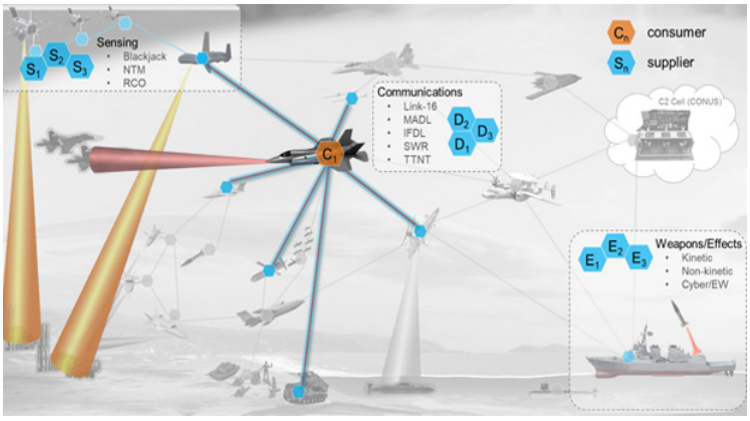

Figure 3: Networked systems facilitate greater control further forward.

level, warfighters will still need to fuze intelligence gathered from individual sensors into actionable targeting information. Initiatives like Project Maven plan to use AI to comb through imagery and flag potential targets for prosecution. AI-assisted targeting can result in identifying potential targets up to 95% faster than traditional approaches.[30] Maven will also assist with populating these targets into shared COPs across the services for rapid target prosecution. AI can also assist leaders at the tactical level as well. Concepts like DARPA's Adaptive Cross-Domain Kill Web (ADK) allows AI to assess the targets nominated through multiple sensors, and "rapidly select options for tasking assets within and across organizational boundaries."[31] Similarly, systems like the US Army's experimental Firestorm program use AI reinforcement learning techniques to find appropriate and available killing assets and "nominates" the best potential options.[32] All these elements combine to speed the detect phase through automating routine tasks and assimilating information to allow warfighters to make choices more rapidly. This also helps to reduce the overall cognitive load associated with performing many of these tasks.

In the next phase of the targeting cycle, several technological innovations can assist the military to improve its ability to deliver effects. These improvements can fall into three main categories: non-kinetic protection and effects, autonomous systems, and improvements to ship-killing ASCMs. Although many of these elements already exist in the US military's arsenal, albeit many in nascent stages, they must be improved upon and engineered in a manner to be disseminated down to the most tactical levels. These enhancements are crucial to effectively executing the kill chain.

First, the military needs to increase its capabilities for offensive and defensive cyber operations as well as EW at the lowest levels. To protect friendly kill chain networks, small units

will need to employ their own cybersecurity capabilities. By 2023, denial of service attacks will reach more than 15 million annually, while internet-oriented devices will likely experience over 5,000 attacks a month.[33] Cyber experts agree the most effective method to defend friendly networks is to detect intrusions early in the cyber kill chain and defeat them quickly.[34] Cybersecurity teams and assets must be nested within tactical units to ensure information protection. Similarly, offensive cyber capabilities must be kept close at hand as well. As the battlefield becomes more complex and interconnected, the military must provide the capability and authority for forward units to conduct offensive cyber operations (OCO) without requests for support or approval from Higher Headquarters.[35] Rapidly developing situations require immediate actions to take advantage of fleeting opportunities. EW and OCO enabled commanders can isolate and attack enemy tactical systems that can assist with out-cycling enemy kill chains.

Next, the military must improve its employment of autonomous systems.[36] These assets can improve persistence, create efficiencies through reducing manpower requirements, and require less logistic support than their human counterparts.[37] Additionally, automated systems allow the acceleration of combat through the use of AI that could potentially outpace human decision-making cycles. Harnessing the unique power of these systems will enable commanders to make decisions and facilitate these systems to accomplish the mission at a rapid pace. The speed and capabilities of these systems will greatly enhance units to meet mission requirements.

Figure 4: Swarm drones can be controlled by a manned flight lead.

This is particularly true when evaluating the concept of swarm technology. Swarm

techniques, modeled after bees who swarm together to protect their queen, consist of large numbers of cheap and disposable drones that function independently towards a common goal. Swarm tactics are unique in that each system functions independently, but communicates with all other systems; in this manner, they can assume losses to their numbers but continue to compensate and accomplish the mission.[38] These systems pose several benefits when viewed in this light. Offensively, drone swarms can be used to overwhelm enemy radar defensive weapons or oversaturate radar arrays – enabling killing assets to filter through automated defensive systems. Defensively, drone swarms can be used to defend against enemy aircraft attacking friendly positions. These systems can be used even more effectively when paired with human teammates. [39] Boeing's "Loyal Wingman" program boasts the capability to tether multiple unmanned "fighter-like" aircraft to a single manned platform. This allows for human control of drone systems and pushes command and control to its further limit into the tactical fight.[40] Moreover, these systems can augment human pilots and increase the capability of the combat formation while decreasing the manpower and training hours required to prepare military pilots for combat. While autonomous systems can make an immediate impact on the kill chain process, they cannot solve the complexities of the delivery phase alone.

The DOD must also develop better ASCMs to ensure a capable multi-layered offensive capability. When the US signed the Intermediate-Range Nuclear Forces in 1987, it limited the development of certain types of cruise missiles and impacted the military's capability to build an adequate medium-range anti-ship missile system.[41] Due to Russian misconduct and violation of this treaty, the US has withdrawn from the agreement and is now free to pursue this capability with fewer restrictions.[42] The US should look to ensure new ASCM developments can be launched from both the surface and air across multiple platforms. Surface-launched ASCMs

must have ranges sufficient to cover large swaths of ocean straits and ensure ground forces can conduct sea denial operations in littoral areas.[43] Air-delivered ASCMs must retain enough range to enable employment outside PLAN newly launched *Luyang III*-class destroyer's Type 346A radar systems to ensure aircraft survivability.[44] More importantly, to increase missile survivability and lethality, several variants of future US-developed ASCM should be hypersonic. This increased speed is vital for limiting the combatant's reaction time and to overcome AI-assisted defensive capabilities. Without these systems, the current US capability to attack PLAN ships is severely limited.

The final phase in the kill chain methodology is the assessment phase. Here, friendly forces conduct an estimation of the effects of the strike and recommend re-attack or follow-on actions.[45] Again, autonomous systems can be beneficial by getting close enough to enemy forces and conduct an extensive battle damage assessment without the fear of losing a manned platform. Additionally, AI can be utilized to rapidly assess and analyze the impacts of those effects. By using stock imagery of enemy assets and comparing it to historical battle damage imagery, AI algorithms can conduct a change comparison analysis to determine what particular enemy systems have been damaged. [46] Specifically, AI could determine if radar systems were still operational or if enemy weapon systems were effectively impacted. This will allow commanders to accurately determine if the strike was effective and if further strikes are required. All this can occur rapidly and with minimal danger to friendly forces.

Lastly, the entirety of the kill chain is predicated on secure, robust, and effective communications. Emerging powers maintain capabilities for jamming multiple waveforms and conducting signals intelligence operations to intercept communications. There are methods to mitigate these techniques, but the DOD must begin to invest in a more secure communications

architecture. Specifically, EABs will require secure, low-emitting, long-haul communications that can be utilized at the lowest tactical levels. Fortuitously, improvements in high frequency (HF) communications may provide a potential solution. Through conducting automated spectrum modulation, US forces can overcome enemy direction-finding techniques and create additional space on the EMS. Additionally, DARPA developed the Protected Forward Communications program that uses structures systems engineering to reinforce communications signals strength and make it more resistant to enemy jamming.[47] Additionally, their Hyper-Wideband Radio Frequency-Messaging System incorporates emerging techniques to broaden the EMS and deter detection systems for identifying friendly signals.[48] Furthermore, emerging improvements to quantum communications promise the potential for completely secure communications. Chinese researchers have bragged of their capabilities to send quantum secured communications through satellites to locations over 700 miles away.[49] The prospect of quantum encrypted information will drastically increase the military's ability to communicate with forward-positioned leadership.

Concurrently, the DOD must invest in countermeasures to increase friendly survivability. Signal spoofing drones and buoys can mimic various EMS signals and be made to look as though friendly positions have multiplied or rapidly moved. Through careful employment and various emission patterns, enemy signal location efforts can be overwhelmed or confused – drastically degrading enemy targeting efforts. A multitude of different methods must be employed to ensure friendly assets maintain access to the EMS and can share information across the joint force to ensure unity of effort and coordinated effects. As identified in his planning guidance, General Berger rightly states "Success will be defined in terms of finding the smallest, lowest signature options that yield the maximum operational utility."[50]

As illuminated in the previous section, future battles will be won and lost in the few seconds it takes to close the kill chain. The US should make strenuous efforts to develop technologies that gain efficiencies where possible. AI, autonomous systems, hypersonic weapons; all must work in concert with each other to create synergistic effects that outpace the enemy's decision-making cycle to gain a strategic advantage. As the pace of combat continues to increase, the margin of error will decrease while the implications for lost opportunities will compound.

Part V: Addressing Counterarguments

> *No piece of paper can prevent a state from building autonomous weapons if they desire it. At the same time, a pell-mell race toward autonomy, with no clear sense where it leads us, benefits no one. States must come together to develop an understanding of which uses of autonomy are appropriate and which go too far and surrender human judgment where it is needed in war.*
>
> - Paul Scharre[51]

In keeping with this paper's foundational assumptions identified in the preface, the author does not address "military feasibility" counterarguments that are not directly relevant to the paper's focus on the kill-chain process. For example, as it stands, US forces currently lacks sufficient "magazine depth"—numbers of missiles in vertical launch containers or on aircraft—for waging a longer-term, high-intensity fight. While multiple political, logistic, and physical aspects would likely hamper the kill-chain process in a high-end conflict against apeer competitor, they reside outside the limited scope of the process itself and have been reduced from overall calculations. This was a conscious effort to ensure the focus remained on the identification of kill chain-related issues and their potential solutions.

The promise of vigorously adopting advanced technologies to improve and speed up the US kill chain faces moral and safety counter-arguments that need to be addressed to confidently move forward. One of the most pressing concerns is the use of AI to automate portions of the targeting process. Removal of human interaction within the decision-making loop brings to bear both ethical and safety concerns that must be confronted. Opponents of AI implementation will often refer to the "Trolly Problem" to illuminate the issues surrounding AI-developed decisions. The "Trolly Problem" is an iconic hypothetical scenario where a runaway trolly car is in line to

kill five people but can be diverted to another track where it may only kill one. The subject of the experiment is questioned whether they would choose to interfere and pull the lever to switch tracks, or not. The mental experiment demonstrates the moral decision-making behind the choice to act.[52]

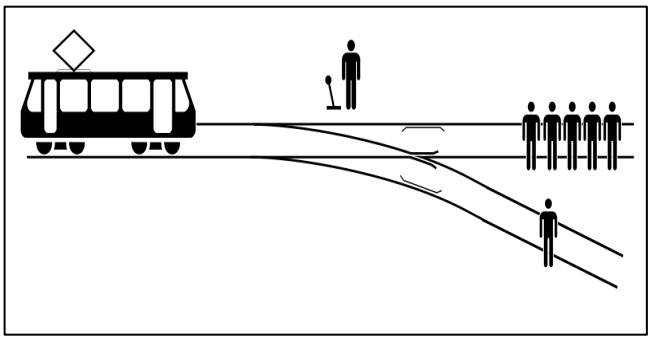

Figure 5: The trolly problem illuminates the foundations of choice

When applied to the context of potential future military implementation, this takes the form of an algorithm "making the decision" of who should live and who will die.[53] While AI does not make decisions in a traditional sense, it is bounded by algorithms developed by teams of people who do. Seeking to address these types of issues, researchers from the Massachusetts Institute of Technology (MIT) developed the Moral Machine Experiment. The program used an AI-assisted "self-driving" car to gather over 40 million ethical decisions it encountered while driving. These decisions were then distilled, categorized, and posed as dilemmas to millions of people from 223 countries and territories. By correlating the responses, MIT sought to develop "socially acceptable principles for machine ethics."[54] Implementations like these can ensure processes are scrutinized and ethical parameters put in place to avoid the wrongful prosecution of targets.

Similarly, many may argue that because we don't fully understand how AI "Deep Learning" techniques make decisions, it would be difficult to hold anything or anyone accountable.[55] This perception reinforces the idea that the military must maintain the "man in the loop" concept.[56] As such, AI should be used to create targeting solutions, but not implement actions resulting in lethal effects; these decisions will be left to human coordinators who select

the best courses of action. Additionally, human interactions facilitate final safety checks to ensure coordination, synchronization, and the ethical employment of systems that require a contextual determination that only resides with human cognition.

While many of these arguments raise valid concerns, they should not dissuade military decision-makers from boldly moving forward with the planning and implementation of these systems and techniques. Furthermore, addressing ethical and safety concerns will not hamper the systemic progress of these systems, but will make their implementation more sound. Military leaders must embrace these concerns, build in the appropriate measure to ensure concurrence from leaders, and continue to progress forward.

Part VI: Vignette of a Potential Future Kill Chain

> …great-power war waged by these technologically advanced competitors would likely be governed by the brutal, unforgiving logic of World War I: forces that are entrenched in defensive positions could stand a decent chance of surviving and fighting effectively, but the moment they step off from their points of departure and try to advance against their opponents, they would likely enter a new "no man's land" that is teeming with ubiquitous sensors, intelligent machines, and advanced weapons, operating from the ocean floor to outer space, that are capable of closing the kill chain at scales and speeds that attacking forces would struggle to survive.
>
> - Christian Brose[57]

The following vignette follows a similar scenario as the first vignette, with hostilities breaking out between the US and China over a conflict in Taiwan. In this instance, the Navy-Marine Corps teams employ several of the systems and methods outlined in part IV of this work. While not exhaustively inclusive of all potential improvements, the vignette demonstrates how advances to the kill chain process may create a strategic advantage for US forces. Clearly, the vignette simplifies the complexities, friction, and human element inherent in war, and the paper decidedly is not trying to depict a technological "magic wand" that assures victory. Rather, the vignette, distilling and summarizing the potential impact of key technologies and concepts, is instead merely illustrating how the integration and fusing of new technologies could improve the kill-chain aspects of a wider fight.

As Marine Corps EABs occupy or activate strategic locations around the Taiwan strait, EW teams immediately conduct actions to protect friendly networks, minimize

friendly signal emission signature, create dummy signals in multiple locations to confuse enemy intelligence, and penetrate and degrade enemy networks. Simultaneously, communications sections quickly establish communications suites that facilitate quantum secured data transmission across multiple waveforms oscillating between each type in designated windows. Concurrently, Marine cyber teams generate false signals and reporting to influence PLAN ships to maneuver into carefully designated kill boxes where Marine EABs have the greatest advantage in conducting kinetic strikes.

As the PLAN assets maneuver into the EAB area of operations, nanosatellites can detect, track, and provide data directly and simultaneously to the EABs and USMC Fire Support Coordination Center (FSCC). Within seconds the Firestorm program identifies these images as PLAN assets and develops three recommendations for kill chain prosecution. The fires coordinator selects the best potential options and the AI algorithm dynamically re-tasks a nearby F-35 composite squadron for target validation and acquisition while also sending warning orders to artillery EAB units. As the F-35 section maneuvers into the weapons engagement range of PLAN assets, EAB and low earth orbit nanosatellites conduct EW jamming to mitigate the PLAN surface group communications and isolate them from reinforcements.

AI-developed targeting solutions including timelines, weapons ballistic solutions, and targeting priorities for each munition are transmitted via data packets. To avoid enemy signals intelligence efforts, this process is conducted over multiple waveforms and aggregated by edge computing at each designated location. As the kinetic strike timeline approaches, the F-35 composite squadron employs its loyal wingman assets directing autonomous drones to swarm the PLAN surface group.[58] Simultaneously, the Firestorm

program cues the EAB artillery assets to launch their hypersonic missiles at the PLAN assets. As the loyal wingman drones swarm the PLAN ships, the *Luyang's* active defense measures expend all ammunition to destroy the attacking drones, leaving the ships defenseless until able to reload. Seconds later, multiple EAB rockets slam into critical locations in each ship, sinking them within minutes.

Alerted to potential distress, two Chinese J-20's launched from a nearby airfield attack and destroy the single F-35 who is now unprotected after deploying its drones. Noting this, the Firestorm program re-tasks a Marine Corps MQ-9 from a nearby EAB to compensate for the lack of coverage. Additionally, cued by radar from the missile launch, PLA rocket forces launch multiple missile strikes against the artillery EAB that fired on the PLAN ships. The EAB suffers heavy losses to its artillery and anti-air assets. It is unable to conduct offensive actions until reconstituted in later stages of the conflict.

As PLAN assets are eliminated in this area of operations, US Navy assets pulse into the newly created vacuum and extend friendly freedom of maneuver by establishing local naval and air superiority. As more US Naval assets arrive in zone, they launch autonomous craft designed to resupply Marine Corps EABs and facilitate survivability movements to new locations where required.

Part VII: Conclusion and The Way Forward

The sobering reality is, no matter how you look at it, technology will continue to advance and customers will find new and exciting ways to use it. If an organization continues to resist progress and decides not to keep up with technology, they face the real risk of fading away into obscurity.

- *Michael Locher, CEO*[59]

Moore's Law states that the number of transistors per microchip will double approximately every two years. Similarly, the computational power of personal computers has doubled approximately every year and a half since being tracked in 1975. In general, technological advancements have followed an linear growth pattern and are projected to continue producing advancements that will only increase computing power while simultaneously decreasing the size, cost, and power requirements for these items.[60] These facts demonstrate that technological advancements will inexorably change and grow with time. The Marine Corps can ill afford to fight the next conflict with yesterday's technology.

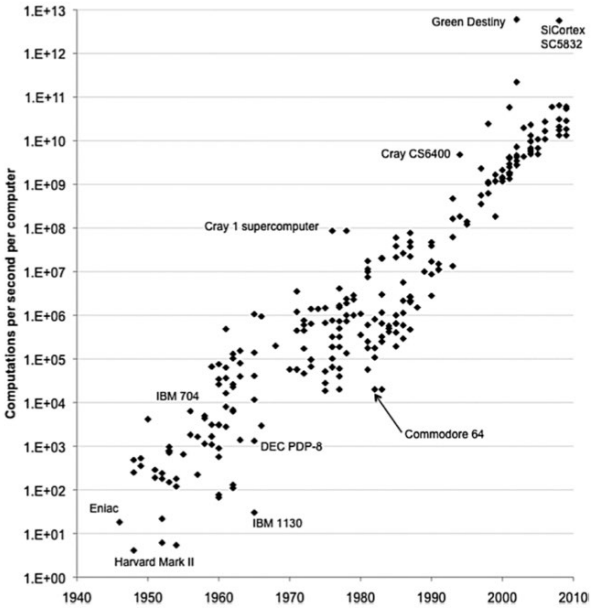

Figure 6: Graphic representation of Moore's Law.

More importantly, the Marine Corps must realize that our adversaries will likely be developing similar technological advancements of their own. As China continues to grow in wealth and scientific sophistication, the most likely scenario is one of technological parity with

the PLA; one where weapons and systems are developed by each country independently, but maintain similar capability and complexity. [61] This demonstrates that stagnation and complacency in American innovation constitute a grave threat to national security.[62] The United States is not likely to "win" the war of technological advancement, but it certainly can lose it by maintaining its present course.

America is by nature a "high-tech" society. The question is whether these inherent technological advantages will be harnessed—and funded—in the military arena. The Russian invasion of Ukraine in 2014 is an admonitory example. At a time when almost all objective measures of power favored the United States over Russia, US observers were amazed at the ability of the Russian army to harness the power of the information domain to rapidly close the kill chain on Ukrainian forces by employing asymmetric techniques. Through the use of social media and electronic warfare, the Russian military targeted Ukrainian forces in ways no one had conceived before. [63] While America was preoccupied with operations in Iraq and Afghanistan, the Russian military developed capabilities that changed American concepts of current technology's employment. The US military must view this as a cautionary tale of American hubris. Assuming technological superiority can facilitate complacency and permit others to better develop our systems against us. Conflict with a peer competitor will be conducted with highly advanced technology and across all domains. The victor will be the one who fully grasps the complexity of the current paradigm and employs emerging technology in novel and disruptive methods to create a strategic advantage.

Notes

[1] Bill Owens and Ed Offley, *Lifting the Fog of War* (Baltimore, MD: Johns Hopkins University Press, 2001), 19.
[2] Lawrence Freedman, *The Future of War: a History* (New York, NY: Public Affairs, 2019), 142.
[3] "Summary of the National Defense Strategy." Defense.gov. Department of Defense, January 1, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 1.
[4] David H. Berger, "38th Commandant's Planning Guidance," Marines.mil (United States Marine Corps , July 17, 2019), https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/, 1.
[5] Chairmen of the Joint Chiefs, Joint Targeting, JP 3-60. Washington DC: Joint Staff, January 31, 2013, I-10.
[6] Edmund J. Burke et al., "China's Evolving Military Strategy and Doctrine," RAND Corporation, September 29, 2020, https://www.rand.org/pubs/research_reports/RRA394-1.html, 4.
[7] Terrence K. Kelly, David C. Gompert, and Duncan Long, "Exploiting U.S. Advantages to Prevent Agression," *Smarter Power, Stronger Partners* 1, no. 1 (2016): pp. 1-278, https://doi.org/https://doi.org/10.7249/RR1359, 22.
[8] David H. Berger, "38th Commandant's Planning Guidance," Marines.mil (United States Marine Corps , July 17, 2019), https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/, xi.
[9] Jim Garamone, "Esper Discusses Moves Needed to Counter China's Malign Strategy," Defense News (Department of Defense, August 27, 2020), https://www.defense.gov/Explore/News/Article/Article/2326863/esper-discusses-moves-needed-to-counter-chinas-malign-strategy/.
[10] V. I. Venugopal , "How Effective Is China's A2/AD in the South China Sea; By Commodore V Venugopal (Retd)," C3S India (Chennai Centre for China Studies, October 21, 2020), https://www.c3sindia.org/defence-security/how-effective-is-chinas-a2-ad-in-the-south-china-sea-by-commodore-v-venugopal-retd/.
[11] Ngo Minh Tri , "China's A2/AD Challenge in the South China Sea: Securing the Air From the Ground," Flashpoints (The Diplomat, May 19, 2017), https://thediplomat.com/2017/05/chinas-a2ad-challenge-in-the-south-china-sea-securing-the-air-from-the-ground/.
[12] Mark Stokes et al., "China's Space and Counterspace Capabilities and Activities" (Washington, DC: Pointe Bello, 2020), pp. 1-216, 8.
[13] Peter Kouretsos, "Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Pacific," Capability Analysis (Center for International Maritime Security, October 1, 2019), http://cimsec.org/tightening-the-chain-implementing-a-strategy-of-maritime-pressure-in-the-pacific/41928.
[14] Leo Blanken and Jason Lepore, "America's Military Is Choking on Old Technology," Foreign Policy, January 29, 2018, https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/.
[15] Graham Tillett Allison, Destined for War Can America and China Escape Thucydides's Trap? (New York, NY: Mariner, 2020), 141.

[16] Gompert, David C., Astrid Stuth Cevallos, and Cristina L. Garafola, War with China: Thinking Through the Unthinkable (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1140.html.
[17] A reshuffling of the High Payoff Target List would be required due to potential limitation of detection assets. This would strain U.S. ability to surveil as many targets as desired, which may eliminate some targets from the list due to target acquisition limitations.
[18] Joseph Dunford, "United States Committee on Armed Services," Hearing | Hearings | United States Committee on Armed Services, June 13, 2017, https://www.armed-services.senate.gov/hearings/17-06-13-department-of-defense-budget-posture.
[19] David H. Berger, "38th Commandant's Planning Guidance," Marines.mil (United States Marine Corps , July 17, 2019), https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/, 11.
[20] Julian Nettlefold, "1 Million Times More GEOINT Data In 5 Years By COLIN CLARK," Battlespace Updates (Breaking Defense, June 12, 2017), https://battle-updates.com/cardillo-1-million-times-more-geoint-data-in-5-years-by-colin-clark/.
[21] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette Books, 2020), 51.
[22] Li, Wang. "Toward Open Manufacturing: A Cross-Enterprises Knowledge and Services Exchange Framework Based on Blockchain and Edge Computing." *Industrial management + data systems* 118.1 (2018): 303–320. Web.
[23] Theresa Hitchens and Colin Clark, "Commercial Satellites: Will They Be Military Targets?," Breaking Defense (Above the Law, September 6, 2019), https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/.
[24] Freddy Alexander Díaz, Pablo Roberto Pinzón, and Claudio Marcel Hernández, "Design of a Nanosatellite Ground Monitoring and Control Software – a Case Study," Journal of Aerospace Technology and Management (Departamento de Ciência e Tecnologia Aeroespacial, June 1, 2016), http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2175-91462016000200211.
[25] Robert Scammell, "Astrocast Announces Three Partners to Pilot Its IoT Nanosatellite Network," Verdict, January 7, 2019, https://www.verdict.co.uk/astrocast-partners-pilot-nanosatellite/.
[26] Lawrence Freedman, *The Future of War: a History* (New York, NY: PublicAffairs, 2019), 241.
[27] John A. Tirpak, "'Air Force We Need 2.0' Exploring Low-Cost, Unmanned Aircraft," Air Force Magazine (Garnet Communications , October 2, 2020), https://www.airforcemag.com/air-force-we-need-2-0-exploring-low-cost-unmanned-aircraft/.
[28] Talal Husseini, "Autonomous Underwater Robots: from Swordfish to the Orca," Naval technology@2x, January 29, 2021, https://www.naval-technology.com/features/autonomous-underwater-robots-navy/.
[29] Mark Pomerleau, "Is the Pentagon's 'Fragile' Network Ready to Handle a Slew of Connected Weapon Systems?," C4ISRNET (C4ISRNET, November 20, 2020), https://www.c4isrnet.com/it-networks/2020/11/20/is-the-pentagons-fragile-network-ready-to-handle-a-slew-of-connected-weapon-systems/#:~:text=Combined%20Joint%20All-Domain%20Command%20and%20Control%2C%20or%20CJADC2%2C,decisions%20at%20the%20increasingly%20rapid%20speed%20of%20war.

[30] Courtney Crosby, "Operationalizing Artificial Intelligence for Algorithmic Warfare," Army University Press (U.S. Army, 1, 2020), https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Crosby-Operationalizing-AI/.
[31] Daniel Javorsek, " Adapting Cross-Domain Kill-Webs," DARPA RSS (DARPA, 2020), https://www.darpa.mil/program/adapting-cross-domain-kill-webs.
[32] Andrew Eversden, "A Weapon System 'Raises Its Hand' If Available under DARPA Program," C4ISRNET (C4ISRNET, June 16, 2020), https://www.c4isrnet.com/c2-comms/2020/06/16/a-weapon-system-raises-its-hand-if-available-under-darpa-program/.
[33] Rob Sobers , "134 Cybersecurity Statistics and Trends for 2021: Varonis," Inside Out Security, January 30, 2021, https://www.varonis.com/blog/cybersecurity-statistics/.
[34] Ravdeep Kour, Adithya Thaduri , and Ramin Karim, "Journal of Cyber Security and Mobility," Journal of Web Engineering (Luleå Railway Research Center, December 14, 2019), https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1271/607, 50.
[35] Isaac R. Porche et al., "Tactical Cyber," Tactical Cyber Building a Strategy for Cyber Support to Corps and Below (RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1600.html, 48.
[36] In the context of this paper, an autonomous system is defined as: Any artificial system that performs tasks during unpredictable circumstances without human interaction.
[37] Adriana Gibson, Brandon D. Vigneron, and Andrew J. Merchant, "Autonomous Systems in the Combat Environment: The Key or the Curse to the U.S.," The Strategy Bridge (The Strategy Bridge, October 8, 2020), https://thestrategybridge.org/the-bridge/2020/10/8/autonomous-systems-in-the-combat-environment-the-key-or-the-curse-to-the-us.
[38] Spencer Lynn, "Drone Swarms: A Transformational Technology," Tech Briefs (Techbriefs Media Group, May 15, 2020), https://www.aerodefensetech.com/component/content/article/adt/features/articles/36813.
[39] "Boeing," Boeing, accessed February 27, 2021, https://www.boeing.com/defense/airpower-teaming-system/.
[40] Tyler Rogoway, "Everything We Learned From Boeing About Its Potentially Game-Changing Loyal Wingman Drone," The Drive (The Drive, May 4, 2020), https://www.thedrive.com/the-war-zone/33271/everything-we-learned-from-boeing-about-its-potentially-game-changing-loyal-wingman-drone.
[41] Daryll Kimbal, "The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance ," The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance | Arms Control Association (Arms Control Association, August 1, 2019), https://www.armscontrol.org/factsheets/INFtreaty.
[42] Congressional Research Service. *U.S. Withdrawal from the INF Treaty: What's Next?* Washington D.C. 2020.
[43] David H. Berger, "38th Commandant's Planning Guidance," Marines.mil (United States Marine Corps , July 17, 2019), https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/, 3.
[44] Franz-Stefan Gady, "China Commissions Fourth 'Carrier Killer Destroyer'," The Diplomat (The Diplomat, August 9, 2016), https://thediplomat.com/2015/07/china-commissions-second-carrier-killer-destroyer/.
[45] Chairmen of the Joint Chiefs, Joint Targeting, JP 3-60. Washington DC: Joint Staff, January 31, 2013, I-10.

[46] Nathan Strout, "Can AI Automate Damage Assessments after a Disaster?," C4ISRNET (C4ISRNET, October 11, 2019), https://www.c4isrnet.com/intel-geoint/2019/10/04/can-ai-automate-damage-assessments-after-a-disaster/.
[47] Brian Berg, "To Be Detected Is to Be Killed," *US Naval InstituteProceedings* 146, no. 12 (December 1, 2020): pp. 18-23, https://doi.org/0041-798X.
[48] Ibid.
[49] William J. Broad, "China Reports Progress in Ultra-Secure Satellite Transmission," The New York Times (The New York Times, June 15, 2020), https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html.
[50] David H. Berger, "38th Commandant's Planning Guidance," Marines.mil (United States Marine Corps , July 17, 2019), https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/.
[51] Paul Scharre, *Army of None* (New York, NY: WW NORTON & CO, 2019), 386.
[52] "Trolley Problem," Wikipedia (Wikimedia Foundation, February 21, 2021), https://en.wikipedia.org/wiki/Trolley_problem.
[53] Lauren Cassani Davis, "Would You Pull the Trolley Switch? Does It Matter?," The Atlantic (Atlantic Media Company, October 9, 2015), https://www.theatlantic.com/technology/archive/2015/10/trolley-problem-history-psychology-morality-driverless-cars/409732/.
[54] Edmond Awad et al., "The Moral Machine Experiment," Nature News (Nature Publishing Group, October 24, 2018), https://www.nature.com/articles/s41586-018-0637-6.
[55] Will Knight, "The Dark Secret at the Heart of AI," MIT Technology Review (MIT Technology Review, April 2, 2020), https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/.
[56] Adrian Bridgwater, "Machine Learning Needs A Human-In-The-Loop," Forbes (Forbes Magazine, March 8, 2016), https://www.forbes.com/sites/adrianbridgwater/2016/03/07/machine-learning-needs-a-human-in-the-loop/?sh=7aef210e4cab.
[57] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette Books, 2020), 164.
[58] Although completely hypothetical, potential F-35 composite squadrons could include F-35 flight leads who control autonomous drones in a synchronized manner. The F-35 pilot may act as the Armed Reconnaissance lead, who directs the autonomous systems, but stays out of the enemy weapon system's effective range.
[59] Michael Locher, "The Future of Information Technology and MSP's," Enterprise Integration, October 19, 2020, https://entint.com/why-ei/tools-automation-and-it/.
[60] Max Roser and Hannah Ritchie, "Technological Progress," Our World in Data, May 11, 2013, https://ourworldindata.org/technological-progress.
[61] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette Books, 2020), 72.
[62] Larry Alton, "Staying Technologically Relevant Has Suddenly Become A Full-Time Responsibility," Forbes (Forbes Magazine, October 21, 2016), https://www.forbes.com/sites/larryalton/2016/10/21/staying-technologically-relevant-has-suddenly-become-a-full-time-responsibility/.
[63] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette Books, 2020), 32.

Bibliography

Allison, Graham Tillett. *Destined for War Can America and China Escape Thucydides's Trap?* New York, NY: Mariner, 2020.

Alton, Larry. “Staying Technologically Relevant Has Suddenly Become A Full-Time Responsibility.” Forbes. Forbes Magazine, October 21, 2016. https://www.forbes.com/sites/larryalton/2016/10/21/staying-technologically-relevant-has-suddenly-become-a-full-time-responsibility/.

Awad, Edmond, Sohan Dsouza, Richard Kim, Jonathan Schulz, Joseph Henrich, Azim Shariff, Jean-François Bonnefon, and Iyad Rahwan. “The Moral Machine Experiment.” Nature News. Nature Publishing Group, October 24, 2018. https://www.nature.com/articles/s41586-018-0637-6.

Berg, Brian. “To Be Detected Is to Be Killed.” *US Naval InstituteProceedings* 146, no. 12 (December 1, 2020): 18–23. https://doi.org/0041-798X.

Berger, David H. “38th Commandant's Planning Guidance.” Marines.mil. United States Marine Corps , July 17, 2019. https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/1907265/38th-commandants-planning-guidance-cpg/.

Blanken, Leo, and Jason Lepore. “America's Military Is Choking on Old Technology.” Foreign Policy, January 29, 2018. https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/.

Blanken, Leo, and Jason Lepore. “America's Military Is Choking on Old Technology.” Foreign Policy, January 29, 2018. https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/.

Bridgwater, Adrian. “Machine Learning Needs A Human-In-The-Loop.” Forbes. Forbes Magazine, March 8, 2016. https://www.forbes.com/sites/adrianbridgwater/2016/03/07/machine-learning-needs-a-human-in-the-loop/?sh=7aef210e4cab.

Broad, William J. “China Reports Progress in Ultra-Secure Satellite Transmission.” The New York Times. The New York Times, June 15, 2020. https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html.

Brose, Christian. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York, NY: Hachette Books, 2020.

Burke, Edmund J., Kristen Gunness, Cortez A. III Cooper, and Mark Cozad. “China's Evolving Military Strategy and Doctrine.” RAND Corporation, September 29, 2020. https://www.rand.org/pubs/research_reports/RRA394-1.html.

Chairmen of the Joint Chiefs, Joint *Targeting*, JP 3-60. Washington DC: Joint Staff, January 31, 2013.

Congressional Research Service. *U.S. Withdrawal from the INF Treaty: What’s Next?* Washington D.C. 2020.

Crosby, Courtney. “Operationalizing Artificial Intelligence for Algorithmic Warfare.” Army University Press. U.S. Army, 2020. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Crosby-Operationalizing-AI/.

Davis, Lauren Cassani. “Would You Pull the Trolley Switch? Does It Matter?” The Atlantic. Atlantic Media Company, October 9, 2015. https://www.theatlantic.com/technology/archive/2015/10/trolley-problem-history-psychology-morality-driverless-cars/409732/.

Díaz, Freddy Alexander, Pablo Roberto Pinzón, and Claudio Marcel Hernández. “Design of a Nanosatellite Ground Monitoring and Control Software – a Case Study.” Journal of Aerospace Technology and Management. Departamento de Ciência e Tecnologia Aeroespacial, June 1, 2016. http://www.scielo.br/scielo.php?script=sci_arttext&pid=S2175-91462016000200211.

Dunford, Joseph. “United States Committee on Armed Services.” Hearing | Hearings | United States Committee on Armed Services, June 13, 2017. https://www.armed-services.senate.gov/hearings/17-06-13-department-of-defense-budget-posture.

Eversden, Andrew. “A Weapon System 'Raises Its Hand' If Available under DARPA Program.” C4ISRNET. C4ISRNET, June 16, 2020. https://www.c4isrnet.com/c2-comms/2020/06/16/a-weapon-system-raises-its-hand-if-available-under-darpa-program/.

Freedman, Lawrence. *The Future of War: a History*. New York, NY: Public Affairs, 2019.

Gady, Franz-Stefan. “China Commissions Fourth 'Carrier Killer Destroyer'.” The Diplomat. The Diplomat, August 9, 2016. https://thediplomat.com/2015/07/china-commissions-second-carrier-killer-destroyer/.

Garamone, Jim. “Esper Discusses Moves Needed to Counter China's Malign Strategy.” Defense News. Department of Defense, August 27, 2020. https://www.defense.gov/Explore/News/Article/Article/2326863/esper-discusses-moves-needed-to-counter-chinas-malign-strategy/.

Gibson, Adriana, Brandon D. Vigneron, and Andrew J. Merchant. “Autonomous Systems in the Combat Environment: The Key or the Curse to the U.S.” The Strategy Bridge. The Strategy Bridge, October 8, 2020. https://thestrategybridge.org/the-bridge/2020/10/8/autonomous-systems-in-the-combat-environment-the-key-or-the-curse-to-the-us.

Gompert, David C., Astrid Stuth Cevallos, and Cristina L. Garafola, War with China: Thinking Through the Unthinkable. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1140.html.

Hitchens, Theresa, and Colin Clark. “Commercial Satellites: Will They Be Military Targets?” Breaking Defense. Above the Law, September 6, 2019. https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/.

Husseini, Talal. “Autonomous Underwater Robots: from Swordfish to the Orca.” Naval Technology 2X, January 29, 2021. https://www.naval-technology.com/features/autonomous-underwater-robots-navy/.

Javorsek, Daniel. “ Adapting Cross-Domain Kill-Webs.” DARPA RSS. DARPA, 2020. https://www.darpa.mil/program/adapting-cross-domain-kill-webs.

Kelly, Terrence K., David C. Gompert, and Duncan Long. “Exploiting U.S. Advantages to Prevent Aggression.” *Smarter Power, Stronger Partners* 1, no. 1 (2016): 1–278. https://doi.org/https://doi.org/10.7249/RR1359.

Kimbal, Daryll. “The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance .” The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance | Arms Control Association. Arms Control Association, August 1, 2019. https://www.armscontrol.org/factsheets/INFtreaty.

Knight, Will. “The Dark Secret at the Heart of AI.” MIT Technology Review. MIT Technology Review, April 2, 2020. https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/.

Kour, Ravdeep, Adithya Thaduri, and Ramin Karim. “Journal of Cyber Security and Mobility.” Journal of Web Engineering. Lule̊a Railway Research Center, December 14, 2019. https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1271/607.

Kouretsos, Peter. “Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Pacific.” Capability Analysis. Center for International Maritime Security, October 1, 2019. http://cimsec.org/tightening-the-chain-implementing-a-strategy-of-maritime-pressure-in-the-pacific/41928.

Li, Zhi, W. M. Wang, Guo Liu, Layne Liu, Jiadong He, and G. Q. Huang. "Toward Open Manufacturing." *Industrial Management & Data Systems* 118, no. 1 (2018): 303-320. doi:http://dx.doi.org.lomc.idm.oclc.org/10.1108/IMDS-04-2017-0142. https://www-proquest-com.lomc.idm.oclc.org/scholarly-journals/toward-open-manufacturing/docview/1990858058/se-2?accountid=14746.

Locher, Michael. “The Future of Information Technology and MSP's.” Enterprise Integration, October 19, 2020. https://entint.com/why-ei/tools-automation-and-it/.

Lynn, Spencer. “Drone Swarms: A Transformational Technology.” Tech Briefs. Techbriefs Media Group, May 15, 2020. https://www.aerodefensetech.com/component/content/article/adt/features/articles/36813.

Nettlefold, Julian. “1 Million Times More GEOINT Data In 5 Years By COLIN CLARK.” Battlespace Updates. Breaking Defense, June 12, 2017. https://battle-updates.com/cardillo-1-million-times-more-geoint-data-in-5-years-by-colin-clark/.

Owens, Bill, and Ed Offley. *Lifting the Fog of War*. Baltimore, MD: Johns Hopkins University Press, 2001.

Pomerleau, Mark. “Is the Pentagon'sFragile' Network Ready to Handle a Slew of Connected Weapon Systems?” C4ISRNET. C4ISRNET, November 20, 2020. https://www.c4isrnet.com/it-networks/2020/11/20/is-the-pentagons-fragile-network-ready-to-handle-a-slew-of-connected-weapon-systems/#:~:text=Combined%20Joint%20All-Domain%20Command%20and%20Control%2C%20or%20CJADC2%2C,decisions%20at%20the%20increasingly%20rapid%20speed%20of%20war.

Porche, Isaac R., Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. “Tactical Cyber.” Tactical Cyber Building a Strategy for Cyber Support to Corps and Below. RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1600.html.

Roser, Max, and Hannah Ritchie. “Technological Progress.” Our World in Data, May 11, 2013. https://ourworldindata.org/technological-progress.

Rogoway, Tyler. “Everything We Learned From Boeing About Its Potentially Game-Changing Loyal Wingman Drone.” The Drive. The Drive, May 4, 2020. https://www.thedrive.com/the-war-zone/33271/everything-we-learned-from-boeing-about-its-potentially-game-changing-loyal-wingman-drone.

Scharre, Paul. *Army of None*. New York, NY: WW Norton & Co, 2019.

Sobers, Rob. “134 Cybersecurity Statistics and Trends for 2021: Varonis.” Inside Out Security, January 30, 2021. https://www.varonis.com/blog/cybersecurity-statistics/.

“Summary of the National Defense Strategy.” Defense.gov. Department of Defense, January 1, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Stokes, Mark, Gabriel Alvarado, Emily Weinstein, and Ian Easton. Rep. *China’s Space and Counterspace Capabilities and Activities*. Washington, DC: Pointe Bello, 2020.

Strout, Nathan. “Can AI Automate Damage Assessments after a Disaster?” C4ISRNET. C4ISRNET, October 11, 2019. https://www.c4isrnet.com/intel-geoint/2019/10/04/can-ai-automate-damage-assessments-after-a-disaster/.

Tirpak, John A. “'Air Force We Need 2.0' Exploring Low-Cost, Unmanned Aircraft.” Air Force Magazine. Garnet Communications, October 2, 2020. https://www.airforcemag.com/air-force-we-need-2-0-exploring-low-cost-unmanned-aircraft/.

Venugopal, V. I. “How Effective Is China's A2/AD in the South China Sea; By Commodore V Venugopal (Retd).” C3S India. Chennai Centre for China Studies, October 21, 2020. https://www.c3sindia.org/defence-security/how-effective-is-chinas-a2-ad-in-the-south-china-sea-by-commodore-v-venugopal-retd/.

Wittman, Rob. “United States Must Continue Investing in a Strong, 355-Ship Navy.” TheHill. The Hill, February 10, 2020. https://thehill.com/blogs/congress-blog/foreign-policy/482344-united-states-must-continue-investing-in-a-strong-355-ship.

Images

Figure 1: “The Odds on a Conflict between the Great Powers.” The Economist. The Economist Newspaper, January 25, 2018. https://www.economist.com/special-report/2018/01/25/the-odds-on-a-conflict-between-the-great-powers.

Figure 2: Scammell, Robert. “Astrocast Announces Three Partners to Pilot Its IoT Nanosatellite Network.” Verdict, January 7, 2019. https://www.verdict.co.uk/astrocast-partners-pilot-nanosatellite/.

Figure 3: Javorsek, Daniel. “ Adapting Cross-Domain Kill-Webs.” DARPA RSS. DARPA, 2020. https://www.darpa.mil/program/adapting-cross-domain-kill-webs.

Figure 4: Rogoway, Tyler. “Everything We Learned From Boeing About Its Potentially Game-Changing Loyal Wingman Drone.” The Drive. The Drive, May 4, 2020. https://www.thedrive.com/the-war-zone/33271/everything-we-learned-from-boeing-about-its-potentially-game-changing-loyal-wingman-drone.

Figure 5: “Trolley Problem.” Wikipedia. Wikimedia Foundation, February 21, 2021. https://en.wikipedia.org/wiki/Trolley_problem.

Figure 6: Roser, Max, and Hannah Ritchie. “Technological Progress.” Our World in Data, May 11, 2013. https://ourworldindata.org/technological-progress.