The Future of the Cyber Theater of War

Dr. Elizabeth Cook

Liberty University

Author Note

Dr. Elizabeth Cook

I have no known conflict of interest to disclose.

Correspondence concerning this article should be addressed to Dr. Elizabeth Cook.

Email: ecook57@liberty.edu

Abstract

Few could imagine how it would develop when the air was the new theater of war. The literature showcases that a lack of imagination and state-level institutionalized power structures, particularly in the U.S., hampered the progress of air as a new theater of war both in thought and application. Today, a similar lack of imagination on the cyber theater of war is a great source of insecurity in the world system; it sets the stage for strategic shocks like the ones to the U.S. on December 7, 1941, and 9/11. To avoid this, states should imagine how a convergence of cyber technologies into new weapons could be used in war and by whom. Popular movies today form the basis for considering what has yet to be realized in the cyber theater of war. Its nascent history and designation as a theater of war foreshadow the expectation that eventual traditional war will occur in the cyber realm. When nanocomputers, artificial intelligence, quantum computing, speed, and advanced robotics fully converge, new weapons are possible and likely. The Just War Theory, understood through the Christian lens rather than only as a matter of secular international law, is applied to the evolving cyber theater of war to fill current doctrinal gaps in the just cause and conduct of future war within the cyber realm.

Keywords: warfare, cyberspace, air, theater of war, Just War Theory

The Future of the Cyber Theater of War

Few could imagine how it would develop when the air was the new theater of war. At first, it was seen by most as being limited to being a force multiplier for ground forces in the land and sea theaters of war[1]. The literature showcases that a lack of imagination and state-level institutionalized power structures, particularly in the U.S., hampered the progress of air as a new theater of war both in thought and application. Perhaps because of the constrictions after WWI, Germany was much more successful in both, at least until Stalin's execution campaigns[2]. Commercial endeavors drove military endeavors and vice versa[3], and international humanitarian law was forward-thinking but inadequate to forestall war[4]. In 1933, the U.S. was the greatest air power globally, with 1,800 aircraft[5]. France and Russia closely followed it[6]. Italy, Japan, and Great Britain trailed, with Great Britain having only 850 aircraft[7].

Today, a similar lack of imagination on cyberweapons is one of the greatest sources of insecurity in the world system; it sets the stage for strategic shocks like the strategic shocks to the U.S. on December 7, 1941, and again on 9/11. When nano computers, artificial intelligence, quantum computing, speed, and advanced robotics fully converge, new weapons are possible and likely.

---

[1] Ellis, “Aerial-Land”; Douhet, *Command of the Air*; Ledwidge, *Aerial Warfare*.

[2] Ledwidge, *Aerial Warfare*.

[3] Ledwidge.

[4] Ellis, “Aerial-Land.”

[5] Chamier, “England.”

[6] Chamier.

[7] Chamier.

Just since the middle of 2020, both exoskeletons and warp drives have advanced significantly[8], which were two things that were purely science fiction just a few years ago. The world's smallest nano computer now fits on a grain of rice [9] and NASA and Google recently achieved quantum (computing) supremacy, which looks like it will be a driving force behind advances in the space theater of war [10] although China's use of a "hypersonic glide vehicle launched from a rocket in low-earth orbit" in October of 2021 [11] certainly seems visionary. Laughing at what can be imagined is foolhardy.

Cyberspace is admittedly different from the other four theaters of war. Simply put, land, sea, air, and space are on Earth or relative to it. Cyberspace is not, and it is hard to envision the possibilities for war. Napoleon's comment that state strategies are dependent on geography[12] does not appear that it will hold, given that the possibility of a virtual nation-state is at hand thanks to the cyber realm[13]. Virtual (digital) currency already exists, and virtual communities of all sorts, including nations, abound on the internet[14]. It could also be about to evolve into something potentially more potent.

Multinational corporations (M.N.C.s) like Apple and Walmart already possess resources on par or in excess of some functioning states like Portugal and Belgium [15]. Others like Microsoft, Google, and Facebook are joining state-based agreements like the Paris Peace Forum cybersecurity

[8] Asthana, “Watch”; Yirka, “A Potential Model.”

[9] Yan, “The Smallest Computer.”

[10] “Google and NASA.”

[11] Duster, “Top Military Leader Says,” para. 9.

[12] Stewart, “Britain’s.”

[13] De Filippi, *Citizenship in the Era of Blockchain-Based Virtual Nations*.

[14] De Filippi.

[15] Terzi and Marcuzzi, “Are Multi-Nationals.”

agreement and setting public policies like Microsoft and affordable housing in Seattle, for example[16]. The E.U., in particular, is trying to restrict the power of 'big tech' M.N.C.s, but who will be the victor is not obvious[17].

The cyber realm increasingly permeates human physical lives across society's political, economic, and social aspects. Its nascent history and designation as a theater of war foreshadow the expectation that eventual traditional war will occur in the cyber realm. Drawing from Ledwidge (2018) and his research on airpower, the four elements needed to make full-scale war a genuine possibility in cyberspace are control, reconnaissance, attack, and mobility. In cyberspace, all four elements have already been achieved.

Today, the U.S., China, and Russia vie for power in the all-domain military environment[18]. In 2015, China re-envisioned its military forces and created a Strategic Support Force that combined important information warfare structures, including space and cyberspace, into one cohesive unit due to its desire for force projection[19].

Ultimately, innovation will determine who pulls ahead in the cyberspace theater of war [20]. If the lack of imagination persists in the cyber realm, particularly regarding the convergence of cyber technologies into new weaponry, insecurity will rise to a level deemed unacceptable, and (neo)realist thought will prevail in the world system. To avoid a knee jerk reaction after a strategic shock, states should imagine how a convergence of cyber technologies into new weapons could be

[16] Terzi and Marcuzzi.

[17] Terzi and Marcuzzi.

[18] Titus, “Establishing a Space Profession.”

[19] Costello and McReynolds, “China’s Strategic Support Force”; Dossi, “On the Asymmetrical Advantages.”

[20] Dossi, “On the Asymmetrical Advantages.”

used in war and by whom. Apparently, it is not an easy task given the lack of representation in popular movies today.

The fictional book, *The Last Sword Maker*, by Nelson (2018), provides a good example, though, because it has a strong cyber component that combines nanotechnology with super-fast computing. The plot includes two rival states with one being a superpower and the other one a rising regional power [21]. It also puts a new twist on an old character: the cyborg [22]. Although the storyline still has a fair amount of "giggle factor" in it, borrowing from Titus (2020) on page 23 of his article, it is an imaginative combination of two aspects of the cyber realm. More of this is needed so it can be addressed in international law before it becomes a reality.

Just War Theory provides a moral standard for entering into and conducting war[23]. It is heavily integrated into international law[24], which is easy to locate. However, finding information on its pagan beginning and adoption by Christians[25] is considerably more challenging. In this paper, the Just War Theory, understood through the Christian lens rather than only as a matter of secular international law, is applied to the emerging cyber theater of war and as a means to fill current gaps and stave off strategic shocks. Historical lessons, the current state of affairs, and the future imagined are analyzed to determine what future cyberwar might look like and how international law should develop.

Air as the New Theater of War

[21] Nelson, *The Last Sword Maker*.

[22] Nelson.

[23] *International Relations*.

[24] Griffiths, O'Callaghan, and Roach.

[25] Draper, "The Origins."

In 1914, three aircraft types existed: balloons, airships (driven or maneuverable balloons), and aero planes [26]. However, by this point, balloons were largely set aside as military assets since they were not drivable [27]. Aircraft were originally understood as supporting elements to land and sea forces [28]. Most decision-makers of the time simply understood war as something fought on land or sea, which was reasonable given the lack of a theoretical basis for aerial warfare [29]. When the sea was the new theater of war, it progressed similarly until a solid theoretical basis for waging war at sea was developed [30].

Understanding future wars in 1914 based on the introduction of the aero plane included conflicts plane-to-plane, plane-to-land, plane-to-maritime, and, separately, aerial bombing missions [31]. Reconnaissance missions by balloon and airship were already common, as were naval blockades [32]. Reconnaissance missions performed by aero planes and to thwart naval blockades were also easily envisioned [33]. Tactically, they fought one-on-one rather than in an enduring formation, but that began to change in 1942 when ideas on tactical airpower evolved [34].

In 1914, aerial warfare was considered a land and sea warfare component in the realm of (international) law [35]. The term "aerial warfare" was understood as an aspect of warfare associated with land or sea warfare [36]. The argument was that the air asset originated either from the land or

---

[26] Ellis, “Aerial-Land.”

[27] Ellis.

[28] Douhet, *Command of the Air*; Ledwidge, *Aerial Warfare*.

[29] Ledwidge, *Aerial Warfare*.

[30] Ledwidge.

[31] Ellis, “Aerial-Land.”

[32] Ellis.

[33] Ellis.

[34] Stewart, “Britain’s.”

[35] Ellis, “Aerial-Land.”

[36] Ellis.

sea, eventually returning there [37]. War in the air seemed unlikely as objects were only passing through [38]. Commercial aeronautics (as it was known then) was only beginning to take shape [39]. Laws built around a yet-to-be-developed commercial application were thought to be premature by some and timely applied by others [40]. Either way, the laws of neutrality applicable to naval ships did not yet apply to aero planes [41]. They could not be measured like naval ships in terms of tonnage for relative strength [42].

General strategic thought was that fighting in the air was unattainable or limited to supporting land and sea forces [43]. Conversely, Douhet, from Italy, believed that the air was a new frontier that aircraft could control [44]. Douhet (2014) felt that "the technical means of war available" dictated the "form" of war experienced (p. 5). Unpopular in his day, he went so far as to argue that air forces should be independent because controlling the air would result in decisive action and quick victories [45]. As such, they should be independent of land and sea commands, although they would continue to support forces in those theaters [46].

His ideas largely fell on deaf ears until the beginning of WWII [47]. The British were an exception; they created the Royal Air Force in 1918 [48]. Britain's Marshall of the Royal Air Force

---

[37] Ellis.

[38] Ellis.

[39] Ellis.

[40] Ellis.

[41] Ellis.

[42] Warner, “Can Aircraft.”

[43] Douhet, *Command of the Air*.

[44] Ledwidge, *Aerial Warfare*.

[45] Douhet, *Command of the Air*.

[46] Douhet.

[47] Ledwidge, *Aerial Warfare*.

[48] Chamier, “England.”

Lord Trenchard also advocated, purportedly before Douhet, that independent air forces were needed for strategic bombing missions [49]. The U.S. did not create a separate Air Force until 1947 [50].

In 1919, Brigadier General Billy Mitchell, a U.S. general, argued that navy battleships were no longer effective weapons of war because they could be destroyed by bombers in the air [51]. As such, they were no longer needed [52]. His statements were met with derision by Newton D. Baker, the U.S. Secretary of War, who seemed to think that the argument was nothing short of ridiculous [53].

By 1926, the relative importance of dominating the air in war was well understood, as was the role of "heavier-than-air craft," as they were sometimes referred to as the primary weapons to achieve that goal [54]. Many believed that future war would be fought in the air, that it would be concluded with hours or days, and that the losing state would suffer hefty damages in its cities [55]. Most military men, though, were skeptical of this view [56].

The U.S. was believed to be outside the range of attack at the time and for the foreseeable future [57]. However, England and France were within range both for reconnaissance and bombing missions [58]. As such, "whole countries [became] a battlefield," although it certainly was not limited

[49] Stewart, “Britain’s.”

[50] Ledwidge, *Aerial Warfare*.

[51] Ledwidge.

[52] Ledwidge.

[53] Ledwidge.

[54] Warner, “Aerial Armament,” 624.

[55] Warner, “Can Aircraft.”

[56] Warner.

[57] Warner, “Aerial Armament.”

[58] Warner.

to only England and France [59]. Both set about increasing their aerial capabilities heedless of concerns that an aerial race would ensue like the naval race before WWI [60]. This was further bolstered by the commercial application of aero planes in 1926, which were already firmly established as vehicles of transport and fire surveillance, for example, meaning that they could not be prohibited outright, although prohibiting military aviation was a topic of discussion among the British [61].

Advances in commercial flight prompted advancements in military flight and vice versa [62]. However, in the Draft Convention of 1927 prepared by the Preparatory Committee, sharp lines were drawn regarding funding the advancement of civilian aircraft by the military [63]. It was ultimately voted down [64]. By 1935, England understood that "a flourishing civil aviation industry is the foundation of military aviation," much as it was for the Royal Navy based on merchant marines [65].

This trend continued well into the future and today, particularly in space, with corporations like SpaceX advancing associated technologies with amazing speed. At this point, it was understood that necessity in war drives invention and that technology influences what is considered necessary by military and political leaders, just as Douhet argued in his book published in 1921 [66]. Early successes in reconnaissance missions by airplanes in WWI quickly gave birth to the idea

[59] Slessor, “Air Power.”

[60] Warner, “Aerial Armament.”

[61] Warner; Warner, “Can Aircraft.”

[62] Ledwidge, *Aerial Warfare*.

[63] Warner, “Can Aircraft.”

[64] Warner.

[65] Chamier, “England,” 316.

[66] Ledwidge, *Aerial Warfare*.

that fighter planes were needed [67]. The need for a fighter plane to attack another plane in front of it was also quickly realized [68]. However, the propellor created an obstacle, which was solved by synchronizing the propellor with the gun [69]. Likewise, early in WWII, the inability to create a propellor capable of handling the power of new engines was likely going to be answered by "[t]he use of as many as eight blades and counter-rotating propellers" [70]. Presumably, the creation of the jet engine changed that expectation.

Distrust among states was paramount because aero planes could be built in secret, unlike most naval ships, and they could penetrate far past lines of defense or front lines of conflict [71]. Ultimately, it was easy to imagine how WWI might have been fought differently had increased aerial capabilities existed, even if they were merely commercial aero planes originally [72].

Aero planes developing in terms of power was assumed [73]. Calculating the aircraft's destructive capacity using information from WWI, Douhet showed its comparable effectiveness [74]. He went so far as to say that commanding the air would bring about a decisive victory in war both because of the ability to negate defensive lines and due to the aircraft's offensive application [75]. However, his calculations overestimated the destructive capacity of aerial bombing missions, thereby losing the initiative to wage a decisive campaign, as evidenced in WWII [76].

---

[67] Ledwidge.

[68] Ledwidge.

[69] Ledwidge.

[70] Arnold, “The Air Forces,” 547.

[71] Warner, “Aerial Armament.”

[72] Warner.

[73] Van Creveld, *The Interwar Period*; Warner, “Aerial Armament.”

[74] Douhet, *Command of the Air*; Van Creveld, *The Interwar Period*.

[75] Douhet, *Command of the Air*; Van Creveld, *The Interwar Period*.

[76] Van Creveld, *The Interwar Period*.

Douhet's ideas on aerial warfare nullifying the other theaters of war were nearly realized when the U.S. released atomic bombs on Nagasaki and Hiroshima in Japan at the end of WWII [77]. Dropping atomic bombs also gave rise in 1954 to a vision of future-war being "robot pilotless aircraft or guided missile" [78]. However, Douhet's thoughts on the decisiveness of air power have not since come close to fruition, and conflicts like the one in Vietnam are an antithesis to the theory [79]. Today, Douhet's notion of commanding the air is known as air supremacy [80]. It is also the first of four roles for airpower [81]. The other three are reconnaissance, attack, and mobility [82].

By 1937, parachute forces were developed in Russia and Italy along with the airplanes needed to deliver them [83]. Air-borne forces were an important development for the time since it was related to the notion that the ability to surprise an enemy conveyed great strategic advantage [84]. The U.S.S.R. had already gone so far as to create a doctrine that later would be known as 'deep battle,' but it had little effect in WWII because most of the theorists were victims of Stalin in the late 1930s [85]. Unlike Douhet's belief, air defense was also developing in thought and application [86]. It would become fully realized during WWII; however, at this point, the ability of airplanes to transport troops or material was still a concept in its infancy [87].

---

[77] Van Creveld.

[78] Slessor, “Air Power,” 43.

[79] Ledwidge, *Aerial Warfare*; Van Creveld, *The Interwar Period*.

[80] Dudney, “Douhet”; Ledwidge, *Aerial Warfare*.

[81] Ledwidge, *Aerial Warfare*.

[82] Ledwidge.

[83] Hart, “The Armies.”

[84] Hart.

[85] Ledwidge, *Aerial Warfare*.

[86] Ledwidge.

[87] Ledwidge.

Combined with increasing mechanization and mobility of ground forces through various vehicles, including the tank, increased the range and tempo of war [88]. Offensive air bombing missions on the outbreak of war allowed states to amass ground forces while still dealing blows to the enemy [89]. By 1941, it was well understood that controlling the air was necessary for land and sea forces to succeed in their missions [90].

The merging of naval and air power in the early days of WWII redefined what it meant to have sea power [91]. This showcases how one theater of war impacts another and shows how advances in one theater impact other theaters. Theaters of war are not separate but fully connected, which is how the all-domain environment is understood today [92].

In 1941, what would later become the U.S. Air Force, was still a component of the Army [93]. Some commanders in the U.S. Army did not want to embrace the air component (Army Air Forces), but the demonstrated destructive capacity of the airplane in the early days of WWII left them little choice [94]. It was well understood by this point that fighter planes like the P-40 Warhawk and their pilots were necessary to keep from losing a war and that bombers like the B-17 and their pilots were necessary to win it [95].

U.S. Army Air Forces were still heavily connected to land and naval forces in combined arms warfare, which occurred as early as 1918, but they were also developing as a force that could

[88] Hart, "The Armies."

[89] Hart.

[90] Arnold, "The Air Forces."

[91] Arnold.

[92] Titus, "Establishing a Space Profession."

[93] Arnold, "The Air Forces."

[94] Arnold.

[95] Arnold.

pursue separate missions [96]. By the end of 1942, the British had mostly abandoned the idea that war could be won exclusively in the air and instead adopted a doctrine of "balanced force[s]," which was a hard transition in light of opposing viewpoints coming from the United Nations [97]. The basic strategy behind aerial operations was to use them in such a way as to have them, potentially along with other land or sea forces, deliver "maximum force at the decisive place and time" [98].

Airplanes were rapidly engineered and manufactured in concert with needs created by WWII [99]. Supplying R.A.F. airplanes in mid-WWII proved difficult, though, which impeded the true independence of air forces since materials like bombs and fuel were still carried over land and sea [100]. Their eventual true independence was anticipated as soon as materials could be transported for air forces by airplanes [101].

In 1942, the British felt that the fighter bomber was just as effective as the dive bomber but less risky [102]. In 1942, the stratosphere bomber, thanks to pressurized cabins, was developed and put to good use [103]. Conversely, some airplanes enjoyed stronger engines in still small airplanes [104]. Differences in airplanes based on their function as high or low flyers were anticipated but not a reality in 1942 [105].

---

[96] Arnold; Ledwidge, *Aerial Warfare*.

[97] Stewart, “Britain’s,” 442.

[98] Arnold, “The Air Forces,” 547.

[99] Arnold, “The Air Forces.”

[100] Stewart, “Britain’s.”

[101] Stewart.

[102] Stewart.

[103] Stewart.

[104] Stewart.

[105] Stewart.

In 1943, the U.S. formally designated air and ground forces as "coequal and interdependent forces" with separate commands, which allowed for better target selection [106]. The concept of air superiority was fully achieved in mid-1944, and the 'fighter-bomber' was consolidated into reality [107].

In 1945, the U.S. released two atomic bombs on Nagasaki and Hiroshima in Japan in a massive display of airpower that developed in less than 50 years after the first airplane and that heralded in the concept of mutually assured destruction [108] that characterized the Cold War between the U.S.S.R. and the U.S., which lasted another 44 years. With mutually assured destruction nearly guaranteed, total war was no longer a policy option [109]. Through the use of atomic airpower, future world wars were expected to fully realize Clausewitz's notion of absolute war [110].

Cyberspace as a New Theater of War

Cyberspace and its military application as a theater of war suffers from a lack of imagination similar to when the air was a new theater of war. For now, it is easily understood as a force multiplier for other traditional means of warfare associated with the land, sea, and air [111]. Current weapons consist of: trojans, viruses, worms, DoS/DDoS, and logic bombs [112].

Cyberwar is not often described in terms of the current anti-access, area-denial all-domain military environment. It is, perhaps, easier to understand the military application of cyberwar

[106] Nichols, “Theater,” 52.

[107] Ledwidge, *Aerial Warfare*.

[108] Slessor, “Air Power.”

[109] Slessor.

[110] Slessor.

[111] Eun and Abmann, “Cyberwar.”

[112] Eun and Abmann.

within this construct. The Russian-Georgian War of 2008 provides a good example. Russia presumably prepped the battlefield by disrupting communications, banking, and government websites before the ground invasion [113].

Although cyber superiority also does not seem to be a widespread term yet, it is another helpful construct to understand the current reality of cyberwar and its prospects. It is envisioned that cyberwar will be the proverbial 'first shot' that can subdue the enemy before the onset of war in the land, sea, or air theaters of war [114]. Dossi (2020) argues that an effective cyberattack against an enemy state's critical infrastructure can provide a strategic advantage so great that it will become a decisive factor in all other war domains, which is reminiscent of Douhet.

With the total war that ensued in WWII, bombing raids deep behind enemy lines killed enemy troops and, tragically, civilians [115]. Drawing on the power outages during the severely cold weather in Texas in February of 2021 and the resulting civilian deaths [116], it is easy to see how a cyber-attack on critical infrastructure like a power grid could result in significant damage[117]. In this way, cyberwar is independent of the other theaters of war [118]. Responses to cyberwar are not limited to the cyber realm [119]. The U.N. Group of Governmental Experts determined, in 2015, that the U.N. charter includes cyberspace and that international humanitarian law, specifically the Law of Land Warfare, still applies [120].

---

[113] Eun and Abmann.

[114] Dossi, “On the Asymmetrical Advantages.”

[115] Dudney, “Douhet.”

[116] McDonnell Rieto del Rio, Fausset, and Diaz, “Extreme Cold.”

[117] Hatch, “Defining a Class of Offensive Destructive Cyber Weapons As Weapons of Mass Destruction: An Examination of the Merits”; Lester and Moore, “Responding to the Cyber Threat”; Dossi, “On the Asymmetrical Advantages.”

[118] Dossi, “On the Asymmetrical Advantages.”

[119] Lester and Moore, “Responding to the Cyber Threat.”

[120] Lester and Moore.

Although the definition of cyberwar is far from set, Eun and Abmann (2016) argue that espionage is not an act of war. It is a threat, though, that is not likely to go away [121]. In 2001, China stepped out early with a large military force of hackers numbering between 50,000 to 100,000 members known as Blue Force [122]. The force appeared to be capable of defensive and offensive measures [123]. In 2015, it re-envisioned its military forces and created a Strategic Support Force, which includes both space and cyberspace operations [124].

China, in particular, realizes the importance of the military-commercial nexus in the cyber realm, and, as such, it is moving in that direction [125]. Espionage is one method for obtaining information about advancements in technology [126]. When that information is a weapon, it improves the ability of states like China to avoid embargoes by stealing the information needed with the added benefit of potentially being able to deny it [127]. Duqu and Flame are two such worms capable of exactly that and more like using Bluetooth to gather information from nearby devices [128]. Espionage does not usually rise to the point of being an act of war, and it probably does not in the cyber realm as well [129]. That does not mean that cyber espionage or reconnaissance is without consequences [130].

---

[121] Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons."

[122] Eun and Abmann, "Cyberwar."

[123] Eun and Abmann.

[124] Costello and McReynolds, "China's Strategic Support Force"; Dossi, "On the Asymmetrical Advantages."

[125] Dossi, "On the Asymmetrical Advantages."

[126] Eun and Abmann, "Cyberwar."

[127] Eun and Abmann.

[128] Eun and Abmann.

[129] Eun and Abmann.

[130] Eun and Abmann.

One interesting aspect of the cyber theater of war is that less-advanced states easily use cyberweapons against advanced industrialized countries like the U.S. [131]. It can also be used by non-state actors like terrorists and activists [132]. Estonia in 2007 serves as an apropos example. Russian servers were used to create a DDoS attack on government and banking institutions, which caused a temporary disruption of those services [133]. Since the attack cannot be pinned on the Russian government, Russian 'hacktivists' may have been to blame [134]. Again, attribution could not be definitely assigned [135].

Where the Russian-Georgian War of 2008 showcases the force-multiplying aspects of cyberwar in the all-domain military environment, Stuxnet showcases the independent nature of the cyber theater [136]. The threshold for military action independent of another theater of war was crossed in 2010 when a western state, mostly like the U.S. or Israel, unleashed Stuxnet, a worm, into the cyber realm for a directed attack on Iran's uranium enrichment nuclear facility in Natanz, Iran [137]. It was not assumed to be a non-state actor or activist's work due to the complexity and resources needed to create and deploy it [138]. Again, attribution cannot be assigned [139]. It infiltrated Iran's closed system by innocuously catching rides on varying networks, computers, and

[131] Eun and Abmann.

[132] Dossi, “On the Asymmetrical Advantages.”

[133] Eun and Abmann, “Cyberwar.”

[134] Eun and Abmann.

[135] Eun and Abmann.

[136] Eun and Abmann.

[137] Eun and Abmann.

[138] Dossi, “On the Asymmetrical Advantages”; Eun and Abmann, “Cyberwar”; Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons.”

[139] Eun and Abmann, “Cyberwar.”

removable drives [140]. It remained harmless until it arrived at its destination [141]. Then it went to work on altering the functions of the machinery, which damaged the centrifuge [142]. An aerial bombing presumably would have had a similar but perhaps greater effect [143]. To date, Stuxnet provides the best example of the mobility of cyberweapons. It was delivered to its target completely independent of the other theaters of war [144]. Under the 'cyber-revolution thesis,' cyberspace is autonomous and independent of other war theaters [145].

Actions by Anonymous in February of 2022 changed the paradigm of the cyber theater of war. Ledwidge (2018) argues that four elements are needed to achieve an independent cyber theater of war and Anonymous has taken control, reconnaissance, attack, and mobility into new territory. Independence has already been achieved [146] although that is not well understood or accepted. The nature or character of that independence has now advanced.

Regardless of their political motivations or leanings, Anonymous attacked Russia due to its invasion of Ukraine and purportedly controlled their satellites, military communications, terminal and gas control systems, water systems, and railway systems, banks, state-run media, airports, hospitals, and companies [147]. Several tactics like malware and DDoSing were used to achieve control of these sites with objectives that included defacing, disrupting, rendering systems

[140] Eun and Abmann.

[141] Eun and Abmann; Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons.”

[142] Eun and Abmann, “Cyberwar.”

[143] Eun and Abmann.

[144] Eun and Abmann.

[145] Dossi, “On the Asymmetrical Advantages.”

[146] Dossi; Eun and Abmann, “Cyberwar.”

[147] Johnson, “Anonymous Claims More Than 2,500 Targets Hacked in First Week of #OpRussia Offensive.”

offline, distributing propaganda, and leaking data [148]. The exact tactics and objectives were directly related to the specific site being hacked. Non-hackers wanting to join the fight were encouraged to become hashtag armies [149].

Importantly, Anonymous reported that they could not control Russia's nuclear arsenal [150] although no explanation was given to explain why not. Superpowers in the international system are partially identified based on military capabilities, which includes nuclear first- and second-strike capabilities. To remove the ability of a superpower to access or control its nuclear arsenal would elevate the importance of the cyber theater of war among the other theaters.

Future Cyberwar

To "imagine what has yet to be imagined"[151] is difficult at best. This design is oriented towards exploring what is currently imagined and serving as a source of inspiration for what could be. The design used in this study is a collective case study, and the methodology is purposeful sampling. Instrumental cases for the cyber theater of war were selected based on bounded criteria. Cases included audiovisual materials (popular movies and T.V. shows) that were analyzed using an embedded analysis derived from the exploration of air when it was a new theater of war to identify themes with limited within-case analysis and extensive cross-case analysis.

Movies and T.V. shows from 1960 forward with a main or minor plot related to cyber technology were considered for cyberspace as a new theater of war. Preference was given to newer movies and T.V. shows with plots involving cyberwar, cyber-espionage, cyber-related disaster,

[148] Johnson.

[149] Johnson.

[150] Johnson.

[151] Peakin, "'Our Most Powerful Weapon Will Be Ingenuity; Our Ability to Imagine What Has yet to Be Imagined' – GCHQ Director," para. 6.

future cyber technologies akin to the advancement of artificial intelligence or the like. The sample size for each new theater of war was twenty or fewer movies. Movies with prequels or sequels were considered one case.

A review of 11 popular movies and T.V. shows provide a framework for envisioning how the cyber theater of war may develop. The goal here is not to disregard science or technology but rather to see where advancements might go in terms of future cyberspace-related war. Presumably, science will eventually catch up with many of the ideas represented. See table 1 for a complete list of the movies selected.

Table 1

Table of Movies and TV Shows Reviewed

Movie/TV Show	Year
Avatar	2009
Chappie	2015
Guardians of the Galaxy	2014/2017
Elysium	2013
Ender's Game	2013
Independence Day	1996/2016
iRobot	2004
Singularity	2017
Star Trek	1966-present
The Matrix	1999-2003

Transformers 2007-2017

According to Hollywood, future wars in cyberspace often revolve around artificial intelligence (A.I.) systems that can learn and seek solutions to human problems as a part of their programming, which inevitably leads them to conclude that humankind is the problem. As a result, humankind is either enslaved or eradicated to solve the world's ills. Weapons included E.M.P.s, smart exoskeletons, advanced robots, cyborgs, drones, and rovers. A.I. kept tabs on humans through embedded cyber monitors, invasive bots, robot police, and robot armies that often start as friendly, helpful servants. Nanotechnology and mechanical engineering are mostly implied except in movies like *iRobot*. Quantum computing seems underrepresented except in the *Transformers* franchise. Interestingly, Hollywood seemingly imagines cyberwar as an independent theater as evidenced by its use of control, reconnaissance, attack, and mobility in its plots.

Conclusion

Cyberspace is harder to 'see', especially in the application of quantum computing to war. Conversely, movies on space versus cyberspace have a different focus[152]. Space movies are mostly on the theater of war[153]. Plots revolve around space first and characters second[154]. Movies on cyberwar are often the opposite. Characters are developed to pique interest in the plot, followed by cyber enemies. The connection between human nature and cyberwar is paramount. Human nature does not seem to be a common theme in space movies except that humans are a valuable

[152] Cook, "Shifting Sands: Space and Cyberspace Warfare and the Realist Turn in International Relations."

[153] Cook.

[154] Cook.

species in the universe as expressed in both *Star Trek* and *Guardians of the Galaxy*[155]. For movies related to either theater of war, the distribution of power is vastly different from today.

Remember that Douhet (2014) felt that "the technical means of war available" dictated the "form" of war experienced [156]. War was once considered a state endeavor because other actors in the world system presumably could not match the destructive capacity of state-based weapons, which were created with state-based resources [157]. Terrorist groups like al Qaeda reframed that understanding [158]. Today, corporations are again reframing that understanding, in part because costs have decreased [159] and non-state actors are now capable of waging cyberwar alongside states[160].

Considering the technical weapons of cyberwar through the Just War Theory and its Christian heritage can fill in the gaps currently left in international law and secular philosophical thinking. War viewed through this lens should be both “just and pious”[161]. The current weapons of cyberwar (trojans, viruses, worms, DoS/DDoS, and logic bombs [162]) fall short of creating the destructive capacity that is usually associated with traditional forms of war in the land, sea, and air theaters of war. That does not mean that current cyberwar weapons are “just” or “pious” to use Draper’s (1964) argument. If they were, cyberwar weapons, for example, wouldn’t target civilians per the *jus in bello* portion of the current doctrine, but Anonymous did in 2022 when it controlled

[155] Cook.

[156] Douhet, *Command of the Air*, 5.

[157] Grygiel, “The Power of Statelessness.”

[158] Grygiel.

[159] Zwart and Stephens, “The Space (Innovation) Race.”

[160] Lopez, “DOD: It’s Not Just State Actors Who Pose Cyber Threat to U.S.”

[161] Draper, “The Origins,” 84.

[162] Eun and Abmann, “Cyberwar.”

water systems and hospitals however briefly. In a longer siege type approach, civilian deaths would undoubtedly occur proving that unjust and impious cyberwar weapons already exist if the perpetrators can hang onto them long enough.

Draper (1964) argued that the acceptance of war into Christian theology stems in 313 A.D. from the Emperor Constantine, who was no stranger to war, and the Edict of Milan both of which caught the early church unsettled on the issue of war. The result was the sanctification of war into Christianity[163]. Regardless of the premise that more thought should have been given by the early church about war before sanctifying it, Just War Theory is an important segway between the two extremes of pacifism and total war[164].

Given the sinful nature of man, the application of pacifism is difficult to enact as a matter of state policy, especially when the other extreme of total war is one without constraints[165]. Drawing from Catholicism, the idea of using force with the purpose of ensuring or regaining peace[166] sets a good foundation for how to approach future cyberwar and, more specifically, cyberweapons. As cyberweapons continue to develop, ensuring or regaining peace is an important goal, both from the Christian standpoint and as a matter of state policy in the preservation of order. Like in the application of traditional war, order and peace will be on a continuum rather than a binary[167] and the same will be true for future cyberwar. Finally, the Catholic perspective on war accepts it as an evil, a failure of government, and a consequence of humankind's fall from grace[168].

[163] Draper, "The Origins."

[164] Patterson, Charles, and Ashcroft, *Just War and Christian Traditions*.

[165] Patterson, Charles, and Ashcroft.

[166] Patterson, Charles, and Ashcroft.

[167] Patterson, Charles, and Ashcroft.

[168] Patterson, Charles, and Ashcroft.

Some, like Hatch (2017), argue that U.S. policy should be focused on concepts like deterrence and mutually assured destruction, like in nuclear war, which implies a distinctive threat ensuring great loss of life or material by all involved. Instead, offensive anti-access/area denial seems to be a better approach for the U.S. to ensuring peace in the cyber theater of war. However, it requires anticipating and controlling cyber technologies both as they can be reimagined and utilized and as they develop into new capabilities.

It is easy to point to Al Qaeda's attack on the U.S. on 9/11 and the reapplication of commercial technology, the airplane, to the air theater of war by a non-state actor on civilians as evidence that a lack of imagination can result in strategic shocks[169] and unjust and impious war. It is also easy to disregard fiction venues, but such viewpoints ignore examples like John Carpenter's *Escape from New York* 1981 movie where Air Force One "is hijacked and crash-lands near the 'old' World Trade Center"[170]. Strategic shocks don't have to come from future weapons[171]. Reapplication of current technologies is enough[172].

Also, future cyberwar weapons will likely advance their destructive capacity[173] especially when nano computers, artificial intelligence, quantum computing, speed, and advanced robotics fully converge to say nothing of the impact of advances in cybertechnology on the other theaters of war, which blends the analysis on the application of Just War thinking with already established norms and geographical territoriality. It is in this area where the most risk of strategic shock to a state can occur.

---

[169] Hoover, "A Failure of Imagination in the U.S. Intelligence Community."

[170] Canby, "'Escape from New York,'" para. 6.

[171] Hoover, "A Failure of Imagination in the U.S. Intelligence Community."

[172] Hoover.

[173] Hatch, "Defining a Class of Offensive Destructive Cyber Weapons As Weapons of Mass Destruction: An Examination of the Merits."

Regaining peace through anti-access/area denial after a strategic shock is a paltry second place to avoiding the strategic shock in the first place. States, which fit the Lutheran perspective on the "divine ordination" of governments [174], should develop an extremely forward leaning posture to ensure offensive anti-access/area denial in the cyber realm over time. International law on Just War must establish norms for the just cause and conduct of cyberwar both to set the conditions for avoiding unjust and impious cyberwar and to provide an immediate recompense towards peace if violated.

[174] Patterson, Charles, and Ashcroft, *Just War and Christian Traditions*, loc. 1983.

References

Arnold, Harold H. “The Air Forces and Military Engineers.” *The Military Engineer* 33, no. 194 (December 1941): 545–48. https://www.jstor.org/stable/44555646.

Asthana, Mansij. “Watch: Rostec Arms Russian Troops with 300,000 ‘Ratnik’ Exoskeleton Suits for next Gen Warfare.” *The EurAsian Times*, December 19, 2020. https://eurasiantimes.com/watch-rostec-arms-russian-troops-with-300000-ratnik-exoskeleton-suits-for-next-gen-warfare/.

Birkeland, Bonny. “Space: The Final next Frontier.” *Minnesota Law Review* 104 (April 23, 2020): 2061–2103. https://minnesotalawreview.org/wp-content/uploads/2020/04/Birkeland_Final.pdf.

Canby, Vincent. “‘Escape from New York.’” *The New York Times*, July 10, 1981, sec. C. https://www.nytimes.com/1981/07/10/movies/escape-from-new-york.html.

Chamier, J.A. “England and Air Power.” *Foreign Affairs*, January 1935. https://www.jstor.org/stable/20030665.

Cook, Elizabeth A. “Shifting Sands: Space and Cyberspace Warfare and the Realist Turn in International Relations,” 1–30. Las Vegas, NV, 2021.

Costello, John, and Joe McReynolds. “China’s Strategic Support Force: A Force for a New Era.” Washington, D.C.: Institute for National Strategic Studies, National Defense University, October 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

De Filippi, Primavera. *Citizenship in the Era of Blockchain-Based Virtual Nations*. In: Bauböck R. (Eds) Debating Transformations of National Citizenship. IMISCOE Research Series.

Spring, Cham., 2018. https://link.springer.com/chapter/10.1007/978-3-319-92719-0_48#citeas.

Dossi, Simone. “On the Asymmetrical Advantages of Cyber Warfare. Western Literature and the Chinese Journal Goufang Keji.” *Journal of Strategic Studies* 43, no. 2 (February 23, 2020): 281–308. https://doi.org/10.1080/01402390.2019.1581613.

Douhet, Guido. *Command of the Air*. Translated by Dino Ferrari. 2nd ed. www.picklepartnerspublishing.com: Pickle Partners Publishing, 2014.

Draper, G.I.A.D. “The Origins of the Just War Tradition.” *New Blackfriars* 46, no. 533 (November 1964): 82–88. https://www.jstor.org/stable/43244075.

Dudney, Robert S. “Douhet.” *Air Force Magazine*, April 1, 2011. https://www.airforcemag.com/article/0411douhet/.

Duster, Chandelis. “Top Military Leader Says China’s Hypersonic Missile Test ‘Went around the World.’” *CNN*, November 18, 2021. https://www.cnn.com/2021/11/17/politics/john-hyten-china-hypersonic-weapons-test/index.html.

Ellis, Wilmot E. “Aerial-Land and Aerial-Maritime Warfare.” *The American Journal of International Law* 8, no. 2 (April 1914): 256–73. https://www.jstor.org/stable/2187132.

Eun, Yong-soo, and Judith Sita Abmann. “Cyberwar: Taking Stock of Security and Warfare in the Digital Age.” *International Studies Perspectives* 17 (2016): 343–60. https://doi.org/10.1111/insp.12073.

NASA. “Google and NASA Achieve Quantum Supremacy,” October 23, 2019. https://www.nasa.gov/feature/ames/quantum-supremacy.

Griffiths, Martin, Terry O’Callaghan, and Steven C. Roach. *International Relations: The Key Concepts*. Third edition. Routledge Key Guides. London: Routledge, 2014.

Grygiel, Jakub. “The Power of Statelessness.” *Policy Review*, May 2009, 35–50.

Hart, Liddell. “The Armies of Europe.” *Foreign Affairs*, 1937.

Hatch, Benjamin B. “Defining a Class of Offensive Destructive Cyber Weapons As Weapons of Mass Destruction: An Examination of the Merits.” *United States Air Force Center for Unconventional Weapons Studies, the Air University*, December 2017. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.airuniversity.af.edu/Portals/10/CSDS/assets/trinity_site_paper10.pdf.

Hoover, David L. “A Failure of Imagination in the U.S. Intelligence Community.” *American Intelligence Journal* No, 1 (2013): 59–71. https://www-jstor-org.ezproxy.liberty.edu/stable/26202043.

Johnson, Bridget. “Anonymous Claims More Than 2,500 Targets Hacked in First Week of #OpRussia Offensive.” *Government Technology & Services Coalition’s Homeland Security Today*, March 3, 2022. https://www.hstoday.us/.

Ledwidge, Frank. *Aerial Warfare: The Battle for the Skies*. First edition. Oxford, United Kingdom: Oxford University Press, 2018.

Lester, Phil, and Sean Moore. “Responding to the Cyber Threat: A UK Military Perspective.” *Connections: The Quarterly Journal* 19, no. 1 (2020): 39–44. https://doi.org/10.11610/Connections.19.1.04.

Lopez, C. Todd. “DOD: It’s Not Just State Actors Who Pose Cyber Threat to U.S.” *DOD News*, May 20, 2022. https://www.defense.gov/News/News-Stories/Article/Article/3039462/dod-its-not-just-state-actors-who-pose-cyber-threat-to-us/.

McDonnell Rieto del Rio, Giulia, Richard Fausset, and Johnny Diaz. “Extreme Cold Killed Texans in Their Bedrooms, Vehicles and Backyards.” *The New York Times*. February 19, 2021. https://www.nytimes.com/2021/02/19/us/texas-deaths-winter-storm.html.

Nelson, Brian A. *The Last Sword Maker*, 2018. https://www.overdrive.com/search?q=7413ABF0-01C4-4440-89F7-422A34DD69BD.

Nichols, Franklin A. “Theater Air Forces.” *Naval War College Review* 5, no. 8 (April 1953): 45–66. https://www.jstor.org/stable/44640208.

Patterson, Eric, J. Daryl Charles, and John Ashcroft, eds. *Just War and Christian Traditions*. 1st ed. Notre Dame: University of Notre Dame Press, 2022.

Peakin, Will. “‘Our Most Powerful Weapon Will Be Ingenuity; Our Ability to Imagine What Has yet to Be Imagined’ – GCHQ Director,” April 24, 2019. https://futurescot.com/our-most-powerful-weapon-will-be-ingenuity-our-ability-to-imagine-what-has-yet-to-be-imagined/.

Schmitt, Clayton J. “The Future Is Today: Preparing the Legal Ground for the United States Space Force.” *University of Miami Law Review* 74 (2020): 563–97.

Slessor, John. “Air Power and World Strategy.” *Foreign Affairs*, October 1954. https://www.foreignaffairs.com/articles/1954-10-01/air-power-and-world-strategy.

Smeets, Max. “A Matter of Time: On the Transitory Nature of Cyberweapons.” *The Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32. https://doi.org/10.1080/01402390.2017.1288107.

Stewart, Oliver. “Britain’s Air Effort.” *Foreign Affairs*, April 1943. https://www.jstor.org/stable/20029240.

Terzi, Allesio, and Stefano Marcuzzi. “Are Multi-Nationals Eclipsing Nation-States?” *International Politics and Society Journal*, June 2, 2019. https://www.ips-journal.eu/regions/global/are-multinationals-eclipsing-nation-states-3245/.

Titus, Bryan M. Lt Col. “Establishing a Space Profession within the US Space Force.” *Air and Space Power Journal*, Fall 2020, 10–28.

Van Creveld, Martin. *A History of Strategy, From Sun Tzu to William S. Lind*. 2nd ed. Kouvola, Finland: Castalia House, 2015.

Warner, Edward P. “Aerial Armament and Disarmament.” *Foreign Affairs*, July 1926. https://www.jstor.org/stable/20028489.

———. “Can Aircraft Be Limited?” *Foreign Affairs*, April 1932. https://www.jstor.org/stable/20030447.

Yan, Laura. “The Smallest Computer in the World Fits on a Grain of Rice.” *Popular Mechanics*, June 30, 2018. https://www.popularmechanics.com/technology/a22007431/smallest-computer-world-smaller-than-grain-rice/#:~:text=Researchers%20at%20the%20University%20of,powered%20by%20solar%20cell%20batteries.

Yirka, Bob. “A Potential Model for a Real Physical Warp Drive.” *Phys.Org*, March 4, 2021. https://phys.org/news/2021-03-potential-real-physical-warp.html.

Zwart, Melissa De, and Dale Stephens. “The Space (Innovation) Race: The Inevitable Relationship between Military Technology and Innovation.” *Melbourne Journal of International Law* 20 (2019): 1–28.