Accountability in Data-Centric Warfare: Insights from a former insider

Lisa Ling · Whistleblower, former Technical Sergeant, US Air Force Drone Surveillance Program, US

28 November 2024

DISRUPTION NETWORK INSTITUTE

INVESTIGATING THE KILL CLOUD

Information Warfare, Autonomous Weapons & AI

Director & Editor: Tatiana Bazzichelli

Creative Producer & Layout: Jonas Frankki

Copy Editor & Proofreading: Janine Römer

Disruption Network Institute
disruption.institute

Disruption Network Institute is a project
of Disruption Network Lab e. V.
disruptionlab.org

Accountability in Data-Centric Warfare: Insights From a Former Insider

Lisa Ling · Whistleblower, former Technical Sergeant, US Air Force Drone Surveillance Program, US

Published 28 November 2024

There is now enough declassified information to engage in a robust dialogue about what is happening behind connected autonomous and semi-autonomous drone platforms. This research draws on a number of available documents calling readers to look beyond the symbols of modern Network Centric Warfare and calls into question if ethical use, effective oversight and/or good governance of these emerging technologies and military frameworks is even possible in the current context.

The views expressed are those of the author and do not reflect the policy or position of the US government or military, nor do they contain classified, operational, or other protected information.

Lisa Ling began her military career in the early 1990s as a medic and nurse. She became recognised for her information systems skills, and was encouraged to enter the combat communications field, where she participated in the operations, maintenance, and security of networked communications technology. The Intelligence Surveillance Reconnaissance (ISR) enterprise required more people to build and operate it, so her Combat Communications Squadron was assimilated into the Drone Program and moved to Beale Air Force Base. During her Military Career she was sent to various locations, including the DCGS headquarters at Joint Base Langley-Eustis in Virginia, an Air National Guard site in Kansas, as well as several overseas deployments. Lisa served her last active-duty assignment with the site at Beale Air Force Base in California. After her military service, she travelled to Afghanistan to see first-hand the effects of what she participated in. She has a BA in History from UC Berkeley.

This paper takes a closer look at what the author has come to call the “Kill Cloud,” a rapidly growing networked structure of global reach with the primary intent of dominating every conceivable spectrum of warfare. There is a need for critical analysis of how the “Kill Cloud” operates, to interrogate this vast system of systems as it exists today and as an evolving weapons framework. Its architects seek to incorporate connecting, disconnecting and traversing data from different ingestion, dissemination, targeting, and killing technologies, with states, militaries, corporations, agencies, individuals, and government entities. The Department of Defense (DOD) has developed an insatiable appetite for mass quantities of data from a multitude of sources. The weapons industry of today is not only big data, big compute, data brokers and others that were not previously broadly considered part of the military weapons acquisition, engineering or procurement chain; now it includes companies such as Microsoft, Google and Amazon Web Services (AWS) as integral parts of the military weapons ecosystem. This research attempts to answer the following questions: Will too much data from disparate sources be able to render and distribute information necessary to do enough to protect civilian life in a theater of war, as required by International Humanitarian Law? Will the Boyd cycle, a framework often presented as four distinct states represented by the acronym for Observe, Orient, Decide, Act (OODA), scale from an individually situated perspective to a framework that can successfully protect civilian life when implemented on a multi-platform, multi domain weapon system while prosecuting war? Will a reliance on AI within this massive system hinder the ability to regulate autonomous and semi-autonomous weapon systems or make investigations of war crimes aided by this technology impossible to pursue?

I begin with a general overview of what I have come to call the "Kill Cloud." Then I provide an autoethnographic history to explain how I have come to my situated perspective of these and other emerging military technologies and to illustrate the sometimes subtle encroachment of such technologies into our daily lives. As a baseline, and as a reference, I examine the Aegis Weapons System (AWS), an autonomous weapon that is initiated by a human to achieve autonomous targeting when a specific criterion is met, followed by a brief explanation of the Distributed Common Ground System (DCGS) using unclassified publicly available information. Drawing on a number of available documents, I will then ask readers to look beyond familiar military devices like tanks, planes, and drones to engage a newer 'connect and surveil' military targeting paradigm that expands the current notion of a battlefield. War was once geographically determined; today's modern weaponry can project power from and to anywhere on Earth, making global war an actuality and borders less constraining with regard to the use of military force. Add the ability of a government contracted Space X to move the equivalent of a C-17 payload in less than an hour, and another geographic barrier to war is removed.[1] This work attempts to examine connected weapons systems and their global reach, calling into question if ethical use, effective oversight and/or good governance of these emerging technologies and military frameworks is possible. Additionally, the fog of war, corporate, military or intelligence community secrecy along with any bureaucratic hurdles that come with it, will further demonstrate how finding or creating instruments capable of oversight and/or good governance of these weaponized multi-use technologies, within a global weapons system, will be a particularly complex undertaking. Much of these evolving systems and moving parts have yet to be classified, so where they fall under International Humanitarian Law (IHL) remains

[1] Published, "US Military Eyes SpaceX Starship for 'Sensitive and Potentially Dangerous Missions.'"

unclear. By using autoethnography, along with supporting open-source documentation, I pursue these questions from the vantage point of a former military service member and participating military technologist, an insider who spent time working with many of these and prior stove piped systems as they evolved. The views expressed in this paper are my own and do not reflect the policy or position of the US government or military, nor does this paper contain classified, operational, or other protected information.

When I first entered military service in 1991, for much of the general public, computer and communications equipment was not broadly thought of as weapons technology in the same way it is today. At the time, it was still viewed as an efficiency improvement tool used mostly for office work to increase production; later, it was used to reduce the massive amounts of paper the initial use of technology created.[2] It was a transitional period when the Army was starting to move toward what they called an electronic culture.[3] What I understood then about computer automation and communications technology used during war was that documents still needed processing from a battlefield, radios and telephony were used to communicate the mundane, and encrypted systems could communicate battle plans and logistics information. It was common knowledge that cameras were placed on surveillance airframes, and satellite technology was used to do various transmission and/or surveillance tasks. I knew nothing about information warfare other than propaganda existed and states participated in it. I learned to identify different weapons, which ones were ours and which ones were not, and that some were "smart", and others were not. I knew that there were remotely detonated weapons like Claymore mines, but those were different and were not networked as such. That was all I knew about the technology used in war. Basically, I knew what all trainees are taught, just enough to go fight and possibly die in a war somewhere when physically deployed far from home. During Army Basic Combat Training (BCT), all soldiers were trained as infantry first, before any other skills so we would understand the importance of knowing how to fight in war as newly minted practitioners of the profession of arms. We learned to "shoot, move, and communicate" in areas where there were copious amounts of trees, bugs, foliage and mud. We learned to conceal ourselves, dig foxholes, assemble small groups of us into a hasty defensive position, create shelter, and perform well in simulated ground combat exercises. During BCT and the Advanced Individual Training (AIT) that followed, we were educated on the importance of the infantry for the prosecution of war. It was drilled into the consciousness of every new soldier that we were either part of the infantry, or that we would be spending our careers supporting it. Along with that knowledge, we were all provided with an abundance of infantry style training, regardless of what each of our primary duties

[2] THE ELECTRONIC CULTURE.

[3] Ibid.

would be. I was formally trained as a combat medic, surgical technician, and a nurse; what I did with technology following my initial army training, was a side job or an additional duty – until it wasn't.

In 1991 when I initially joined the military, I went to basic training and then to Advanced Individual Training (AIT) to train as a combat medic. A combat medic is a soldier who administers emergency medical care in both combat, and/or humanitarian deployments. Shortly after graduating AIT, I started full-time duty as a medic for a National Guard officer training school in California before continuing on with more medical training. Later, while there, I entered the main office to fill out mandatory paperwork when I saw several exasperated officers standing around a computer irritated about a report that they could not get to print. As a low ranking private, I nervously offered to help them. It took me only a moment to notice a missing orange comma delineating a column on the cathode ray tube, so I replaced it. I then navigated the cursor to print, pressed the return key and watched the document begin to print on a dot matrix printer before proceeding with the business that brought me there in the first place. Apparently, that single moment changed the trajectory of my military career for good. I found myself doing both computer and medical work for the same commanders who were having difficulty printing their report. It was there I taught myself dBase III to program something of a user interface to collect data about unit members and where they performed duty, or what skill identifiers they had. Lotus 1-2-3 still managed payroll in many places as it was the state of the art for spreadsheet technology. Man-days was a Lotus1-2-3 creation used for payroll and there was also a text based office suite called Enable that we affectionately called "disable". At the time, the military used Banyan Vines, Novell, Unix and DOS; Windows came later. The army was not yet connected to the Air Force in many places; joint exercises or logging other services on to the same networks and devices could still be a challenge when newly implemented domains and access controls were used. Systems at that time were neither uniform nor coherent, they were a sometimes-connected hodge podge of machines and software. Sometimes compatible with one another, sometimes not. When graphics and pictures could be displayed as a means to individually personalize systems, the view in many offices was more locker room pin-up than professional. Fortunately, when screensavers were available it was mostly fish, pipes and stars that were displayed; many computers were connected and managed by administrative staff who were held accountable for what was available, used, or displayed on their systems.

By 1997, many officers still connected to the "Internet" via America Online (AOL), and it was their preferred mode of communication, even for military business. America Online was a private company, but no one seemed too concerned at the time. PINE, a text-based email program, was sometimes still used. Graphics were still being simulated with overlays on cathode ray tubes (CRT) computer monitors, not quite rendered as they are now. This made the new presentation technology far more daunting and cumbersome than software like PowerPoint or Canva. Back then, programming was done with Turbo Pascal and ADA with a smattering of SQL. I used these languages to program things the officers above me and my coworkers wanted to use for daily tasks. The mouse was a relatively new addition to the office computers, alongside a keyboard, as an everyday user interface when we got the first iteration of Windows. The military was often behind on new technology, but in 1992 with the release of Windows 3.1, it almost looked like we were catching up with the rest of the world. In reality we were still using old Zenith Data Systems and other proprietary computers with large optical disks the size of record albums. This was where I began to use tech in the military. Tackling presentations from a presentation creator system packaged in a large suitcase, building networks, assembling computers from reclaimed spare parts, recovering lost files, networking classrooms, setting up old school telephone switches, affiliating field phones, and installing such things as the recently released Mavis Beacon Teaches Typing[4] for the new 71L administrative MOS troops.[5] Honestly, I had a mind for technology – it fascinated me and it was fun, so I continued doing both tech and medical assignments for years, until there was more tech and less medical to be done.

Communications and computer technology was not a weapon per se, nor was it weaponized broadly as it is today; it was a tool mostly used to get mundane office tasks done, expedite training, or to give touch-typing speed tests to groups of new administrative soldiers. It was also used for communication devices, radios, or for the field telephones and switches I used as a combat medic. Working with different technologies and fixing things that broke was interesting and I continued to be tasked with more and more of it. It justified the supervisory medical slot I was often placed in so I could continue to be used as both a technologist and a medic. People with my knowledge of computers, programming, and software were rare at that time and badly needed in the military. As a result, I was able to work in some highly coveted indoor spaces. I still made use of a local BBS[6] with my personal computer before and after it became an Internet Service Provider (ISP) called Fix.net.[7] I brought my personal computer into my office to be used for work with the agreement of the commander that I could stay on-site late into the night to connect to my BBS or write code. When I returned from the deployment we were preparing for, I got a

[4] "Mavis Beacon Teaches Typing Was a Software Program First Released by *Software Toolworks* in Late 1987. It Was Useful for Practice, and to Administer Touch Typing Tests to an Entire Classroom of Students Replacing the Cumbersome Task of Testing Students on Typewriters."

[5] Wikipedia Editors, "A United States Military Occupation Code, or a Military Occupational Specialty Code (MOS Code), Is a Nine-Character Code Used in the United States Army and United States Marine Corps to Identify a Specific Job. In the United States Air Force, a System of Air Force Specialty Codes (AFSC) Is Used."

[6] Wikipedia Editors, "A Bulletin Board System (BBS), Also Called a Computer Bulletin Board Service (CBBS), Is a Computer Server Running Software That Allowed Users to Connect to the System Using a Terminal Program. Once Logged in, the User Could Perform Functions Such as Uploading and Downloading Software and Data, Reading News and Bulletins, and Exchanging Messages with Other Users through Public Message Boards and Sometimes via Direct Chatting. In the Early 1980s, Message Networks Such as FidoNet Were Developed to Provide Services Such as NetMail, Which Is Similar to Internet-Based Email."

[7] "Fix Net Archive" is still available at https://web.archive.org/web/19980109152404/http://www.fix.net/."

steep bill from the base communications command. While it was not a long-distance call to access the BBS, the base charged me personally for off-site calls. Back then, being charged for telephone connections was common. Neither my commander nor I knew about the charges, so the best we could negotiate was for me to pay half of what I was charged. Back then, connecting had a price; I mention this to juxtapose it with how impossible it is to not be connected today. Early on, the changes were subtle, very few saw it coming. On the plus side, my technical skills afforded me opportunities that some would consider rare. Eventually, mostly due to post 9/11 deployments, I gave up my nursing MOS and was transferred to the Air Force overnight, donning an Air Force uniform the very next day. The paperwork followed and the Air Force deployments began; I was waivered into a communications Air Force Specialty Code (AFSC), which meant I did not have to go to an Air Force Training Base. An AFSC is the same as an MOS, essentially a military job title. MOS is used by the Army, and AFSC by the Air Force. I was awarded mine after the waiver went through channels. From then on out, I became a combat communications troop, not knowing what that would mean or what I would do with it in the field. All of these experiences allowed me to witness different aspects of communications and infrastructures; after working with transmission, I began to appreciate the nature of discretion as data sharing one's personal information became normalized. People did not really notice, as storage devices grew and backups became more and more cumbersome, until the day it became a contractor's sole responsibility to back up our work lives onto magnetic tape, erasing what we once knew as privacy in our workplaces.

During my early Army years, credit cards were rarely used, and they were not yet mandated for military or most corporate travel use. In the '90s paper checks or cash were the go-to spending instruments. When service members required military travel pay, personnel waited in long lines for a cash advance equal to the per diem they would be entitled to for travel. Government travel cards came later. Using credit was not digitized like it is now; accepting credit cards was still a manual process that required a mechanical contraption to place an imprint of the card onto a paper form that was written on with black or blue ink by the cashier to complete a transaction. While the use of credit cards issued by retail outlets were common in the '70s, the use of bank type cards did not pick up significantly until the late '80s to early '90s. By 1995, bank type credit cards were the most common type of card in use.[8] There were already rumors about the evils of having and using credit cards, or "plastic" as they were often called at the time. Many people still preferred to use cash and blamed credit cards for various societal ills, some along religious lines as my then-supervisor disclosed to me on numerous occasions. He suggested they were 'the mark of the beast,' and I thought he was a bit paranoid. As it turns out, he was right

[8] Durkin, "Credit Cards."

to be wary. We did not yet know how these cards would follow our shopping and travel habits, gleaning personal data as we used them. Did we purchase alcohol? Medications? What books did we read? What meals did we eat? Whose cards were used in proximity to ours? Was there an aura of guilt by association to be gleaned from their use?

When soldiers and airmen first received their travel cards, they were issued by Bank of America (B of A). There were interesting stories of how young service members used their government B of A cards for weddings, to purchase expensive goods like cars, to buy and borrow trouble on a large scale. Slowly users began to learn that they would get caught, and the rumor mill was awash with stories about crazy exploits paid for with military travel credit. This information was kept close, service members were given numerous chances to quietly pay up before it scarred their personal records. Administrative staff began to manage soldiers by turning their cards on to travel and off when personnel were no longer on travel orders. When outside agencies began to catch up with those who did not pay their bill, it was grounds for a transfer or an abrupt exit from military service in some cases. If a supervisor had trouble finding a young private, we could call a travel card administrator to find out where their card was last used. The doctrine began to catch up to the new payment method, and limits were put on which establishments could accept military plastic. As the use of bank cards increased, so did the amount of data that could be collected about individuals at home and abroad. For those of us working at a headquarters, it was easier to keep track of soldiers. The cards were fraught with problems as they were implemented without sufficient doctrine in place to govern their use. Perhaps it was a missed lesson, one that I look back on as being minimal compared to the guardrails necessary for the burgeoning technologies of today. One could argue that the beginning of data capitalism started in the mid-1990s. Sarah Meyers West examined the "...1990s as a period of technological and economic change for the nascent Internet industry, during which companies turned from an understanding of the Internet primarily as a marketplace for the sale of goods to one that placed primacy on the role of technology in the production and harvest of users' data."[9] I did not realize it at the time, but I was experiencing major changes in military technology and surveillance as it happened from the vantage point of a military technologist. What I did not yet know was just how much the experience would shape my view of the systems used for war. I was watching, using, and building technical solutions for the military as it evolved. I worked on a multitude of different databases, connected and troubleshot different systems, but nothing could have prepared me for the intrusive systems in contemporary use, or for the massive amounts of our personal data being exploited by individual, state, and commercial entities, every single day. To be honest, I did not want to know how or if

[9] West, "Data Capitalism."

computers and communications equipment were being used to target or kill. Up to that point, the closest I had been to connected weaponry was the Claymore mine. Every army troop was taught how to use the Claymore anti-personnel mine in basic training. I did not think of it as a connected or remote weapon, but it was a remotely detonated and rudimentarily wired portable anti-personnel weapon system, with a detonation device that transmits 3 volts of electricity over a wire to ignite. It was a simple but deadly device one could point, connect, and use to kill numerous enemy personnel with a single button press, an ominous sign of what followed. Despite that, once I passed the practical exam for the Claymore in basic training, I quickly put it out of my mind until this writing. When I think about it, I was privileged to be able to put weapons and war out of my mind for much of my military career, especially during some of my early army deployments. Ironically, technology has always been a distraction for me, until I recognized its dual use.

Anyone who has been through basic military training knows that killing, if deployed to war, is a distinct possibility for every soldier, but it was not something many of us thought much about in the '90s. We certainly did not envision killing with the same technology used to send an email or connect Mavis Beacon to a typing class, but that is essentially what happened. We didn't envision credit cards as targeting data, but here we are. It is frightening to consider so many technologies as being both so beneficial and so lethal depending on their configuration and use. As multi-use technologies were becoming more commonplace, this could create obstacles with regard to how they could be effectively controlled and governed. The switch from analog to digital transmission brought more connected devices permeating every aspect of human life. Frequency Division Multiplexing (FDM), used to transmit data in bulk, then became Time Division Multiplexing (TDM); more bits shoved into time slots than across single frequencies, more connections, and longer hauls, with many of the same speed limits as before, but that too was changing rapidly. Code Division Multiplexing (CDM), also called Code Division Multiple Access (CDMA), could then hold more users, and is not limited by bandwidth but by power and codeword length. It is not important to understand FDM, TDM, or CDM technology, only that each made room for more users and more data over multiplexed circuits. Today the Internet of Things (IOT) can include children's toys, printers, refrigerators, and much more deadly devices that most of us would prefer not to learn about, but many of us did.

Even the least curious and technologically uninitiated learned about weaponizing connected devices when electronic pagers and radios began simultaneously exploding across Lebanon and Syria on the 17th and 18th of September 2024. The Internet itself is composed of a plethora of connected multi-use devices. Communications equipment can be weaponized, similar to this recent detonation of pagers and radios, an act condemned by United Nations UN human rights experts as "terrifying" violations of international law.[10] Israel aimed to kill or injure not only the user, but anyone who was close to the devices. The "Kill Cloud," like the Internet, is a connected space that is difficult if not impossible to govern or control. These connected technologies have many, if not all of the same attributes and/or components, regardless of what is connected to them or how they are used. While most people blissfully ignore the fact that connected weapons exist, this is a privilege that few will be able to maintain long-term. Unless we collectively address their use in a constructive way, this category of weaponry could become normative inside and outside combat zones. As we witness what is happening in Palestine, Syria and Lebanon, few will remain uninitiated with respect to what is possible with the weaponization of connected devices. It is important to understand that nobody is immune to such attacks; such targeted attacks can happen anywhere there is connectivity, anywhere there is data that can be accessed to do so.

After September 11th, 2001 (colloquially 9/11), armed conflict was all many of us were thinking about as we deployed multiple times to several different combat zones, military bases, or even airports. I had already been sent to Washington DC to work on a database when 9/11 happened and was immediately thrust into the center of supporting high-ranking individuals with technical solutions. I was the only one on temporary orders, so I was not obligated to wait for any existing contracts to be fulfilled before I was able to touch the equipment and enter a Secret Compartmented Information Facility (SCIF). I ended up being positioned there for over a year while a new post 9/11 reality took hold. Multiple deployments happened both physically and virtually for some of us; for those who did not deploy, their working hours increased by a lot. Many Service members with communications skill identifiers were deployed overseas, and some – including me – were pulled into the drone program. My unit, once a Combat Communications Unit, was assimilated into the drone program. We were assigned to a unit hosting the Distributed Common Ground System (DCGS) upon returning home from a physical deployment. "The Air Force Distributed Common Ground System is also referred to as the AN/GSQ-272 SENTINEL weapon system,"[11] according to the U.S. Air Force. "It is the Air Force's primary intelligence, surveillance and reconnaissance collection, processing, exploitation, analysis and dissemination system. ...The weapon system employs a global communications architecture that connects multiple intelligence platforms, sensors, and sites. Airmen assigned to AF DCGS produce actionable intelligence from data collected by a variety of data sources, to include sensors on the U-2 Dragon Lady, RQ-4 Global Hawk, MQ-9 Reaper and other ISR (Intelligence,

[10] "Exploding Pagers and Radios: A Terrifying Violation of International Law, Say UN Experts."

[11] US Air Force, "The Air Force Distributed Common Ground System Is Also Referred to as the AN/GSQ-272 SENTINEL Weapon System."

Surveillance and Reconnaissance) platforms."[12] In a nutshell, the DCGS is a system that consists of the equipment and personnel to ingest multiple data streams from multiple platforms, and to analyze and/or distribute data to customers who want or need it. At least that is what multiple contractors, government personnel, and others have posted online. The DCGS was once part of the fledgling concept of a new data dependency, a paradigm shift that continues to redefine the military notions of military reach, and of what constitutes a combat zone. When armed peripheral surveillance devices are connected and controlled remotely from anywhere, it changes the character of war.

I never cared for the drone program once the airframes were armed. I have always felt that if the reason for war is not critical enough to place soldiers into the physical proximity of a contested area or combat zone when dropping ordnance or surveilling a population, then we shouldn't be dropping ordnance or conducting war there. Ethically, I preferred physical deployments; I believed, and still do believe, that there is something profoundly wrong with telecommuting to combat. It makes war far too easy for politicians and war-makers. I do not believe technologically mediated killing from the other side of the globe can reasonably be conducted with the necessary situational awareness to truly know who is or is not an enemy combatant in counterinsurgency operations. I do not believe going after a single individual with a missile is proportional, nor does it allow for an avenue of surrender when a connected airframe, like the Reaper, is used, even though it is required by international law. When I also consider the constant surveillance of innocent people of all ages, it is not something I would have willingly signed up for – if I had known more about it – before entering this once highly secretive program. Unfortunately, once I was in, it was very difficult to leave due to the endless staffing shortfalls.[13]

I loved early technology: the promise it held for bringing people together, the access it gave to people in developing countries, the encyclopedic amounts of information that became available to anyone with a device that could connect to a Bulletin Board System (BBS), and the fledgling Internet. In the late '80s and early '90s, technology was exciting and the promise of decreased workloads for those who used staplers to collate typewriter-generated documents sounded better and better. Keyboards took much less effort to type on, and even the simplest of word processors ended the need for the numerous small bottles of Wite-Out or correction tape, which required some artistry and skill to cover some of the more egregious errors. (The truth is that most of us just started documents over to avoid the tedium of error corrections; back then, there were relatively few documents to type compared to the number of documents created and stored after automation initially took hold.) In time, what happened for administrative work was different and far less exciting.

[12] US Air Force.US Air Force, "The Air Force Distributed Common Ground System Is Also Referred to as the AN/GSQ-272 SENTINEL Weapon System."

[13] "Norton - Staffing for Unmanned Aircraft Systems (UAS) Ope.Pdf."

Neither the production of documents nor individual workloads decreased. Instead, workloads increased exponentially. As the rate of return on technology increased, so did the acquisition, dissemination, and storage of data. What actually happened as a result of technological proliferation was indeed ironic: less paper, but reams more data to manipulate, manage, store and distribute. Less paper, juxtaposed by more work, more personnel, and increasingly more data. This change placed many soldiers in front of computers for most of the workday. This included manually inputting all types of personnel and personal data, from simple memos to advertising and recruiting material, and of course later the massive quantities of what became known as 'intelligence' data. Ultimately, some of those very same types of data could be used to determine whether or not to kill someone on the other side of the planet. The integration of automation started as a way to work more efficiently, to eliminate the endless reams of paper churned out by the military after its initial adoption of office computers and printers. The end result was an insatiable appetite for surveillance and data collection.

The use of computer technology in war is not new. Computers have long played a part in warfare, from organizing air defenses to decrypting Nazi codes in WWII, but it was definitely not the basis for military weaponry. "In the 1950s computer manufacturers had estimated that six computers could serve the needs of the entire United States. By January 1968 fifty thousand computers were operating in the country, of which fifteen thousand had been installed in the past year."[14] In 1969, the precursor to the Internet began with the U.S. Defense Department's ARPAnet who funded the development of many of the networking protocols that are still used today. In the 1980s, there was university access to network iterations like NSFNet, sponsored by The National Science Foundation.[15] Dial-up access to the internet was more widely available in the early 1990s, and with it came hope for what was going to be possible as a result of the World Wide Web (WWW). Things that seem relatively simple and low-cost by today's standards were groundbreaking back then. A simple phone call to a cousin on the opposite coast from a dial-up telephone attached to the wall could be an expensive undertaking. Friends and family plans priced at 10 cents per minute, and more when multiple operators were needed. Time spent on calls was manually calculated for billing purposes, until it was automated. Human operators wouldn't be completely phased out until January 1st, 2023.[16] Early on, we could connect with people all over the world using Internet Relay Chat (IRC). IRC was similar to what social media is today minus the destructive algorithms. Pictures and emojis could be shared while we chatted about whatever parts of the world we were in. We played around with Voice Over IP (VOIP), and sometimes still arranged

[14] Kurlansky, 1968.

[15] "A Brief History of NSF and the Internet."

[16] "Operator and Directory Assistance Is Ending."

to meet face-to-face (F2F) across cities, states, and even countries. Not many were focusing on the Defense Department's involvement in the bourgeoning internet until Yasha Levine, a Russian American journalist, wrote about its military beginnings in his book *Surveillance Valley: The Secret Military History of the Internet.*[17] In 2018, when it was first published, it was considered a must-read for hacker communities everywhere, but the promise of connectivity with different cultures and people everywhere overshadowed the nascent beginnings of a united future. Many of us were distracted by the possibilities of what this new global connectivity could foster.

None of even the most experienced soldiers I worked or spent time deployed with, saw telecommuting to battlefields in our future. I certainly did not see it coming. Data collection, sales, and dissemination have become the keystone of all that we do, and all that we are. Most of our lived experiences are somewhere online; endless amounts of our own personally generated data follow us wherever we go, across locations and lifetimes. It is hard to imagine from the vantage point of today that this was not always the case, but there was a time when telephones and computers were tethered to our homes and offices as we roamed away to the great outdoors, free of connected devices. There was a time when privacy was respected while simultaneously taken for granted. There was actually a time when surveillance cameras were not nearly as prevalent as they are now, and when cameras were installed, they were on closed circuits where people had to physically access them to collect video footage. Laws back then required there to be signage letting us know where cameras were used. We did not see the trajectory we were on until it was too late, until there was no turning back. The financial and surveillance incentives were just too great. NSA intelligence contractor and whistleblower Edward Snowden put it best when he wrote: "If government surveillance was having the effect of turning the citizen into a subject, at the mercy of state power, then corporate surveillance was turning the consumer into a product, which corporations sold to other corporations, data brokers, and advertisers."[18] I believe that Snowden may have known, before the rest of the world, that this very data was being purchased and used by militaries and contractors to contribute to life-and-death decisions on modern battlefields. Another effort amounted to killing faster, building on the shock and awe of the Iraq War. John Boyd's OODA loop became the codified decision-making doctrine, used to increase the kill ratio in a way that oversimplifies targeting. What was once a system conceived of by an Air Force fighter pilot is now a central part of a novel war-fighting framework. John Boyd first conceived of the OODA loop as the process he used as a fighter pilot. He used the OODA Loop as a targeting/maneuvering tool whereby the decision-making cycle was compressed using a kind of muscle memory training approach to speed up the assessment process from within the cockpit. A way to

[17] Levine, *Surveillance Valley.*

[18] Snowden, *Permanent Record.*

orient and situate himself while piloting before and during combat, to survive and win in the air. In the context of dog fighting, it makes a lot of sense to compress the time it takes to make decisions, because in that context, every decision is potentially one of a pilot's life or death. As a nurse, we used the same kind of tools when triaging mass casualty events, when there was a limited time frame to effectively do otherwise. But can this approach scale to a modern interconnected battlefield while still following International Humanitarian Law?

The current Israel/Palestine war has Israeli forces fighting asynchronously and asymmetrically with an insurgent force using an Artificial Intelligence (AI) enabled targeting system. According to WestPoint's Lieber Institute, and Ploughshares, a Canadian peace research institute, the IDF acknowledged using Gospel and other similar systems like "Alchemist" and "Depth of Wisdom" in May of 2021 during Operation Guardian of the Walls. According to Ploughshares, the IDF used data from satellite imagery and signals intelligence in at least three AI decision-making support systems developed by Unit 8200, the IDF intelligence corps responsible for clandestine operations signal intelligence (SIGINT) collection. Unit 8200 dubbed the action "the world's first AI war".[19] Not long after that, on May 25th, 2021, Google announced that it had been selected for a four-phase project known as Project Nimbus. This project was described as a "multi-year flagship project led by the Israeli Government Procurement Administration, that is intended to provide a comprehensive framework for the provision of cloud services to the Government of Israel".[20] There was nothing in Google's initial announcement that described what specific services would be provided; that information came over a year later with the help of Jack Poulson at Tech Inquiry, who found it on a publicly available procurement feed. Google is providing Israel with advanced artificial intelligence and machine learning tools capable of supporting the IDF with surveillance and targeting. Of course, the latter is not without error. According to the Intercept, "Google workers who reviewed the documents said they were concerned by their employer's sale of these technologies to Israel, fearing both their inaccuracy and how they might be used for surveillance or other militarized purposes."[21] Some military experts from the US and elsewhere are putting faith in algorithms augmented by AI, where AI assists a human in the decision-making process with a goal of shortening the decision loop. Augmented intelligence is a subset of artificial intelligence in which AI technologies assist humans rather than replace them.

The Palestinian people have lived under panoptical surveillance for decades. The knowledge that the same technology doing the surveilling could also send an autonomous or semi-autonomous system to kill is terror, without ever firing a shot.

[19] "AI Targeting in Gaza and Beyond."

[20] "Google Cloud Selected to Provide Cloud Services to Digitally Transform the State of Israel."

[21] Biddle, "Documents Reveal Advanced AI Tools Google Is Selling to Israel."

Watching the devastation and carnage happening in Palestine, even from a place of privilege, is hard. I could not imagine what it would be like to have family living there.

What is being used in Israel today, is not the first automated targeting system used in a theater of war. The Aegis Weapons System (AWS) uses technology to track and guide weapons to destroy hostile aircraft. AWS is a centralized, automated, C2[22] and weapons control system that was designed to automatically move from detection to kill without the necessity of human intervention, once it has been set to weapons free. The US Navy describes the system as using the AN/SPY 3D radar system, an advanced automatic detect and track, multi-function phased-array radar. “This high-powered radar is able to perform search, track and missile guidance functions simultaneously, with a track capacity of more than 100 targets. The first Engineering Development Model (EDM-1) of the SPY-1 was installed in the test ship USS NORTON SOUND (AVM 1) in 1973.”[23] The weapon is designed to target any aircraft not sending out a friendly signal. In a contested area, any aircraft not sending out the appropriate signal is considered to be hostile. Unlike Lavender, a targeting system that is currently in use by Israel against Palestine, the Aegis looks for a specific internationally recognized signal. According to the Stop Killer Robots Campaign, Lavender bases its targeting recommendations on behavioral attributes, including communications patterns, social media connections, and frequent address changes. The campaign contends that “Lavender is a data processing system, not an autonomous weapon, and the actual decision whether or not to strike a recommended target is made and carried out separately by a human and not a machine. However, the use of this system demonstrates key issues with autonomous weapons, namely digital dehumanization and loss of meaningful human control.”[24,]

The Aegis is not AI-enabled, nor is it generally used as an offensive weapon. The Aegis, when fully autonomous for targeting, uses a simple binary criteria: is there a squawk identifying the airframe as civilian, or not? Conversely, Lavender weeds through massive amounts of information. The AWS is used to defend Navy ships and personnel with clearly defined targeting parameters that profile who is and is not considered a hostile. It is used to defend clearly defined physical spaces, vessels, and personnel. When the system is fired autonomously, an investigation can reveal whether targeting parameters have or have not been met. Unlike AI targeting systems, decision parameters or variables are not purported to be in an impenetrable black box where the logic for choosing a target is inaccessible due to corporate secrecy, patents, complexity, or state secrets. While it may not technically be a black box, it is not the same as the automated audit trail offered by the Aegis system.

[22] “The US Department of Defense Dictionary of Military and Associated Terms Defines Command and Control as: "The Exercise of Authority and Direction by a Properly Designated Commander over Assigned and Attached Forces in the Accomplishment of the Mission. Also Called C2.”

[23] “AEGIS Weapon System.”

[24] “Use of Lavender Data Processing System in Gaza.”

Oversight of the Aegis is possible because the decision criteria are simple and clearly established; actions performed by the system are logged and can be audited. Responsibility for the firing of the Aegis ultimately rests with the ship's commander when used by the Navy from a Navy vessel. This type of clarity and transparency is helpful to good governance and, when needed, a solid investigation revealing whether the targeting criteria was met is possible. Even under these clear-cut parameters, the fog of war can still muddy the waters, but at least there are accessible system-generated logs that can be used for clarity.[25] Of course, investigations during wartime are fraught, and in the end not all sides will publicly agree, as happened with Iran Air Flight 655 on July 3rd, 1988. The civilian plane was shot down during the Iran-Iraq War by the USS Vincennes, a Ticonderoga-class guided missile cruiser equipped with the Aegis combat system. According to the United States, the Vincennes's crew misidentified the aircraft as an F-14 Tomcat, a fighter jet, despite it transmitting proper identification codes, as was seen during the subsequent investigation.[26] The investigation revealed a plethora of errors, and the US ultimately paid the survivors while not taking responsibility for the incident. As it turned out, despite conflicting information from Navy personnel, the Aegis recorded that the airliner was climbing and its radio transmitter was squawking on the Mode III civilian frequency, not military Mode II. Shortly after lift-off from an airport that serves both military and civilian aircraft, Iranian Flight 655 was (mis)identified by crew members on the USS Vincennes as an F14 fighter plane; in an uncertain environment, it appears that was not broadly questioned.[27] The civilian plane had its transponder on, used a squawk code that identifies it as a civilian aircraft, and yet it was shot down. Could this be the canary in the coal mine when it comes to the use of AI in war?

After being read into the drone program, I began to understand that international legally binding instruments limiting the destructive nature of connected systems was badly needed, yet this was not discussed publicly due to the secretive ecosystem. Today, the DCGS is old news, yet it remains a window into what the future of war might look like. I trained on and saw various interconnected parts of the system in several different locations. I spent a short time working maintenance on an airframe as well. From the moment weapons were mounted on these hovering connected data collection and distribution platforms, the mission priority of drone systems changed from a defensive surveillance tool used to watch over and protect troops on the ground, to a belligerent and bellicose weapon. The addition of an AI targeting system, similar to what is being used by Israel today, could dramatically change the system to one capable of data-driven unimpeded mass destruction by targeting and

[25] Department Of Defense Washington Dc, "Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988."

[26] Colum Lynch, "Anatomy of an Accidental Shootdown."

[27] Colum Lynch.

dropping munitions on “combatants” faster than humans alone are capable of.[28] Of course this depends on how it is used and what procedures are in place. Gospel and other decision support systems are not considered fully autonomous because they require a person to approve the targets, but how exactly does that work? When thinking about this kind of process, I instinctively consider all of the ‘Accept’ buttons I have clicked, having not read the End User License Agreement (EULA). How many words have I let spell-check change without paying much attention? How many times I have had to press the back button because I clicked too quickly? Will there be a back button? I do not want to be callous about targeting real human beings, or buildings possibly with families inside them, but humans have the tendency to press ‘Enter’, to experience automation bias. Will the human in the loop care how or when the AI targeting data was acquired? Will there ever be more than one approval authority? What training will the individual in this position be subject to? When I consider questions about any automated process, the accuracy of AI is still highly suspect, and the training data used is more than likely not going to be known. I am sure the training data will include “targets”, but how about non targets? Is it taught who not to target? Regardless of outcomes, the commercial implications of “battle tested” systems are on the rise. The propagation of these systems will not be limited to our allies.

One of my greatest fears while a small cog inside this massive system was that the only connection to these wars was mediated through wires, screens, and keyboards; if that was the only thing between us and these brutal wars, why stop warring at all? I witnessed policymakers no longer informing the public about much of anything at all because service members are sent to places a safe distance away from the bullets and bombs. This new politically expedient way of war has won out. If that does not frighten all of humanity into policies, treaties or other measures to ensure these weapon systems are being used in compliance with international law, I am not sure what, if anything, will.

DOD’s umbrella concept for managing the combination of connected technologies I am calling the “Kill Cloud,” is described as Joint All-Domain Command and Control or JADC2.[29] The concept of JADC2 is to connect sensors from all branches of the U.S. armed forces into a networked structure that will be powered by AI in an all-out quest for an Enders' Game-like situational awareness. When I left the military in 2012, the parts of the system I understood included a massive infrastructure designed to gather and distribute a seemingly endless amount of data, much of it without proper context. Operators began tagging collected data, adding what context was available and connecting data from different sources in the hope of gathering a full picture of the current battle spaces. I worked on a DCGS responsible for ingesting and distributing data from connected weapons systems from connected

[28] Iraqi, “‘Lavender,’” April 3, 2024.

[29] “SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.”

devices that could have been located almost anywhere on Earth, whether it be inside or outside of the designated combat zones.

The goal of militaries has always been to use data to build situational awareness sufficient to be considered knowledge, albeit mediated and in many ways cobbled together from disparate sources. In warfighting, JDAC2 is the approach being used to connect and protect data, sensors, shooters, and related storage and transmission devices of the U.S. military into a resilient, agile, and cohesive system for all levels of the modern battlefield. That includes moving beyond former conceptions of war-making to the electromagnetic spectrum itself and beyond. The integration process brings Nuclear C2 and Communications (NC2/NC3) into the JADC2 Technical Enterprise.[30] The still-evolving construct aims to coordinate and connect all military assets, including personnel across all domains, thereby creating a command and control (C2) structure that is supposed to bring a competitive advantage to future conflicts. Further, the connectivity between sensors and shooters aims to speed up decision-making by using AI. Even kill decisions can be accelerated by this new technology, and that is happening well before doctrine is in place to mitigate collateral damage, or what today could very well be considered 'corporate externalities.' The connectivity will also work to modernize information sharing with military partners, in an effort to deliver what is often referred to by military stakeholders as an information advantage.[31]

Shared situational awareness and increased decision-making speed are two commonly stated objectives of Network Centric Warfare (NCW), a theory of war that asserts information superiority is a winning strategy. Information superiority has always been considered a winning strategy for C2; the difference is how the information is obtained. From battlefield maps, to spies, to cracking the Enigma code, information has always been sought by commanders in an effort to win wars. Today, information is acquired using various technologies, then it is digitally distributed in real- or near real-time according to customer and classification. Targets are also acquired using technology, and in the case of the current conflict in Palestine, the integration of AI into the decision of who or what to target is happening now.[32] The 2022 Department of Defense (DOD) Summary of the *Joint All Domain Command and Control Strategy* (JADC2), states: "The ability of the U.S. military to regain and maintain information and decision advantage is one of the Department's top priorities."[33] The summary goes on to describe, in a general way, how that is to be accomplished across the DOD:

[30] "SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF."

[31] Ibid.

[32] Iraqi, "'Lavender,'" April 3, 2024.

[33] "SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF."

> “JADC2 transcends any single capability, platform, or system; it provides an opportunity to accelerate the implementation of needed technological advancement and doctrinal change in the way the Joint Force conducts C2. JADC2 will enable the Joint Force to use increasing volumes of data, employ automation and AI, rely upon a secure and resilient infrastructure, and act inside an adversary's decision cycle.”[34]

“Acting inside an adversary’s decision cycle” is a reference to the OODA Loop, also known as the Boyd Cycle. This is an important concept because it speaks to the current goals and priorities intended to deliver a competitive edge in modern warfare. In “Automating the OODA Loop in the Age of Intelligent Machines,” James Johnson argues “that artificial intelligence (AI) enabled capabilities cannot effectively or reliably compliment the role of humans in understanding and apprehending the strategic environment to make predictions and judgments that inform strategic decisions.”[35] The Boyd Cycle consists of observation-orientation-decision-and action, repeated not necessarily in that order. It is a loop applied according to new and unforeseen circumstances that can arise on the battlefield. The OODA loop compresses the decision cycle, but crucially, with the massive quantities of data within a comparatively small timeline before a strike, is there a meaningful place for a human to remain “in the loop?” The OODA Loop decision-making framework emphases sorting currently available information, placing it into an applicable context so the most appropriate decision can be made in the quickest time, while continuing to adjust as more and more data becomes available, in what military planners call the speed of relevance.[36] This is done even in the fog of war where it would be difficult to know what the speed of relevance actually is; the goal, of course, is to glean more and more detailed and accurate information as it becomes available. The Boyd Cycle appears in a targeting methodology called F3EAD, an acronym for ‘Find, Fix, Finish, Exploit, Analyze, and Disseminate.’ This is not a new strategy; it was designed for use in Latin America. “F3EAD was designed and adapted for Foreign Internal Defense (FID) missions in Latin America in the 1980[s] to counter the growing Communist threat.”[37] As this history demonstrates, technology is vastly different than it was in the ‘80s. The technology being used to assist in parsing available data, at least in the case of Israel’s targeting decisions, is subject to hallucinations and other reasoning defects.[38,39]

[34] Ibid.

[35] Johnson, “Automating the OODA Loop in the Age of Intelligent Machines.”

[36] “JADC2.”

[37] Jimmy A. Gomez, “The Targeting Process: D3A and F3EAD.”

[38] Biddle, “Documents Reveal Advanced AI Tools Google Is Selling to Israel.”

[39] “AI Targeting in Gaza and Beyond.”

Oversight of the “Kill Cloud,” a vast connected assemblage of different technologies, is hampered not only by size and scope, but also because its legal category is as yet unclear. The National Institute of Standards and Technology (NIST) describes a weapons system as “a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment.” Clearly, the Kill Cloud, as a weapons system, or an as yet burgeoning framework, requires effective governance, doctrine and universally agreed-upon norms. An early Air Force vision of Network Centric Warfare (NCT) “anticipates a future in which each force element, no matter how small, is constantly collecting data and ‘publishing’ it (data) over the military Internet. Information would flow in from every corner, from big intelligence-surveillance-reconnaissance collectors, such as the E-3 AWACS and E-8 Joint STARS, all the way down to airmen on the ground.”[40] It is hard to predict how such a vast interconnected system will be parsed, for national or international oversight and governance. Will a new legally binding instrument require a new protocol to be added to The International Convention on Conventional Weapons? Or will there be a different process moving forward? There has been movement for years to ban fully autonomous weapons, but progress is painfully slow, especially considering its active use in Palestine. In a paper published on October 18th 2024, Heidy Khlaaf, Sarah Myers West, and Meredith Whittaker examine urgent national security risks posed by AI systems used in military contexts: "Personal data embedded within existing commercial foundation models thus positions AI as a link between commercial personal data and automated weapons’ target lists and surveillance capabilities."[41] They argue that “... even with additional data restrictions in place, no effective approaches exist that reliably prevent personal data exposure in current foundation models, from contributing to (intelligence, surveillance, target acquisition, and reconnaissance) ISTAR capabilities.”[42] In Israel, Gospel, Lavender, and Where’s Daddy, are the military decision-making systems used and they depend on personally identifiable information (PII) to target.[43] This alone is reason to define and regulate military AI systems from within their own category. As discussed, when AI is used for targeting decisions -- whether a human presses the final button or not -- the battlefield becomes the entire planet, and potential targets include every person who has ever used a credit card, cell phone, email, web browser, or any other connected device.

[40] “The Network Way of War.”

[41] Khlaaf, West, and Whittaker, “Mind the Gap.”Khlaaf, West, and Whittaker, “Mind the Gap.”

[42] Khlaaf, West, and Wittaker.

[43] “AI Targeting in Gaza and Beyond.”

References

"A Brief History of NSF and the Internet." Accessed November 1, 2024. https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

A Fix Net Archive is still available on the Internet Archive at https://web.archive.org/web/19980109152404/http://www.fix.net/, n.d.

"AI Targeting in Gaza and Beyond." Accessed November 5, 2024. https://www.ploughshares.ca/publications/ai-targeting-in-gaza-and-beyond.

"AI Targeting in Gaza and Beyond." Accessed November 5, 2024. https://www.ploughshares.ca/publications/ai-targeting-in-gaza-and-beyond.

Air & Space Forces Magazine. "The Network Way of War." Accessed November 7, 2024. https://www.airandspaceforces.com/article/0305network/.

AT&T. "Operator and Directory Assistance Is Ending." Accessed November 4, 2024. https://www.att.com/support/article/u-verse-voice/KM1511460/.

Biddle, Sam. "Documents Reveal Advanced AI Tools Google Is Selling to Israel." The Intercept, July 24, 2022. https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/.

Colum Lynch. "Anatomy of an Accidental Shootdown Three Decades Ago, a Perfect Storm of Miscommunication, Miscalculation, and Human Error in the Heat of Battle Caused the United States to Make a Mistake Similar to the One Iran Just Did." *Foreign Policy*, January 17, 2020. https://web.archive.org/web/20210228041413/https://foreignpolicy.com/2020/01/17/accidental-shootdown-iran-united-states-ukraine/. https://foreignpolicy.com/2020/01/17/accidental-shootdown-iran-united-states-ukraine/.

Department Of Defense Washington Dc. "Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988:" Fort Belvoir, VA: Defense Technical Information Center, August 18, 1988. https://doi.org/10.21236/ADA203577.

Durkin, Thomas A. "Credit Cards: Use and Consumer Attitudes, 1970-2000." *Federal Reserve Bulletin* 86, no. 9 (2000): 0–0. https://doi.org/10.17016/bulletin.2000.86-9.

Exploding pagers and radios: A terrifying violation of international law, say UN experts. "Exploding Pagers and Radios: A Terrifying Violation of International Law, Say UN Experts." Press Release, September 19, 2024. https://www.ohchr.org/en/press-releases/2024/09/exploding-pagers-and-radios-terrifying-violation-international-law-say-un.

Google Cloud Blog. "Google Cloud Selected to Provide Cloud Services to Digitally Transform the State of Israel." Accessed November 5, 2024. https://cloud.google.com/blog/topics/inside-google-cloud/google-cloud-selected-to-provide-cloud-services-to-the-state-of-israel.

Iraqi, Amjad. "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza." *+972 Magazine*, April 3, 2024. https://web.archive.org/web/20241010022042/https://www.972mag.com/lavender-ai-israeli-army-gaza/. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

———. "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza." +972 Magazine, April 3, 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

"JADC2: Accelerating the OODA Loop With AI and Autonomy." Accessed November 7, 2024. https://www.rti.com/blog/jadc2-the-ooda-loop.

Jimmy A. Gomez. "The Targeting Process: D3A and F3EAD." *Small Wars Journal Blog* (blog), July 16, 2011. https://smallwarsjournal.com/blog/journal/docs-temp/816-gomez.pdf.

Johnson, James. "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age." *Defence Studie*s 23, no. 1 (January 2, 2023): 43–67. https://doi.org/10.1080/14702436.2022.2102486.

Khlaaf, Heidy, Sarah Myers West, and Meredith Whittaker. “Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting.” arXiv, October 18, 2024. https://doi.org/10.48550/arXiv.2410.14831.

Kurlansky, Mark. *1968: The Year That Rocked the World*. New York: Random House Trade Paperbacks, 2005.

Levine, Yasha. Surveillance Valley: The Secret Military History of the Internet. New York: PublicAffairs, 2018.

“Mavis Beacon Teaches Typing Was a Software Program First Released by *Software Toolworks* in Late 1987. It Was Useful for Practice, and to Administer Touch Typing Tests to an Entire Classroom of Students Replacing the Cumbersome Task of Testing Students on Typewriters.,” n.d.

“Norton - Staffing for Unmanned Aircraft Systems (UAS) Ope.Pdf,” n.d.

published, Brett Tingley. “US Military Eyes SpaceX Starship for ‘Sensitive and Potentially Dangerous Missions’: Report.” Space.com, January 31, 2024. https://www.space.com/spacex-starship-pentagon-military-missions.

Snowden, Edward J. *Permanent Record*. Toronto: CELA, 2019.

Stop Killer Robots. “Use of Lavender Data Processing System in Gaza,” April 4, 2024. https://www.stopkillerrobots.org/news/use-of-lavender-data-processing-system-in-gaza/.

“SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF,” n.d.

THE ELECTRONIC CULTURE, 2010. https://www.youtube.com/watch?v=r5lrPLE06fM.

“The US Department of Defense Dictionary of Military and Associated Terms Defines Command and Control as: "The Exercise of Authority and Direction by a Properly Designated Commander over Assigned and Attached Forces in the Accomplishment of the Mission. Also Called C2.,” n.d.

United States Navy. “AEGIS Weapon System.” Accessed April 5, 2024. https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2166739/aegis-weapon-system/https%3A%2F%2Fwww.navy.mil%2FResources%2FFact-Files%2FDisplay-FactFiles%2FArticle%2F2166739%2Faegis-weapon-system%2F.

US Air Force. “The Air Force Distributed Common Ground System Is Also Referred to as the AN/GSQ-272 SENTINEL Weapon System.,” n.d. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/.

West, Sarah Myers. “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business & Society* 58, no. 1 (January 2019): 20–41. https://doi.org/10.1177/0007650317718185.

Wikipedia Editors. “A Bulletin Board System (BBS), Also Called a Computer Bulletin Board Service (CBBS), Is a Computer Server Running Software That Allowed Users to Connect to the System Using a Terminal Program. Once Logged in, the User Could Perform Functions Such as Uploading and Downloading Software and Data, Reading News and Bulletins, and Exchanging Messages with Other Users through Public Message Boards and Sometimes via Direct Chatting. In the Early 1980s, Message Networks Such as FidoNet Were Developed to Provide Services Such as NetMail, Which Is Similar to Internet-Based Email.” Information. Wikipedia, n.d.

———. “A United States Military Occupation Code, or a Military Occupational Specialty Code (MOS Code), Is a Nine-Character Code Used in the United States Army and United States Marine Corps to Identify a Specific Job. In the United States Air Force, a System of Air Force Specialty Codes (AFSC) Is Used.,” n.d.

“A Fix Net Archive Is Still Available on the Internet Archive at Https://Web.Archive.Org/Web/19980109152404/Http://Www.Fix.Net/,” n.d. https://web.archive.org/web/19980109152404/http://www.fix.net/.

“AI Targeting in Gaza and Beyond.” Accessed November 5, 2024. https://www.ploughshares.ca/publications/ai-targeting-in-gaza-and-beyond.

“AI Targeting in Gaza and Beyond.” Accessed November 5, 2024. https://www.ploughshares.ca/publications/ai-targeting-in-gaza-and-beyond.

Air & Space Forces Magazine. “The Network Way of War.” Accessed November 7, 2024. https://www.airandspaceforces.com/article/0305network/.

AT&T. “Operator and Directory Assistance Is Ending.” Accessed November 4, 2024. https://www.att.com/support/article/u-verse-voice/KM1511460/.

Biddle, Sam. “Documents Reveal Advanced AI Tools Google Is Selling to Israel.” The Intercept, July 24, 2022. https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/.

Colum Lynch. “Anatomy of an Accidental Shootdown Three Decades Ago, a Perfect Storm of Miscommunication, Miscalculation, and Human Error in the Heat of Battle Caused the United States to Make a Mistake Similar to the One Iran Just Did.” *Foreign Policy*, January 17, 2020. https://web.archive.org/web/20210228041413/https://foreignpolicy.com/2020/01/17/accidental-shootdown-iran-united-states-ukraine/. https://foreignpolicy.com/2020/01/17/accidental-shootdown-iran-united-states-ukraine/.

Department Of Defense Washington Dc. “Formal Investigation into the Circumstances Surrounding the Downing of Iran Air Flight 655 on 3 July 1988:” Fort Belvoir, VA: Defense Technical Information Center, August 18, 1988. https://doi.org/10.21236/ADA203577.

Durkin, Thomas A. “Credit Cards: Use and Consumer Attitudes, 1970-2000.” *Federal Reserve Bulletin* 86, no. 9 (2000): 0–0. https://doi.org/10.17016/bulletin.2000.86-9.

Exploding pagers and radios: A terrifying violation of international law, say UN experts. “Exploding Pagers and Radios: A Terrifying Violation of International Law, Say UN Experts.” Press Release, September 19, 2024. https://www.ohchr.org/en/press-releases/2024/09/exploding-pagers-and-radios-terrifying-violation-international-law-say-un.

Google Cloud Blog. “Google Cloud Selected to Provide Cloud Services to Digitally Transform the State of Israel.” Accessed November 5, 2024. https://cloud.google.com/blog/topics/inside-google-cloud/google-cloud-selected-to-provide-cloud-services-to-the-state-of-israel.

Iraqi, Amjad. “‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza.” *+972 Magazine*, April 3, 2024. https://web.archive.org/web/20241010022042/https://www.972mag.com/lavender-ai-israeli-army-gaza/. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

———. “‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza.” +972 Magazine, April 3, 2024. https://www.972mag.com/lavender-ai-israeli-army-gaza/.

“JADC2: Accelerating the OODA Loop With AI and Autonomy.” Accessed November 7, 2024. https://www.rti.com/blog/jadc2-the-ooda-loop.

Jimmy A. Gomez. “The Targeting Process: D3A and F3EAD.” *Small Wars Journal Blog* (blog), July 16, 2011. https://smallwarsjournal.com/blog/journal/docs-temp/816-gomez.pdf.

Johnson, James. “Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age.” *Defence Studies* 23, no. 1 (January 2, 2023): 43–67. https://doi.org/10.1080/14702436.2022.2102486.

Khlaaf, Heidy, Sarah Myers West, and Meredith Whittaker. “Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting.” arXiv, October 18, 2024. https://doi.org/10.48550/arXiv.2410.14831.

Kurlansky, Mark. *1968: The Year That Rocked the World*. New York: Random House Trade Paperbacks, 2005.

Levine, Yasha. Surveillance Valley: The Secret Military History of the Internet. New York: PublicAffairs, 2018.

“Mavis Beacon Teaches Typing Was a Software Program First Released by *Software Toolworks* in Late 1987. It Was Useful for Practice, and to Administer Touch Typing Tests to an Entire Classroom of Students Replacing the Cumbersome Task of Testing Students on Typewriters.,” n.d.

“Norton - Staffing for Unmanned Aircraft Systems (UAS) Ope.Pdf,” n.d.

published, Brett Tingley. “US Military Eyes SpaceX Starship for ‘Sensitive and Potentially Dangerous Missions’: Report.” Space.com, January 31, 2024. https://www.space.com/spacex-starship-pentagon-military-missions.

Snowden, Edward J. *Permanent Record*. Toronto: CELA, 2019.

“SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF,” n.d.

THE ELECTRONIC CULTURE, 2010. https://www.youtube.com/watch?v=r5lrPLE06fM.

“The US Department of Defense Dictionary of Military and Associated Terms Defines Command and Control as: "The Exercise of Authority and Direction by a Properly Designated Commander over Assigned and Attached Forces in the Accomplishment of the Mission. Also Called C2.,” n.d.

United States Navy. “AEGIS Weapon System.” Accessed April 5, 2024. https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2166739/aegis-weapon-system/https%3A%2F%2Fwww.navy.mil%2FResources%2FFact-Files%2FDisplay-FactFiles%2FArticle%2F2166739%2Faegis-weapon-system%2F.

US Air Force. “The Air Force Distributed Common Ground System Is Also Referred to as the AN/GSQ-272 SENTINEL Weapon System.,” n.d. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104525/air-force-distributed-common-ground-system/.

West, Sarah Myers. “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business & Society* 58, no. 1 (January 2019): 20–41. https://doi.org/10.1177/0007650317718185.

Wikipedia Editors. “A Bulletin Board System (BBS), Also Called a Computer Bulletin Board Service (CBBS), Is a Computer Server Running Software That Allowed Users to Connect to the System Using a Terminal Program. Once Logged in, the User Could Perform Functions Such as Uploading and Downloading Software and Data, Reading News and Bulletins, and Exchanging Messages with Other Users through Public Message Boards and Sometimes via Direct Chatting. In the Early 1980s, Message Networks Such as FidoNet Were Developed to Provide Services Such as NetMail, Which Is Similar to Internet-Based Email.” Information. Wikipedia, n.d.

———. “A United States Military Occupation Code, or a Military Occupational Specialty Code (MOS Code), Is a Nine-Character Code Used in the United States Army and United States Marine Corps to Identify a Specific Job. In the United States Air Force, a System of Air Force Specialty Codes (AFSC) Is Used.,” n.d.