ABSTRACT

Title of Document: ROBOTICS AND THE FUTURE OF INTERNATIONAL ASYMMETRIC WARFARE

Nicholas Grossman, Doctor of Philosophy, 2013

Directed By: Professor George Quester, Department of Government and Politics

In the post-Cold War world, the world's most powerful states have cooperated or avoided conflict with each other, easily defeated smaller state governments, engaged in protracted conflicts against insurgencies and resistance networks, and lost civilians to terrorist attacks. This dissertation explores various explanations for this pattern, proposing that some non-state networks adapt to major international transitions more quickly than bureaucratic states. Networks have taken advantage of the information technology revolution to enhance their capabilities, but states have begun to adjust, producing robotic systems with the potential to grant them an advantage in asymmetric warfare.

ROBOTICS AND THE FUTURE OF ASYMMETRIC WARFARE

By

Nicholas Grossman

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2013

Advisory Committee:
Professor George Quester, Chair
Professor Paul Huth
Professor Shibley Telhami
Professor Piotr Swistak
Professor William Nolte
Professor Keith Olson

Dedication

To Marc and Tracy Grossman, who made this all possible, and to Alyssa Prorok, who made it all worth it.

Acknowledgements

Thank you to my dissertation committee for all the advice and support, Anne Marie Clark and Cissy Roberts for making everything run smoothly, Jacob Aronson and Rabih Helou for the comments and encouragement, Alyssa Prorok for invaluable help, and especially to George Quester for years of mentorship.

Table of Contents

Introduction

They said September 11th changed the world, but they didn't say for how long. When al Qaeda operatives flew passenger jets into the Twin Towers and the Pentagon, scholars and strategists proclaimed an era of asymmetric warfare, with security threatened by shadowy networks and rogue states, rather than symmetric Great Power armies. Walter Laqueur, of the Center for Strategic and International Studies, confidently predicted in 2003 that "terrorism is bound to remain high on the list of our priorities;"[1] while Israeli scholar Martin van Creveld implored the "developed world" to "shake off its lethargy" and recognize "insurgency, guerrilla warfare, and terrorism, possibly, one day, armed with weapons of mass destruction" as its primary security concern.[2] This followed a series of predictions from RAND scholars John Arquilla and David Ronfeldt that the information age empowered networks of individuals, increasing the threat from terrorist organizations, criminal cartels, and extremist groups.[3] American security officials, such as Secretary of Homeland Security Michael Chertoff, argued that al Qaeda represents an existential threat to the United States,[4] while Michael Scheuer, the former head of the CIA's Bin Laden Issue Station,[5] declared that "America is in a war for survival. Not survival in terms of protecting territory, but in terms of keeping the ability to live as we want."[6] According to this view, the 21st century would prominently feature international terrorism, and the United States should expect a steady stream of attacks from networks of individuals on airplanes, landmarks, shopping malls, train stations, and crowded city centers, with machine guns, explosives, poison gas, biological agents, and radioactive material.

[1] Laqueur, "No End to War," p.7

[2] Van Creveld, "The Changing Face of War," p. 277-278.

[3] Arquilla and Ronfeldt, *In Athena's Camp* and *Networks and Netwars*.

[4] Harris and Taylor, "Homeland Security chief looks back, and forward."

[5] The CIA's Bin Laden Issue Station was a unit devoted to tracking Osama bin Laden and senior al Qaeda leadership. Scheuer ran the Station from 1996-1999 and advised the Station Chief from 2001-2004.

[6] Scheuer, *Imperial Hubris*, p. 242.

At first, this harrowing vision seemed to be coming true, as a series of American officials received mail tainted with anthrax spores in late 2001, and self-proclaimed al Qaeda member Richard Reid attempted to destroy an American Airlines plane flying from Paris to Miami in December with explosives hidden in his shoe. In May 2002, U.S. Customs agents arrested suspected al Qaeda associate Jose Padilla for a plot to release a "dirty bomb," in which radioactive material would spread over a major American city. The threat appeared to encompass American allies as well, perhaps all economically advanced Western nations, as Madrid (March, 2003) and then London (July, 2005) suffered bombings on their transportation systems that killed 191 and 52, respectively. The perpetrators of these attacks were "inspired by," rather than directly sent by the organization behind 9/11,[7] suggesting the frightening possibility that terrorism could come from self-starters with a shared ideology, as well as sleeper cells of trained operatives. With the US, UK, Spain, and their NATO allies engaged in wars in Afghanistan and Iraq while facing terrorist threats at home, the predictions of a prolonged and bloody struggle between the West and radical Islamists appeared to be coming true.

But then nothing happened. At least not much. The United States, Spain, and Great Britain faced few credible threats after the original attacks in, respectively, 2001, 2003, and 2005, and were able to prevent anything on a similar scale. In the decade after September 11th no terrorist managed to detonate a bomb on U.S. soil.[8] The RAND Corporation records 83 terrorist attacks in the United States between 9/11 and the end of 2009, almost all with zero casualties. Over half of these were perpetrated by environmental and animal rights groups, and only three were connected to jihadist causes. This contrasts sharply with the 1970s, during which 60 to 70 terrorist incidents occurred annually, primarily bombings by the Weather Underground, New World Liberation Front, and other radical domestic

[7] On Madrid attacks, see Nash, "Madrid bombers 'were inspired by Bin Laden address." On London, see "Leak reveals official story of London bombings."

[8] Mueller and Stewart, "The Terrorism Delusion," p. 88.

organizations.[9] From 1970 to 1978, 72 people died in America from terrorism,[10] compared to 24 from October 2001-December 2009, 16 of which were linked to jihadists.[11] All 16 were killed in three shooting incidents: two at the El Al ticket counter in Los Angeles airport in July 2002,[12] one at a military recruitment center in Little Rock in May 2009, and 13 by U.S. Army Major Nidal Malik Hasan at Fort Hood in November 2009.[13] Comparatively, disgruntled college student Seung-Hui Cho shot and killed 32 at Virginia Tech in April 2007,[14] in an incident that was not considered terrorism because the shooter lacked a political agenda.

This apparent lack of threat to the American homeland led some strategists and scholars to downplay al Qaeda, as well as terrorism in general. Asking "what Islamic terrorist threat?," Shikha Dalmia argued in 2011 that the absence of post-9/11 terrorist attacks in the United States reveals that al Qaeda is "a rag-tag band of peasants whose malevolent ambitions are far beyond the capacity of their shallow talent pool to deliver."[15] Similarly, former CIA interrogator Glenn L. Carle warned America that "Osama bin Laden and his disciples are small men and secondary threats whose shadows are made larger by our fears." Al Qaeda may threaten "to use chemical, biological, radiological or nuclear weapons," he wrote in 2008, "but its capabilities are far inferior to its desires."[16] Putting it less acerbically, security scholar John Mueller asks "if it is so easy to pull off an attack and if terrorists are so demonically competent, why have they not done it?" Perhaps, he argues, "almost no terrorists exist in the United States and few have the means or the inclination to strike from abroad."[17]

[9] Jenkins, "Would-Be Warriors," p. 9.
[10] Jenkins, "Would-Be Warriors," p. 8.
[11] Mueller and Stewart, "The Terrorism Delusion," p. 88.
[12] "Los Angeles airport shooting kills 3." The deaths included two victims and the shooter.
[13] "Shootings at Fort Hood."
[14] Hauser and O'Connor, "Virginia Tech Shooting Leaves 33 Dead." The deaths included 32 victims and the shooter.
[15] Dalmia, "What Islamist Terrorist Threat?"
[16] Carle, "Overstating Our Fears."
[17] Mueller, "Is There Still a Terrorist Threat?" p. 1.

Terrorism is difficult. It requires immense discipline, skill, and sacrifice to prepare without getting caught and then execute successfully. Few are sufficiently committed to a cause to devote their lives to acts of spectacular violence against non-combatants, of which only a small subset possess the know-how and ability to commit mass murder. As Shikha Dalmia points out, to present a threat to the United States, terrorists "would have to be: radicalized enough to die for their cause; Westernized enough to move around without raising red flags; ingenious enough to exploit loopholes in the security apparatus; meticulous enough to attend to the myriad logistical details that could torpedo the operation; self-sufficient enough to make all the preparations without enlisting outsiders who might give them away; disciplined enough to maintain complete secrecy, and—above all—psychologically tough enough to keep functioning at a high level without cracking in the face of their own impending death."[18] Along these lines, it is probably best to think of the September 11th attackers as al Qaeda's equivalent of Special Forces, an elite product of recruitment and training, rather than common foot soldiers that can be easily replaced or copied.

Noting the paucity of post-9/11 terrorist attacks in the United States, John Mueller and Mark G. Stewart declared in 2012 that the original threat was exaggerated, and that America is operating under a "terrorism delusion," devoting far more resources to the problem than necessary.[19] Tabulating the 50 cases of "Islamist extremist terrorism that have come to light since the terrorist attacks of September 11, 2001, whether based in the United States or abroad, in which the United States was, or apparently was, targeted," Mueller and Stewart find that only seven "actually reached the stage of committing, or trying to commit violence in the United States," of which only the three shootings (El Al ticket counter, Little Rock, Fort Hood) resulted in casualties. Of the 43 remaining cases, 16 were disrupted by authorities, 24 were egged on or assisted by undercover agents until enough evidence had accumulated

[18] Dalmia, "What Islamist Terrorist Threat?"

[19] Mueller and Stewart, "The Terrorism Delusion."

to issue arrest warrants, and three were conspiracy charges in which no violence had actually been planned or attempted.[20] In contrast to the predictions of an Age of Terrorism, this evidence presents a picture of a relatively small problem that is largely under control.

However, on April 15, 2013, two pressure-cooker bombs exploded near the finish line of the Boston Marathon, killing three and injuring 264.[21] Images of bystanders with mangled limbs, bloodied children crying, and security services rushing to the chaotic scene rapidly spread around the world. The horrified public reaction presented a challenge for those who had downplayed the threat of terrorism.

Nevertheless, Mueller and Stewart quickly dismissed the perpetrators as "hapless, disorganized, and irrational."[22] The attackers dropped the bombs near the finish line of a major international race in a developed city, an area covered with cameras. Media photographers, official race cameras, spectators' cell phones, and store security cameras provided hundreds of hours of videos to FBI and police investigators, who spotted two men that entered the area with large backpacks and left without them. Within three days, the FBI publicly released photographs of two suspects, later identified as brothers Tamerlan and Dzhokhar Tsarnaev. This seems to have sent them into a panic. In the next eight hours, the two suspects killed an MIT campus officer, carjacked an SUV, and engaged police in a firefight that killed 26-year old Tamerlan. The next evening, acting on a tip from a homeowner who noticed blood on his boat, police arrested 19-year old Dzhokhar.[23]

The Tsarnaevs did not appear to have a plan for the aftermath of their attack or an idea of what the bombings would accomplish beyond an expression of anger at the United States, and therefore do not fit the picture of competent, strategic terrorists painted by the worst post-9/11 fears. The attack

[20] Mueller and Stewart, "The Terrorism Delusion," p. 7.
[21] Kotz, "Injury toll from Marathon bombs reduced to 264."
[22] Mueller and Stewart, "Hapless, Disorganized, and Irrational."
[23] Herbert, "Boston Marathon timeline: from attack to capture."

created a horrific scene, but caused fewer fatalities than mass shootings in 2012 at Sandy Hook Elementary School in Connecticut, in which Adam Lanza killed 20 children and six adults,[24] and in a Colorado movie theater, in which James Holmes killed 12 and injured 70.[25] The Marathon attack was first successful bombing in the United States since 9/11, more than 11 years later, and it only killed three people. It therefore does not disprove the claim that terrorism poses a relatively small threat to Americans.

However, graphic images of maimed bystanders, disruption of normal life in Boston and the associated economic costs, and the widespread fear associated with unexpected violence gave the Marathon bombing, like other terrorist attacks, a greater impact than the casualties alone. Furthermore, investigations revealed that Tamerlan Tsarnaev sympathized with al Qaeda and the international jihadist cause, especially insurgents in Dagestan fighting against Russia;[26] participated in discussions on jihadist websites where he passionately criticized American foreign policy; and learned how to build the pressure-cooker bombs from an article in *Inspire*, al Qaeda's English-language online magazine, called “Make a Bomb in the Kitchen of Your Mom.”[27] This suggests the possibility that jihadist self-starters—individuals who sympathize with the global movement but act without direction from an organized terrorist group—will attempt similar attacks against the United States in the future. Like the Tsarnaevs, these individuals stoke their grievances and learn terrorist techniques on the internet, rather than in a training camp, which increases the difficulty of tracking them and anticipating their actions. It is unlikely that self-starters could pull off an attack that approaches the scale of 9/11, but the Boston Marathon bombings, and other attacks perpetuated by self-starters such as the London transportation

[24] “As nation mourns, investigators try to figure out what led to tragedy in Newtown, Conn.”

[25] “Officials release complete list of injured victims in Aurora massacre.”

[26] Dewey, “The obscure Russian jihadist whom Tamerlan Tsarnaev followed online.”

[27] Jefferson, “Here's the Jihadist Magazine that Taught the Boston Bombers to Kill.”

bombings, indicate that the United States and other developed countries continue to face a threat from jihadist terrorism.

The Future of International Asymmetric Warfare

Claims that terrorism represents a never-ending existential threat or a hyperbolically exaggerated nuisance both go too far, because both overrate their immediate circumstances. One spectacularly large attack does not indicate an uninterrupted torrent of terrorism, and a string of failed or thwarted attempts does not mean that a spectacularly large terrorist attack will never happen again. The history of security threats tends to follow a back-and-forth pattern, in which powerful states establish security and another state or non-state actor figures out a way to threaten that security. Every once in a while this overturns the prevailing international order, but usually the dominant states find a way to address the threat some time after the vulnerability is revealed. Loophole exploited, loophole closed, new vulnerability discovered. History has shown that every weapon, every strategy, no matter how successful at first, can be countered, by either a new technology or an innovative use of existing capabilities. It is thus possible that September 11th represented a peak of this cycle, the relative paucity of post-9/11 terrorist attacks represents a trough, and another terrorist attack will exploit a different loophole in the future, creating a another peak.

Even though the United States has not suffered a repeat of September 11th, terrorism in general and al Qaeda specifically feature prominently in all American National Intelligence Estimates and Annual Threat Assessments since 2001. This includes Director of National Intelligence Dennis Blair's testimony to Congress on February 2, 2010, which declares that, despite some successes, the “terrorist threat to the homeland remains."[28] Since September 11, 2001, the United States invaded Afghanistan and Iraq—justified primarily to stop ongoing and potential future support for terrorist groups—altered domestic privacy policies to deter and defend against terrorism, and massively expanded intelligence capabilities. Clearly, the United States perceives a significant threat from al Qaeda, and has made the War on Terrorism (or alternative labels like the "Long War," the "Struggle against Violent Extremism," and the highly euphemistic "Overseas Contingency Operations"[29]) one of the most central national and international security concerns of the early 21st century. But should this continue? And to what extent? This dissertation explores the future of international terrorism, insurgency, and other types of conflict between adversaries that control dramatically uneven levels of material resources. Will al Qaeda, a successor organization, or another transnational network with a different ideology be a major feature of the international system, threatening the security of the United States and allies for the indefinite future? Will more localized asymmetric conflicts, like those against the Iraqi and Afghan insurgencies, continue to be the main type of war fought by the United States and other nuclear powers? Or will history look back on this period when terrorism and insurgency were considered major challenges as ephemeral; a brief interlude between the end of the Cold War and another era of competition between powerful states?

To predict whether asymmetric conflicts between powerful states and non-state networks will prominently feature in the 21st century international security environment, the following explores competing explanations for the threat posed by al Qaeda and the relative success of various insurgencies, and then forecasts the likelihood that these trends continue. Given the United States' prominent global position, some people will be unhappy with America's military, institutional, economic, and cultural influence, and a small subset of them will want to use violence in an attempt to

[28] Annual Threat Assessment, February 2, 2010, p. 8.
[29] Wilson and Kamen, "'Global War on Terror' is Given New Name."

resist or change this. The desire to fight the United States won't disappear, but the factors that enabled al Qaeda to threaten American and allied security, and the conditions that allowed the Iraqi and Afghan insurgencies to resist the United States-led efforts to eliminate them, may not persist.

Perhaps prominent terrorist and insurgent groups have developed especially effective strategies that exploit features inherent in asymmetric warfare, elevating the techniques that relatively weak combatants used against stronger opponents in previous conflicts. Alternatively, it may be a function of the type of actors involved. Perhaps the United States has certain vulnerabilities due to its adherence to international norms abroad or the open nature of its society at home, while al Qaeda might be particularly dangerous because of its religious identity. However, asymmetric warfare is hardly a recent phenomenon, and there have been many conflicts throughout history between different types of governments and organizations with religious, nationalist, ethnic, class-based and other motivations, producing various results. Therefore, some feature of the current international system will probably contribute to a comprehensive explanation of modern asymmetric warfare. Recent weak actor successes could be due to a structural feature of the 21st century material environment, a factor of the strategies made available by the spread of weapons and information technology. In that case, al Qaeda or something similar will continue to threaten the international order and insurgencies will continue to frustrate powerful countries until a significant technological change shifts the advantage back to states. Finally, the threat posed by al Qaeda could be a temporary result of recent international transitions, whether political or technological. Non-state networks could be able to adapt to major changes in the global system, such as the end of the Cold War or spread of the internet, more quickly than bureaucratic states, which implies that states will gradually neutralize al Qaeda or another practitioner of transnational terrorism, relegating the threat that defined the first decade of the 21st century back to the nuisance it was considered in the 20th; at least until another political or technological transition opens a new opportunity for networks to exploit.

Al Qaeda's Grand Strategy

The transnational jihadist organization known as al Qaeda has the most ambitious goals of any non-state actor in history. Founded by Osama bin Laden in the late 1980s in the aftermath of the Soviet Union's withdrawal from Afghanistan, and merging with Ayman al Zawahiri's Egyptian Islamic Jihad in the early 1990s, al Qaeda seeks to defeat what it believes is a global conspiracy against Islam.[30] Members and sympathizers embrace a particularly expansive interpretation of jihad, which can refer to either a personal religious struggle or efforts to defend Islam against foreign attack. Al Qaeda's prime targets are the regimes in Muslim countries it believes are apostate, such as Saudi Arabia. However, al Qaeda believes that to overthrow these governments requires defeating their external allies, namely the United States, or the West in general. In contrast to the more hysterical accusations of Western media, al Qaeda's grievances are political—primarily American support for Israel and repressive Muslim governments—rather than cultural (hatred of freedom, democracy, Hollywood, women in skirts, etc). The organization sees itself as the tip of the spear of a broader jihadist struggle against "Jews, Crusaders, Apostates, and Hypocrites"[31] to remove Western influence from the Muslim world, defined broadly to include any land ever controlled by the Muslim Caliphate. This places a loosely connected network of individuals and organizations in a global struggle against the largest military and economy in the world.

The war between al Qaeda and the United States has a greater scope, and features a larger material disparity, than any previous asymmetric conflict. At most, there is only one precedent of a non-state network challenging the prevailing international order, the late 19th-early 20th century European Anarchists. Even this comparison is somewhat strained, as the Anarchists, though transnational, were based in Europe and focused exclusively on the European state system. Al Qaeda,

[30] Brachman, *Global Jihadism*, p. 82; see also Bergen, *The Longest War*, p. 28.
[31] Brachman, p. 83, paraphrasing jihadist strategist Abu Musab al Suri.

by contrast, targets civilians and governments in North America, Asia, Africa, and Europe as part of a strategy to overthrow governments in the Middle East, and Central and South Asia. To fight this globalized insurgency against the American-led international order, al Qaeda's strategists must draw lessons from historical examples of more localized state-network conflicts, and invent the rest.

Nature of the Actors

While the war between al Qaeda and the United States is asymmetric, and therefore subject to the factors inherent in all asymmetric conflicts, it is likely influenced by its unique characteristics: the nature of the adversaries and the environment in which the conflict takes place. It is possible that the United States' democratic political system and relatively open society make it ill-suited for asymmetric warfare and a particularly attractive target for strategies that utilize terrorism. Additionally, as some scholars have argued, al Qaeda's religiosity may increase its resiliency, capabilities, and resolve.

Democracy

Regime type may affect a strong actor's ability to prosecute an asymmetric conflict, endure the associated material costs, stifle domestic opposition, or resist international political pressure. Gil Merom argues that democracies are more likely to lose asymmetric conflicts than authoritarian regimes "because they find it extremely difficult to escalate the level of violence and brutality to that which can secure victory."[32] All powerful states hope to turn their material advantage into rapid, low-cost victory, but democratic polities may hold their soldiers to a higher standard. Employing torture, indiscriminate bombing, or mass killings defies democratic norms of human rights and proper conduct in war, creating additional political costs that increase domestic and international pressure on powerful democracies to

[32] Merom, *How Democracies Lose Small Wars*, p. 15.

withdraw forces. If democracies are less capable of sustaining the political will necessary for victory in asymmetric conflicts, regime type could account for the prolonged nature of America's 21st century counter-insurgency wars, as well as the United States, Great Britain, Israel, and other democracies' inability to eliminate networks like al Qaeda or Hamas.

However, there is no clear evidence that brutal violence grants victory in asymmetric conflicts, or that authoritarian regimes win asymmetric conflicts more often.[33] It is possible that attacks on the weak actor's civilians galvanizes rather than discourages an insurgency, as it confirms their expectations of the strong actor's brutality;[34] which is exactly the reaction some terrorism seeks to provoke.[35] While an alleged democratic distaste for sustained brutality may play a role in the outcome of some asymmetric conflicts—such as France's decision to withdraw from Algeria[36] or the US withdrawal from Vietnam[37]—it cannot possibly explain any wars in which the strong actor was not democratic. The authoritarian Soviet Union employed brutal tactics against the Afghan mujahideen and still did not achieve victory. Furthermore, France and the United States killed masses of civilians in the Algerian and Vietnam wars, and recent studies have found no support for the general claim that democracies kill fewer civilians in international conflicts.[38] As demonstrated by the Abu Ghraib torture scandal and the sustained Israeli policy of bulldozing homes belonging to Palestinian suicide bombers' families, democracies employ tactics that, while far short of mass murder, violate democratic norms; but they are still able to continue fighting despite the accompanying domestic dissent and international criticism. Additionally, non-democratic leaders must also deliver some perceived success, albeit among a smaller pool of influential domestic actors, or risk losing power. Therefore, regime type might influence which costs a strong actor is willing to tolerate in certain conflicts, but cannot

[33] Arreguin-Toft, *How the Weak Win Wars*, p. 28.
[34] Bueno de Mesquita and Dickson, "The Propaganda of the Deed."
[35] Arce and Sandler, "Terrorist Signaling and the Value of Intelligence."
[36] Galula, *Pacification in Algeria*.
[37] Summers, *On Strategy*.
[38] See, Valentino et. al., "Covenants without the Sword"; or Downes, "Restraint or Propellant?"

sufficiently explain why terrorist or insurgent networks can pose a security challenge for powerful states.

Nevertheless, democracies may be attractive targets for networks because of the public's influence on political leaders. By frightening a country into concessions[39] or prolonging the conflict to “create contradictions in the enemy's camp”[40] (i.e. prompting a domestic anti-war movement calling for the government to divert resources to other interests)[41] networks can take advantage of democracies' decision-making processes to achieve their goals, such as the withdrawal of foreign forces.[42] Rapid American withdrawals from Beirut (1983) and Mogadishu (1993), or eventual withdrawal from Vietnam (1973) demonstrate the potential of these strategies for networks fighting against the United States. Israeli withdrawals from southern Lebanon (2000 and 2006) and Gaza (2005) offer additional examples of networks utilizing asymmetric violence against a democracy to at least partially achieve their goals.

It must be noted that powerful democracies that have fought non-state networks, including Israel, Britain, and the United States, have the resources to destroy their enemies with indiscriminate bombing, yet choose strategies designed to avoid civilian casualties when possible. By contrast, Nazi Germany crushed the Warsaw Ghetto uprising (1943) by killing everyone inside, and Syria, another non-democracy, defeated the Muslim Brotherhood's rebellion by indiscriminately bombarding Hama (1982). This suggests that authoritarian regimes may, on rare occasions, be willing to employ total war in asymmetric conflict, obliterating weaker opponents with overwhelming force, while democracies will refrain from utilizing this level of violence. However, the instances of governments of any type doing this are sufficiently rare to conclude that regime type's effect on asymmetric warfare is limited.

[39] Pape, *Dying to Win*.
[40] Mao, “On Protracted War.”
[41] Mack, “Why Big Nations Lose Small Wars.”
[42] Pape, *Dying to Win*.

Religion

Al Qaeda is a religious organization and its interpretation of Islam is central to its worldview.[43] Therefore, individuals committing violence in the name of al Qaeda or other organizations that espouse jihadist ideology could be religiously motivated. Scholars such as Jessica Stern argue that religion is the primary driver of Islamic terrorists.[44] Under this interpretation, the terrorist act is a religious sacrament, with God as the intended audience rather than humanity. The bombers expect to go to heaven and receive a reward—immediately, in the case of suicide attacks—which makes them unconcerned with death. Following this line of argument, religious fanaticism is the problem, and al Qaeda will continue to be a threat as long as the ideology that prompts some Muslims to murder others in the name of jihad remains sufficiently unchecked. This implies that a non-religious transnational terrorist organization would be less threatening.

However, it is more likely that religion plays a role similar to nationality, ethnicity, class, or any other method of group identification: binding the group together and contrasting members with outsiders. There are a number of historical incidents of religious terrorist groups, such as the Jewish Zealots, Hindu Thugs, and Shia Assassins, but also ideological non-religious networks and states that employed suicide attacks, including the Tamil Tigers and Japanese kamikazes.[45] In the 20th century, various communist groups, who adamantly rejected religion, proved among the most successful insurgents.[46] While religion may motivate individual fighters, the organizations to which they belong pursue earthly, political goals. Al Qaeda's strategies and those utilized by Islamic insurgents appear similar to those of non-religious groups, indicating that religiosity cannot primarily explain the threat posed by jihadist organizations. Religion is not the only type of ideology that produces fanatics.

[43] Bergen, *The Longest War*.

[44] Those emphasizing religion include Stern, *Terror in the Name of God*; Juergensmeyer, “Terror in the Mind of God,” and Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*.

[45] Pape, *Dying to Win*.

[46] Arquilla, *Insurgents, Raiders, and Bandits*, p. 4 and ch. 17.

Information Technology and Networks' Capabilities

In the 21st century, the United States suffered the largest mainland attack by a foreign entity since the War of 1812 at the hands of a non-state network rather than a state; easily defeated two governments in Afghanistan and Iraq, but had difficulty suppressing the subsequent insurgencies; and engaged in a global war against al Qaeda and the international jihadist movement. The experience of other nuclear weapons states in the 21st century has been remarkably similar, as Russia, the United Kingdom, India, Pakistan and Israel have all mostly cooperated or at least avoided direct confrontation with symmetric adversaries, easily defeated smaller state governments, engaged in difficult conflicts against non-state networks, and lost civilians to terrorist attacks. (The world's two other nuclear weapons states, China and France, did not engage in any conflicts in the period from January 2000 to July 2013 that caused 25 or more battle-related deaths).[47]

Russia easily won an interstate war against Georgia in 2008, but proved unable to defeat insurgencies in the Caucuses, and lost 186 children in the Beslan school massacre in September 2004.[48] The United Kingdom quickly deposed Saddam Hussein's government in 2003 as part of the American-led coalition, but faced considerably more military casualties in a six-year fight against the Iraqi insurgency and over ten years fighting against the Afghan insurgency, while losing more civilians in the terrorist attack on London's transportation system in 2005 than in any international conflict. India mostly avoided violent confrontation with its longstanding rival Pakistan, losing more soldiers to insurgents in Kashmir, while an attack on Mumbai by Lashkar e Taiba in November 2008 killed 164 and injured an additional 308.[49] Similarly, Pakistan mostly avoided confrontation with India while fighting ongoing conflicts with various non-state networks in the Federally Administered Tribal Areas along its northwest border with Afghanistan. For comparison, Pakistan lost 1,174 soldiers in its last

[47] "UCDP Conflict Encyclopedia."
[48] "Putin meets angry Beslan mothers."
[49] "HM announces measures to enhance security."

major engagement with India in the 1999 Kargil War,[50] but constantly fought non-state networks throughout the 2000s, suffering 3,318 fatalities in 2009 alone.[51] Finally, Israel cooperated with former adversary Egypt to maintain a partial blockade of the Gaza Strip, avoided direct confrontation with current rival Iran while carrying out covert action that has delayed Iran's nuclear program,[52] and destroyed a nuclear reactor in Syria on September 6, 2007 with no repercussions.[53] However, Israel failed to achieve its goals in a war against Hezbollah in the summer of 2006, while enduring ongoing rocket fire from Hamas and other Palestinian resistance networks in the Gaza strip that killed 45 Israeli civilians and injured 1,994 from 2006 through 2012.

In the 21st century thus far, global and regional powers have cooperated or avoided direct confrontation with each other, and faced a much greater security challenge from non-state networks than from states. This pattern is widespread and apparent, suggesting that something about the current international security environment is the cause. Part of the explanation likely rests with 21st century information technology, as the spread of the internet, global media, and mobile phones have greatly enhanced non-state networks' information acquisition and dissemination capabilities.

The internet raises new international security concerns by granting transnational networks the ability to thrive without attachments to territory. Great power retaliation can easily destroy bases and training camps, but does not eliminate networks' ability to organize, recruit, strategize, fund-raise, and spread ideology online. While fleeing or hiding from attacks in the physical realm, non-state networks can remain active on the internet, inspiring followers, sharing information, and planning attacks. This enables networks to extend their reach beyond a specific location and provide sympathizers with the information they need to become self-starters, making networks with a significant internet presence

[50] "UCDP Conflict Encyclopedia."

[51] "Growing Terrorism in Pakistan."

[52] Vick, "Spy Fail: Why Iran Is Losing Its Covert War with Israel."

[53] "IAEA: Syria tried to build nuclear reactor."

more difficult for powerful states to destroy.[54] Every group on the US State Department's list of designated terrorist organizations maintains an internet presence, including over 4,300 separate terrorist-related websites documented by Gabriel Weimann.[55] This demonstrates terrorists' "evaluation of the medium's effectiveness," and suggests additional undiscovered sites, chat-rooms, and forums.[56]

As CIA bin Laden expert Michael Scheuer argues in *Imperial Hubris*, use of the internet is essential to al Qaeda's expansion into a global movement. Through a variety of websites, jihadists debate strategy, spread propaganda, gather intelligence, and educate new recruits or potential allies. "The internet," Scheuer wrote in 2004, "allows militant Muslims from every country to meet, talk, and get to know each other electronically, a familiarization and bonding process that in the 1980s and early 1990s required a trip to Sudan, Yemen, Afghanistan or Pakistan." Additionally, websites directly or indirectly related to al Qaeda's cause share intelligence on targets, justifications by religious scholars, and spread "online military training: small unit-tactics; the use and manufacture of toxins and poisons; trade craft for intelligence activities; martial arts manuals; textbooks, or sections thereof, dealing with the theory and construction of weapons of mass destruction; al Qaeda's now-famous *Encyclopedia of Jihad*" and more.[57] This rapidly increasing trove of information is readily available in English and Arabic to any non-state actor interested in attacking states, not just those that support al Qaeda's cause; and because of the increasing proliferation of information technology and internet cafés, it can be accessed and debated with relative anonymity.

Beyond computer terminals, rapidly proliferating mobile devices with internet access grant networks real-time open-source intelligence as they conduct operations. In November 2008, 10 members of Lashkar e Taiba entered Mumbai by sea, split into five two-man teams, and killed 164

[54] See Atran, "The Moral Logic of Suicide Terrorism."
[55] "Foreign Terrorist Organizations" designated by the U.S. State Department.
[56] Weimann, *Terror on the Internet*, p. 105.
[57] Scheuer, *Imperial Hubris*, p. 81.

people with automatic rifles and grenades over the course of three days.[58] According to Indian officials, the attackers utilized BlackBerry smart phones, planning the route from Karachi to Mumbai by GPS, familiarizing themselves with Mumbai's streets by reviewing online maps, and monitoring the events via internet news sites.[59] Continuous access to news coverage granted the attackers up-to-date details on the actions of their cohorts and the movements of Indian security services. If they did not have mobile internet access, the Mumbai attack probably would not have been as deadly, and may not have occurred at all.

Sharing information on the internet enhances the capabilities of insurgent networks as well as terrorist groups. For example, improvised explosive devices (IEDs) proved to be the most successful weapon Iraqi insurgents deployed against the American-led occupying forces. From 2003 through late 2007, IED attacks in Iraq occurred, on average, every 15 minutes, and accounted for approximately two thirds of American casualties.[60] Instructions on building IEDs proliferate on the internet, with many designs utilizing cheap, commercially available technology. Iraqi insurgents have made bombs out of artillery shells, fertilizer, gasoline, and propane canisters, triggered by cell phones, car key fobs, walkie-talkies, toy remote controls, wireless doorbell buzzers, and garage door openers.[61]

Additionally, because of internet-based information sharing, the United States had difficulty keeping up with IED adaptability. Iraqi insurgents created websites that featured videos of successful attacks, experimental explosions, and counterinsurgent troop movements, providing a forum to share techniques to overcome American countermeasures. According to the United States military, after the

[58] "Pakistan Admits India Attack Link."

[59] "Mumbai Attacks: Terrorists Monitored Coverage on UK Sites Using Blackberry Phones."

[60] According to "Left of Boom: The Struggle to Defeat Roadside Bombs," by the Washington Post's Rick Atkinson, as of September 2007, IEDs account for 63% of 3,092 American deaths and 69% of the 28,009 American wounded since the war began in March 2003.

[61] Saletan, "Technology Lessons from the Iraq War."

US introduced new anti-IED technology, insurgents typically posted instructions on how to defeat it within five days.[62]

The rise of the global media improved network effectiveness as well. Terrorist attacks had a greater psychological and political impact as footage of them played over and over on screens around the world. Meanwhile, the media kept the public informed about distant asymmetric conflicts, highlighting the excesses of strong actors. For example, images depicting the United States' destruction of Fallujah and torture scandals at Abu Ghraib received significant coverage in numerous countries, motivating the insurgency and undermining domestic and international support for the American war effort in Iraq. Similarly, global media coverage of America's "enhanced interrogation techniques" and treatment of "enemy combatants" held extra-judicially in the prison at Guantanamo Bay increased international opposition to the War on Terrorism.

Robotics and States' Capabilities

The spread of the internet, expansion of the global media, and proliferation of cell phones all enhanced the capabilities of non-state networks, improving their performance in asymmetric conflicts against states. However, focusing entirely on how information technology empowers individuals ignores how powerful states have reacted to these developments. While strong actors may have been surprised by the challenges posed by non-state networks in the wake of the information technology revolution, they have adjusted strategies and cultivated new technologies in response.

To anticipate attacks and protect against terrorism, the American intelligence budget has increased dramatically in the last ten years, while over 1,000 new companies related to homeland security have arisen.[63] Meanwhile, the United States' strategy against al Qaeda has evolved, from greater information sharing across American intelligence agencies and those of other countries, to

[62] See Saletan, "Technology Lessons from the Iraq War," or Bush, "President Discusses Freedom and Democracy in Iraq."
[63] Priest and Arkin, "A Hidden World, Growing Beyond Control."

increased attacks on suspected al Qaeda leaders and operatives on foreign soil, including Yemen and Pakistan. In Iraq, after failing to suppress an insurgency composed largely of Sunni Arabs, the United States courted Sunni leaders and switched to a population-centric counterinsurgency strategy, decreasing the frequency of insurgent attacks.[64] Perhaps most significantly, the United States and other advanced countries have developed various types of military robots, which may be able to neutralize some of networks' advantages in asymmetric conflict.

Robots have already taken on some of the most dangerous tasks in warfare, such as transporting supplies through hostile areas, searching for and dismantling roadside explosives, and conducting aerial reconnaissance and attack missions. This reduces the risks to strong actor soldiers, limiting the costs insurgent networks can impose on powerful militaries. Robotic systems do not need to eat, sleep, or use the bathroom; they do not panic or fear attacks by opposing forces. Unmanned aerial vehicles armed with missiles can hover for hours, waiting for the opportune moment to fire, thereby increasing the chances of success while potentially reducing collateral damage. Additionally, whether in the air or on the ground, autonomous machines can gather information using cameras and a variety of sensors. Potentially, a swarm of robots could collectively gather enough information to give soldiers and commanders a detailed, real-time understanding of a given battlespace.

With this in mind, this dissertation argues that networks' exploitation of post-Cold War technological and geopolitical developments helps explain the heightened challenge posed by non-state networks in the early 21st century. In the aftermath of a major international transition, networks' organizational agility enables relatively rapid development of new strategies, while bureaucratic rigidity creates an institutional drag on the development of state counter-strategies. The rise of al Qaeda coincides with world-changing geopolitical and technological transitions: the end of the Cold War and the spread of the internet, mobile phones, and global media. The changes in the international

[64] Petraeus, "Report to Congress on the Situation in Iraq."

order and information technology-driven enhancement of individuals’ capabilities created an opportunity for al Qaeda and more localized insurgent networks to develop strategies that achieved some success against great powers.

It is important to note that not every network will rapidly and successfully adapt to changes in the international system, just that some will. Therefore, major geopolitical transitions and technological changes that empower individuals will likely be followed by an increase in weak actor success in asymmetric warfare in general, not by improvements in every weak actors' capabilities. Many non-state networks, probably most, will fail to adapt, and either stagnate or decline; but those that successfully adapt will find themselves with a window of opportunity to challenge stronger state opponents.

However, this logic would then predict a gradual decline of weak actor success in international asymmetric conflict, as powerful countries turn the ship of state to face the new challenge. This decline will presumably continue until another significant international transition creates a new window of opportunity for networks to exploit. That transition may already be on the horizon, as increasingly sophisticated robots become commercially available, cheaper and easier to acquire. With information-gathering robots, networks can monitor strong actor troop movements, helping them anticipate raids and respond to ground advancements, and case potential targets without needing to send a human operative. By loading small, commercially available robots with explosives, non-state networks could create a kamikaze drone capable of crashing into a target and exploding, almost the weak actor equivalent of a guided missile. Unfortunately, it would not be particularly surprising if someone flew an explosives-laden robotic plane or helicopter designed for aerial photography or another commercial purpose into a building or bridge in the United States or another developed country. However, if networks develop innovative ways to use robots to threaten or resist powerful states, advanced countries will develop anti-robot measures in response, reasserting their resource advantage until another transition facilitates the rise of a new challenge.

Chapter Outline

Part 1: Asymmetric Warfare

1) Chapter 1 – A General Theory of Asymmetric Warfare

This chapter lays out a theory of asymmetric conflict, highlighting the conditions that sometimes enable weaker actors to win confrontations against stronger opponents. I propose that conflicts featuring a large resource asymmetry inherently feature non-material asymmetries as well, of resolve, expectations, organizational structure, responsibility, information, and institutional agility. While material asymmetry benefits the side with more resources, these non-material asymmetries often favor relatively weak actors.

2) Chapter 2 – Testing and Applying the Theory

This chapter introduces some hypotheses derived from the theory of asymmetric warfare that help explain why recent conflicts against non-state networks have proven more challenging for powerful countries than conflicts against weaker states. I test these hypotheses using an original data set consisting of every conflict in which at least one side possesses nuclear weapons and find strong support for the claim that networks are superior to small states when it comes to fighting nuclear powers, especially in the post-Cold War internet era.

3) Chapter 3 – The War on Terror: Al Qaeda the Organization and Al Qaeda the Idea

Chapter three applies the framework laid out in the first two chapters to analyze the United States' War on Terror. In particular, I distinguish between the challenge of fighting al Qaeda, the organization responsible for the September 11th attacks, and combating the larger international jihadist movement, which al Qaeda helped catalyze.

Part 2: Robotics

4) Chapter 4 – Asymmetric Warfare and the Robotics Revolution

The first chapter in Part 2 catalogues the ground-based and aerial military robots developed by the United States and other advanced countries since the end of the Cold War. Existing and forthcoming robotic technologies have the potential to significantly improve strong actors' capabilities against non-state networks, and in many ways they already have.

5) Chapter 5 – Robotics and Non-State Networks

Building on the previous chapter, chapter five considers the ways robotics could enhance the capabilities of weak actors in asymmetric warfare. As autonomous machines, especially small unmanned aerial vehicles, become commercially available and decline in price, it will become progressively easier for non-state networks to acquire robots and put them to use in their fights against stronger opponents.

6) Chapter 6 – Robotics and Strong Actor Strategy against Localized Insurgencies: Pursuing Information Dominance

This chapter discusses Network-Centric Warfare (NCW), a military doctrine developed by the United States that utilizes information technology to improve coordination between military units.

After laying out some criticisms of NCW, I argue that robotics can help practitioners approach their goal of information dominance.

7) Chapter 7 – Robotics and Strong Actor Strategy in Irredentist Conflicts: Defending Israeli Civilians

While the previous chapter focuses on localized insurgencies, chapter seven considers the effect of the robotics revolution on strategies of irredentist conflicts. Analyzing Israel's conflict with Hamas and other Gaza-based groups, I argue that robotic anti-missile systems can potentially protect Israeli civilians from rocket attacks, Hamas' most effective method of imposing costs on Israel since it gained control of Gaza, thereby enabling a more defensive strategy.

8) Conclusion

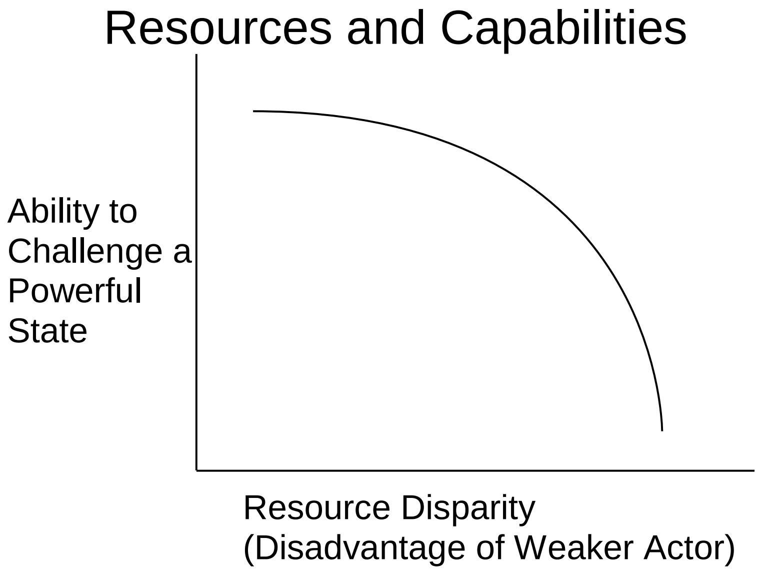
Part 1:

Asymmetric

Warfare

Chapter 1: A General Theory of Asymmetric Warfare

Asymmetric warfare is armed conflict between materially disparate adversaries. While symmetric opponents possess similar levels of material resources and military technologies, asymmetric combatants fight at significantly different resource levels. If everything else is equal, the side with greater resources will win military conflicts. Therefore, the entities that control the most resources, Great Powers, dominate the international system.[65] These powerful states can engage each other in symmetric warfare, while all other entities that wish to challenge a Great Power must fight under conditions of material disparity.



As this graph depicting the relationship between resources and capabilities shows, powerful states are a serious threat to each other, but can neutralize threats more easily as their material

[65] The central insight of structural international relations theory. See Waltz, Mearsheimer, etc.

advantage increases. This represents the foundation of modern international relations theory,[66] and fits the general form C (capabilities) = -aX^2 - bX.

I chose to portray this relationship as exponential (with an X^2) rather than linear (with just X) for two reasons. First, military theory argues, and the history of warfare confirms, that small resource gaps are rarely decisive. For example, in a conflict between 10,000 and 10,050 equally armed soldiers, factors such as strategy, tactics, and resolve will likely be more important than the slight resource gap. However, as resource disparity increases, the rate at which the material gap affects the outcome also increases, making resource advantages increasingly decisive. A force of 10,000 should easily dispatch an equally armed force of 50. This is consistent with Lanchester's Square Law,[67] which predicts that the ratio of casualties in mechanized warfare will be the inverse square of the ratio of forces. (A simple example: in a conflict of 500 airplanes vs. 100 airplanes of the same type, the force ratio is 5:1. Therefore, Lanchester would predict a casualty ratio of $1/5^2$ or 1:25, with the force of 500 eliminating its opponent at the cost of four planes). Second, while I theorize that non-material dimensions of warfare affect the outcome of asymmetric contests, I accept the realist assumption that material resources are the most important factor in any military conflict, and have captured this by depicting the relationship between resources and capabilities as exponential, and the effect of other, non-material factors on capabilities as linear (elaborated below and demonstrated in the graph depicting the Asymmetry of Agility).

While the quantity and quality of soldiers and weaponry may be the most important factor in warfare, a basic glance at history shows that the relationship portrayed in the graph between resources and capabilities does not always hold. Sometimes the weaker side achieves its goals; and Great Powers

[66] Known as structural realism or neo-realism, as introduced by Kenneth Waltz in *Man, the State, and War* and laid out in Waltz' *Theory of International Politics*. Many international relations scholars have expanded upon, challenged, or provided alternatives to structural realism, but few, if any, dispute the claim that more resources can provide greater military capabilities.

[67] Lanchester, *Aircraft in Warfare*, especially chapters 5 and 6.

have occasionally found small enemies more troublesome than midsized opponents. Therefore, an additional factor must affect asymmetric conflicts that enables relatively weak actors to overcome their material disadvantages. Otherwise the side with more resources would always win.

Weak Actor Strategies in Asymmetric Conflict: Guerrilla Warfare, Insurgency, and Terrorism

Guerrillas, insurgents, terrorists, armed resistance, "freedom fighters," rebels, and revolutionaries all fight stronger opponents. Though these non-state actors are all influenced by the dynamics imposed by material disparity, realities of conflict frequently blur the distinction between them. The same individual could be most accurately described as a guerrilla when ambushing or resisting engaged military units, an insurgent when destroying government infrastructure or attacking a police station, and a terrorist when targeting non-combatants. Most terrorist and insurgent organizations utilize a combination of these tactics; and all justify their actions as legitimate resistance, while governments inevitably denounce unsanctioned violence as illegal. Therefore, this study sets aside questions of legitimacy and legality as inherently subjective, and focuses on the adversaries' objective material disparity. Though not perfectly synonymous, guerrilla warfare, insurgency, and terrorism overlap significantly, and together form the set of weak actor strategies in asymmetric conflict.

Vietnamese general Vo Nguyen Giap explicitly defined guerrilla warfare as the strategy "of the people of a weak and badly equipped country who stand up against an aggressive army which possesses better equipment and technique."[68] Echoing earlier guerrilla theorists, al Qaeda strategist Abd Aziz al Muqrin writes that insurgency "is a war waged by a poor and weak party using the

[68] Giap, *People's War People's Army*, p. 103.

simplest methods and the cheapest means against a strong opponent who has a superiority in arms and equipment."[69] Given this material asymmetry, guerrillas must adopt a long-term view of the conflict, aiming to gradually defeat their enemies both politically and militarily. "Another fundamental characteristic of the guerrilla soldier" Che Guevara writes, "is his flexibility, his ability to adapt himself to all circumstances, and convert to his service all the accidents of the action."[70] Guerrilla warfare is based on counter-strategy, creatively employing whatever resources become available, acting underhanded, sneaky, and generally fighting dirty. Guerrillas do not wear uniforms or announce allegiances, which allows them to blend in with the civilian population and hide from retaliation, like fish swimming in a sea of people according to Mao Zedong.[71] They embrace surprise, sabotage, and assassination, and design hit-and-run raids to exploit enemy weaknesses. While traditional armies aim to capture and hold territory, guerrillas move constantly, harassing the enemy wherever possible.

To succeed in asymmetric warfare, writes Andrew Mack, a relatively weak actor must first "refuse to confront the enemy on his own terms."[72] In symmetric conflicts, adversaries possess comparable levels of material power and similar military technologies. Though not perfectly equal, symmetric antagonists have the means to compete on the same plane, and rely on superior mobilization, discipline, maneuver, and luck to succeed. By contrast, in direct combat against asymmetric adversaries, strong actors can usually translate material advantage into overwhelming victory. As Ivan Arreguin-Toft demonstrates, of 173 asymmetric wars from 1800-2000, weak actors won only 23.2% of 151 conflicts when directly confronting their stronger opponents, but defeated more

[69] Al Muqrin, *Al-Qaida's Doctrine for Insurgency,* p. 92.
[70] Guevara, *Guerrilla Warfare*, p. 20.
[71] See Mao, "The Struggle in the Chingkang Mountains," 1928; "Problems of Strategy in China's Revolutionary War," 1936; "Problems of Strategy in Guerrilla War against Japan," 1938; "On Protracted War," 1938.
[72] Mack, "Why Big Nations Lose Small Wars," p. 176.

powerful adversaries in 63.6% of 22 confrontations in which they took an indirect approach and refused to fight on the stronger actor's terms.[73]

Arreguin-Toft's study is perhaps the most prominent international relations research on asymmetric conflict, and offers empirical support for Mack's main contention that weak actors will probably lose if they meet stronger opponents in direct military confrontation. However, his categories of "direct" and "indirect" strategies are too broad to advance the understanding of weak actor successes, and most asymmetric conflict strategies combine elements of both types. "Direct strategic approaches—e.g., conventional attack and defense," he writes, "target an adversary's armed forces with the aim of destroying or capturing that adversary's physical capacity to fight, thus making will irrelevant."[74] This category straightforwardly captures the traditional model of large scale maneuver warfare, which focuses on counterforce attrition and holding territory.[75] In conflicts between a direct offense and a direct defense, "nothing mediates between relative material power and outcomes,"[76] and the stronger actor usually wins decisively, as depicted in the Resources and Capabilities graph above. By contrast, indirect approaches seek to undermine an opponent's will to continue the fight, thus making the balance of forces irrelevant.

However, few weak actors in the modern era are naive or overconfident enough to line up on a battlefield against a materially superior enemy, and most lack the means to even consider primarily direct strategies. Arreguin-Toft's study includes wars between strong states and weak states, along with conflicts between states and non-state actors, which explains the presence of many direct strategic interactions in his database. Nevertheless, his theory fails to capture the strategies of most terrorist,

[73] Arreguin-Toft, p. 45. His database includes all conflicts from the years 1800-2000 with more than 1,000 battle deaths in which the combatants have a measurable material power ratio of 5:1 or greater.

[74] Arreguin-Toft, p. 34.

[75] "Counterforce" attacks target opponents' military resources, reducing war-fighting capabilities. By contrast, "countervalue" attacks target opponents' non-military assets, such as civilian population centers, aiming to cause enough pain to convince opponents to abandon their war effort. See Quester, *Offense and Defense in the International System.*

[76] Arreguin-Toft, p. 34.

insurgent, and guerrilla groups, leaving an opening for this study to explore the variety of weak actor strategies that fall under the broad category of "indirect."

Overcoming Material Disparity

While avoiding direct engagement with more powerful enemy forces, relatively weak non-state actors hope to achieve their primary goals by one of two main strategies: 1) acquire more power while wearing down the enemy's capacity, until material asymmetry is no longer the defining feature of the conflict; 2) impose military, economic, and political costs until the enemy abandons its military campaign, withdraws forces, or alters a particular behavior. Domestic conflicts typically classified as revolutions, civil wars, or guerrilla insurrections fit the first form, as weak actors intend to take over the state, like the Bolsheviks, or become the dominant governing force of a given geographical area, like the American Confederacy. These conflicts end when the challenger to the government becomes the strong actor and can use the state apparatus to crush opponents, or achieves relative symmetry and can oppose the government using conventional military means.

However, many weak actors cannot plausibly reach relative symmetry, and must rely on the second strategy of compellence.[77] This especially applies to localized insurgencies, like Vietnam or Iraq, as the weak actor seeks the withdrawal of foreign forces or a decrease of foreign influence, rather than control of the foreign state's territory. Additionally, the second main strategy describes the early asymmetric phases of domestic conflicts that finish as symmetric, as in the case of Mao and Che's communist revolutions. The greater the weak actor's material disadvantage, the more asymmetric the conflict, and the more restricted weak actors become to strategies that avoid the enemy's strengths.

[77] Thomas Schelling, in *Arms and Influence*, defined "compellence" as using a limited amount of force to convince an opponent (i.e. "compel" them) to abandon a particular behavior. "The threat that compels rather than deters," Schelling writes, "requires that the punishment be administered until the other acts, rather than if he acts," p. 70.

Given this restriction, weak actors must develop strategies that exploit the non-material dimensions of asymmetric warfare.

Non-material Asymmetries

Resource disparity defines asymmetric conflicts, but not the entire difference between relatively strong and weak actors. Discussing guerrilla strategy, Mao argued that "the enemy has advantages only in one respect…but shortcomings in all others," while insurgents "have shortcomings in only one respect but advantages in all others."[78] This implies that material power is only one element of asymmetric warfare, and that weaker actors can overcome their resource disadvantage by exploiting the non-material asymmetries inherent in material disparity. Controlling vast resources conveys a number of benefits, but can be burdensome as well, creating fixed targets that need defending. Relatively strong actors tend to have numerous interests and responsibilities beyond the conflict, heightened expectations of low-cost victory, more information to process and protect, and less flexible institutional structures. Overall, the tradeoff for greater resources is less agility.

Asymmetry of Interest/Resolve

Andrew Mack proposed that resource asymmetry leads the weaker actor to have greater interest in the conflict. The stakes in asymmetric warfare, he argues, are inherently higher for the weaker party because the price of their defeat is the loss of independence or total destruction. By contrast, the strong actor does not face a threat to its survival. When survival is at stake, as in the symmetric World Wars, or domestic revolutions, the war effort takes "automatic primacy above all other goals."[79] However, in international asymmetric warfare the strong actor's interest in the conflict is limited, which allows for

[78] Mao, "On Protracted War," p. 208.
[79] Mack, p. 184.

debates within the foreign state over the ideal allocation of resources, creating the political conditions that could lead to withdrawal.

Beyond material costs—money, soldiers, equipment—an asymmetry of interest leads the strong actor to suffer greater political costs. According to Mack, "when the survival of the nation is not directly threatened, and when the obvious asymmetry in conventional military power bestows an underdog status on the insurgent side, the morality of the war is more easily questioned."[80] This implies that domestic and international opposition to the war will grow due to moral outrage over the death and destruction caused by a powerful state asserting a less-than-vital interest. By contrast, when survival is at risk, as it is for the weaker actor, "the propensity to question and protest the morality of the means used to defeat the enemy is markedly attenuated."[81]

By avoiding direct combat, where material advantage could prove decisive, guerrillas can force their opponents into a "protracted war."[82] According to Mao, denying the enemy victory extends the conflict, and creates a situation in which insurgents' can slowly bleed powerful armies, imposing costs that weaken resolve. Given enough material advantage, a stronger actor will win any contest of force, which implies that weak actors can win only if they can make the conflict a contest of will. As Mack notes, in cases of weak actor victory, "success for the insurgents arose not from a military victory on the ground—though military successes may have been a contributory cause—but rather from the progressive attrition of their opponents' political capacity to wage war."[83]

[80] Mack, p. 186.
[81] Mack, p. 187.
[82] Mao, "On Protracted War."
[83] Mack, p. 177.

Asymmetry of Expectations

Following the relationship between resources and capabilities as depicted in the graph above, strong actors' material advantage leads them to expect rapid, low cost victory. Weaker actors, on the other hand, face an overwhelmingly powerful foe, and cannot expect that victory will be easy or cheap. As a result, prolonged confrontations disadvantage stronger actors by enhancing the weak actors' relative resolve advantage. As conflicts drag on, the resource toll grows, creating "guns-or-butter"[84] debates in actors with multiple interests, which Mao referred to as "contradictions within the enemy's camp."[85] The more a strong actor expects a quick and easy victory, the more protracted conflicts and their accompanying resource drain lead to arguments within the strong actor to shift resources to other priorities.

The asymmetry of expectations also disrupts traditional war assessment metrics. Expecting an easy victory, strong parties are particularly affected when they lose soldiers, and less encouraged by enemy casualties. Expecting safety at home, as well as in embassies or bases, strong actors are more affected by the deaths of civilians or off-duty soldiers. Weak parties, by contrast, expect to lose most battles and suffer greatly in pursuit of victory, and therefore consider individual casualties less costly. Small victories greatly encourage weaker actors, while any developments that do not portend decisive victory discourage strong actors. As a result, as Henry Kissinger noted, "the guerrilla wins if he does not lose," while the conventional state army "loses if it does not win."[86]

[84] See Powell, Robert, "Guns, Butter, and Anarchy" for the role this plays in state decision-making in international relations.

[85] Mao, "Problems of Strategy in Guerrilla War Against Japan."

[86] Kissinger, "The Vietnam Negotiations," p. 214.

Asymmetry of Organization

To utilize large amounts of resources, states have adopted bureaucratic institutions. Bureaucratic organizations are based on centralized power and clearly-defined positions arranged in a top-down structure (frequently depicted as an inverted tree). The positions and the structure outlast any individual members, who can be replaced with another person fulfilling a similar function. All states utilize this structure to organize their governments and militaries, as do all large businesses, with the most powerful states possessing the largest bureaucracies.

By contrast, many non-state actors control considerably fewer resources than states, and have adopted a networked structure. Networks are organized based on nodes (i.e. individuals), and structured by the connections between them. They are "bound together by shared values, a common discourse," and an "exchange of information and services."[87] Networks are thus more fluid than bureaucracies, changing as individuals leave or join and as the relationships between the members evolve. Insurgencies, transnational terrorist organizations, drug cartels, political activists and many smaller businesses organize as networks. This institutional form is less able to concentrate resources or coordinate individual actions than bureaucracy, but more capable of changing rapidly and more open to individual initiative. In other words, compared to bureaucracies, networks have less material power, but greater agility.

To prevent a decisive defeat in asymmetric warfare, relatively weak actors need to minimize their vulnerability to strong actors' militaries. Unlike the vertical hierarchies of state armies, terrorists and insurgent groups tend to organize as horizontal networks to avoid decisive counterattacks or decapitation strikes. As a result, non-state networks are less attached to specific territory, fleeing areas where their enemy is strong, only to regroup and attack elsewhere. Members tend to avoid uniforms or other readily identifiable characteristics, and thus can blend in among local populations. Networks

[87] From Keck and Sikkink's definition of a transnational advocacy network in *Activists Beyond Borders*, ch. 1.

keep the location—or sometimes even the identity—of their leaders hidden, denying their opponents a clear target.

In addition to enhancing the prospects of survival, a networked organization enhances weak actors' ability to surprise opponents with unanticipated attacks and fluid strategies. Networks can employ "idiosyncratic approaches" due to their "cellular and compartmented nature."[88] In *Networks and Netwars*, Arquilla and Ronfeldt argue that this looser organizational form grants networks a "capacity for swarming,"[89] in which they attack unexpectedly, disperse, and later reform to attack in a different manner. This poses a particular difficulty for militaries and security services accustomed to fighting bureaucratic opponents, who utilize consistent strategies, and have known identifies and fixed targets. Unlike bureaucratic state militaries, non-state networks cannot wield vast amounts of material power, but can adapt quickly to changing circumstances. For example, as Gen. Montgomery Meigs argues, the threat al Qaeda poses to the United States "derives from its ability to change its operational system at will in response to the methods needed to approach and attack each new target."[90] Furthermore, non-state networks grant greater operational independence to sub-units, decreasing the value of individual captures, and creating the possible threat of sleeper cells.

However, there are numerous disadvantages to networked organizational forms, primarily an inability to exercise concentrated power.[91] Decentralization limits strategic coordination by decreasing the reliability of communications and efficiency of information sharing. Separate nodes may have similar ideologies or long-term goals, but different immediate circumstances or preferences. "As a result, resources may be used poorly, contradictory tactics selected, and activities carried out that serve

[88] Meigs, "Unorthodox Thoughts about Asymmetric Warfare," p. 8.
[89] Arquilla and Ronfeldt, *Networks and Netwars,* p. 12.
[90] Meigs, p. 10.
[91] See Eilstrup-Sangiovanni and Jones, "Assessing the Dangers of Illicit Networks."

parochial short-term interests rather than the larger mission."[92] Notably, the importance of trust and interpersonal connections limits scalability, and subjects larger networks to splintering. Therefore, bureaucratic organization is probably necessary for symmetric confrontation between powerful adversaries. However, a networked organization mitigates the disadvantages for weak actors facing dramatic material asymmetry. Though their capabilities may be limited, non-state networks pose a greater challenge for powerful states than weak actors organized bureaucratically, because they lack clear targets or reliable negotiating partners, and can changes strategies more easily.

Asymmetry of Responsibility

The less powerful an organization, the fewer its responsibilities to non-combatants. "The insurgent is fluid," writes David Galula, "because he has neither responsibility nor concrete assets; the counterinsurgent is rigid because he has both."[93] Compared to governments, non-state networks are less concerned with maintaining infrastructure, protecting civilians, managing an economy, and honoring international agreements. They depend on commercially available products, makeshift workshops, the black market and theft for military supplies, rather than an industrial base or international trade. To the extent that they provide government-like functions, networks are exceeding expectations.

States, by contrast, have greater responsibilities to their respective populations. All but the most coercive states must provide some security and basic services or face rejection. When non-combatants have the option of assisting or joining an insurgency, a state's need to live up to its governing responsibilities increases; not necessarily because the insurgency has a greater ability to provide government functions, but because it stands in opposition to the failing government. The

[92] Eilstrup-Sangiovanni and Jones, p. 21.
[93] Galula, *Counterinsurgency Warfare*, p. 7.

state’s failure to meet its responsibilities undermines popular support, which decreases a source of material power and intelligence, thereby granting the resistance an advantage.

As a result, violence by the weaker actor can be primarily disruptive. Insurgents or terrorists can hurt states by destroying infrastructure or denying civilians a sense of security, while governments need to protect all major assets at once, requiring far more resources. A disruptive strategy is attractive to materially disadvantaged combatants because, as Galula argues, “disorder... is cheap to create and very costly to prevent.”[94] By sowing disorder, insurgents force states to devote more resources towards guarding against attacks, increasing the material and political costs of the conflict. Therefore, the asymmetry of responsibility suggests a refinement of Kissinger’s maxim: the guerrilla wins if he disrupts the state’s ability to function normally, while the state wins only when it eliminates or prevents the guerrillas’ capacity for disruption.

Asymmetry of Information

A networked organization is particularly advantageous to weaker actors because it capitalizes on the asymmetry of information. Guerrillas possess specific information regarding group membership, the allegiance of local non-combatants, and the timing and location of idiosyncratic attacks. The aim of a terrorist group, therefore, is to keep this information hidden from its enemy; and a networked organization compartmentalizes the information so that revelation of a given operation or identity does not compromise the entire organization.

Powerful states, by contrast, possess an immense amount of general information. From this general information, strong actors try to identify enemies and anticipate attacks. Though fairly straightforward in symmetric battles, “identifying the adversary” is far more difficult in asymmetric

[94] See Galula, “Insurgency is cheap, counterinsurgency is costly,” in *Counterinsurgency Warfare*, p. 6-7.

conflicts,[95] and this is compounded by the difficulty of routing the relevant information through bureaucratic channels in time to act. The inability to identify terrorists or insurgents sometimes leads states to employ indiscriminate violence, in the hope of killing combatants along with civilians, or intimidating them into switching their allegiance and providing more specific information;[96] though this often backfires by galvanizing opposition.[97]

As a result, popular support plays a more significant role in asymmetric wars between states and networks than in symmetric wars between bureaucratic armies. Among military and academic scholars, there is a virtual consensus that terrorists and insurgents utilize violence to “alter the attitudes and behavior of multiple audiences.”[98] Due to their material inferiority, non-state networks cannot hope to defeat state armies in direct combat, and are forced to design strategies that undermine political support for the conflict among the state’s decision-makers. To survive, prolong the conflict, and advance their goals, networks require some local and international legitimacy, which helps a network acquire the sanctuary, financial support, freedom of movement, and steady stream of recruits it needs to counter a state’s material superiority.

Localized insurgents will usually have greater knowledge of local preferences and forms of communication, and can exploit this asymmetry of information to frame foreign opponents as exploitative and imperialistic. Some organizations, like Hamas or Hezbollah, further enhance their domestic legitimacy by providing social services.[99] In general, states will have greater access to networks’ private information if local populations consider the network’s actions illegitimate, or if non-combatants perceive themselves as sharing an identity with the state. If networks use coercion to

[95] Trinquier, *Modern Warfare: A French View of Counterinsurgency*, p. 23.

[96] Valentino, Huth, and Balch-Lindsay, “Draining the Sea.”

[97] Kalyvas, “The Paradox of Terrorism in Civil War.”

[98] Crenshaw, *Terrorism in Context*, p. 4.

[99] See Norton, *Hezbollah*, especially ch. 5, or Levitt, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*.

garner popular support, the state will be unable to counter this intimidation unless non-combatants believe the state wants to protect them.

Networks can enhance their international legitimacy by actively promoting their political position and using local knowledge to highlight the most brutal of their opponents' actions. This helps networks acquire financial assistance or state sponsorship, granting them some of the resources of a state unaccompanied by the responsibilities of governing. Strong actors possess greater material resources to communicate intentions and spin events, but face considerable informational asymmetries when they try to delegitimize resistance networks, decreasing the chances of decisive strong actor victory.

This enforces the notion that wars between materially disparate adversaries are fundamentally political contests. Unless a massively larger party employs unlimited force, like the Nazis in response to the Warsaw Ghetto Uprising,[100] asymmetric conflicts are won or lost based on hearts and minds. "All insurgencies," notes the latest U.S. Army Counterinsurgency Field Manual, "even today's highly adaptable strains, remain wars amongst the people."[101] Therefore, the "battle for the population" is central to any asymmetric conflict.[102] This does not suggest, as Charles Dunlap mockingly argues, that "defeating an insurgency is all about winning hearts and minds with teams of anthropologists, propagandists, and civil-affairs officers armed with democracy-in-a-box kits and volleyball nets."[103] Capturing or killing committed insurgents plays a prominent role, but "there is a more certain way of eliminating the guerrilla than seeking to hunt him down among the civilians; it is to turn the civilians against him."[104] If the stronger actor is unwilling to massacre whole populations, the asymmetric conflict, by its nature, takes place in the political arena. As Audrey Kurth Cronin demonstrates,

[100] "The Warsaw Ghetto Uprising," The United States Holocaust Museum Online.
[101] "Counterinsurgency Field Manual," the U.S. Army and Marine Corps, foreword.
[102] Galula, *Counterinsurgency Warfare: Theory and Practice*, p. 4.
[103] Dunlap, "We Still Need the Big Guns."
[104] Valeriano and Bohannan, *Counter-Guerrilla Operations: The Philippine Experience*, p. 161.

"reducing popular support, both active and passive, is an effective means of hastening the demise of some terrorist groups."[105] Strong actor victory requires considerable political and military efforts, but, as Gen. David Petraeus repeatedly asserts, "there is no military solution to a problem like that in Iraq, to the insurgency of Iraq."[106]

Weak actors engaged in dramatically asymmetric conflicts, like transnational terrorist organizations and anti-colonial resistance, face insurmountable material power disadvantages, and must rely on informational strategies. They utilize violence primarily to demonstrate capabilities and resolve, spread fear, embarrass security services, inspire followers, and provoke overreactions.[107] Along these lines, terrorism can be defined as a strategy of asymmetric warfare that uses violence against non-combatants or civilian infrastructure to disrupt normalcy, creating a larger psychological/social/political impact on various audiences.[108] As Brigitte Nacos argues, "unlike common criminals, terrorists have the need to communicate in mind when they plan and stage their violent incidents; terrorists go out of their way in order to provide the mass media with cruel, shocking, and frightening images."[109] These images and the signals they send are far easier to create than suppress or control, creating an informational asymmetry that favors weaker actors.

Asymmetry of Agility

Conflicts between states and networks are shaped by the adversaries' resource disparity, which creates asymmetries of resolve, expectations, organization, responsibility and information. Taken together, these asymmetries suggest that networks enjoy greater institutional agility than their state

[105] Cronin, "How al-Qaida Ends," p. 42.

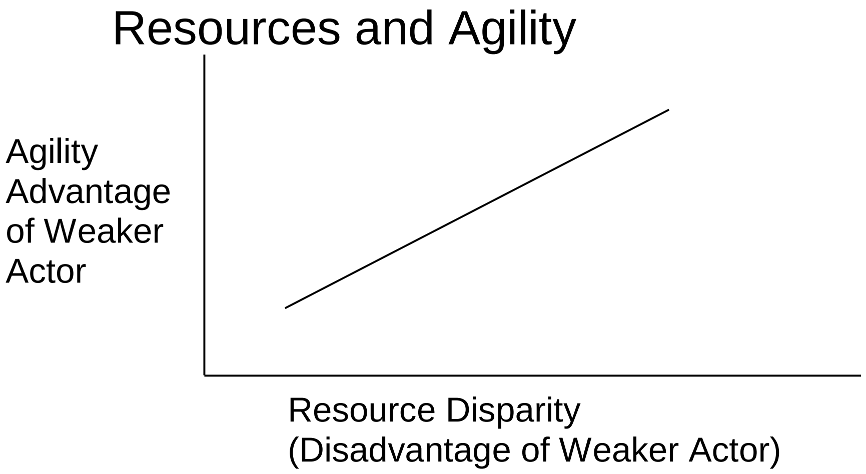
[106] "No Military Solution to Iraq, U.S. General Says."

[107] See Kydd and Walter, "The Strategies of Terrorism," for a discussion of the various signals sent by terrorist attacks.

[108] Non-combatants are anyone other than actively engaged military. This definition of terrorism draws upon, but differs somewhat from, those offered by Bruce Hoffman (see *Inside Terrorism*, pp. 39-40) and Brigitte Nacos (see *Mass-Mediated Terrorism*, pp. 24-28).

[109] Nacos, p. 14.

opponents. With lower expectations, less responsibility to maintain infrastructure or provide security, superior knowledge of their immediate circumstances, and a more flexible organizational structure, relatively weak actors have the potential to adapt more quickly than their stronger, more bureaucratic opponents. Therefore, while conflict between powerful states and weaker states may be determined by the effect of resource disparity on military capabilities ($C = -aX^2 - bX$, as depicted in the Resources and Capabilities graph above), conflicts between states and networks are influenced by the effect on agility as well.

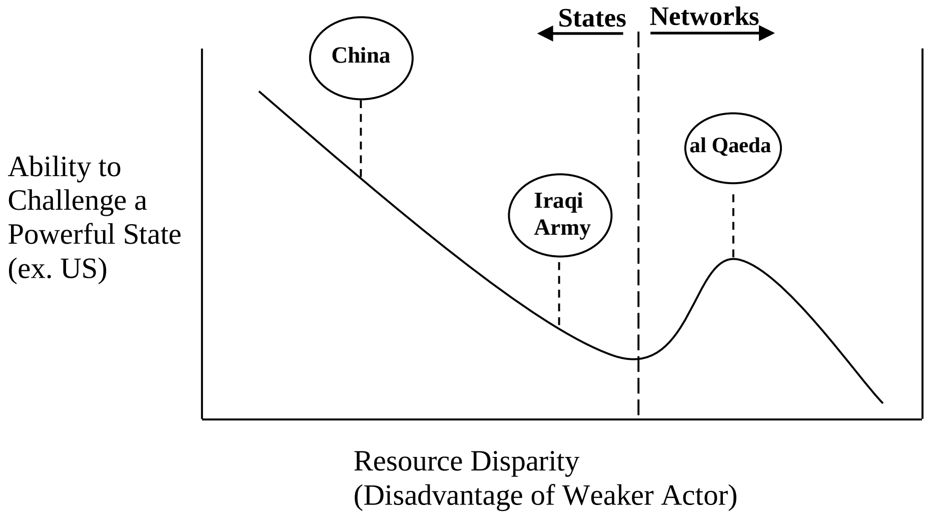


As the graph shows, in symmetric war, with no resource disparity, neither actor is significantly more agile than the other. However, as the resource gap increases, a smaller organization becomes relatively more agile than its larger opponent, fitting the general form $A = X$. This does not assume that every large organization will be less agile than all smaller organizations, just that resources have to be stored and managed, implying a tradeoff in which greater resource levels tend to create a drag on agility. I chose to portray the relationship as linear (with an X), in contrast to the relationship between resources and capabilities, which is portrayed above as exponential (with an X^2), to reflect the standard international relations claim that resources have a more significant effect on capabilities than on agility.

Material disparity thus remains the most significant factor in asymmetric warfare, while non-material asymmetries have an effect, but play a secondary role.

Combining agility (A) with material capabilities (C) by adding the two equations and the effect of their interaction (C+A+CA), creates the pattern demonstrated in the following graph, which takes the general form Threat (T) = $-aX^3 - bX$. It implies that a Great Power would face the greatest threat from a powerful state adversary, but that a network is more threatening than a small state, even though the latter possesses greater resources. Applying this to 21st century asymmetric conflicts, al Qaeda has developed a strategy that takes advantage of the agility associated with a networked form of organization, which, when fighting an opponent with significantly greater resources such as the United States, is superior to a bureaucracy like that of the Iraqi military under Saddam Hussein.

Resources and Threat



As the graph demonstrates, resources remain the primary determinant of which actors could threaten a Great Power. However, after material power falls below a certain threshold, it corresponds with an increasing agility advantage from proprietary information and decreased responsibility. This creates a hump in the tail of the curve, in which small state armies, like Iraq's in 2003, are less capable of threatening powerful states or the globalizing international order than non-state networks like al

Qaeda. With large economies, militaries, and stockpiles of nuclear weapons, states like Russia and China remain highly relevant actors in the global arena. However, with its ability to exploit non-material asymmetries, al Qaeda presents a greater challenge for the United States than the Iraqi army, despite less material power.

Conclusion

Strategies based in terrorism frequently fail to achieve perpetrators' ambitious long-term goals, and their success should not be exaggerated.[110] Surprise attacks and mass-murder of civilians may backfire by motivating opponents or alienating potential allies. However, whether hoping to eventually achieve relative symmetry, or coerce considerably more powerful opponents, networks have utilized terrorism, insurgency, and guerrilla warfare to threaten state security, resist power projection, disrupt efforts to impose order, and influence political decision-making. When facing massive material power disadvantages, weak actors have little choice but to utilize political strategies based on the interplay of violence and communication. To pursue their goals against stronger opponents, non-state networks must exploit non-material asymmetries of interest, expectations, organization, responsibility, and information.

[110] See Abrahms, "Why Terrorism Does Not Work."

Chapter 2: Testing and Applying the Theory

The central insight of the general theory of asymmetric warfare laid out in the previous chapter is that strong actors face a greater challenge from relatively weak actors organized as networks than from those organized as bureaucratic states. This is a testable proposition, one that has not been examined by previous international relations studies. Utilizing data on strong actor fatalities, conflict duration, and conflict outcome, I find strong support for the claim that powerful states have an easier time achieving their goals in conflicts against relatively weak states than against non-state networks. The results imply that the United States and other powerful countries should focus technological and strategic development more on improving their capabilities against networks than against smaller states.

While every asymmetric conflict is subject to the basic dynamics of material disparity, all wars between states and networks are not identical. The proximity of the conflict to the strong actor's main territory affects the strategic options available to both sides. In Localized Insurgencies, such as the United States-led occupation of Iraq, the conflict takes place far from the strong actor, enabling weak actors to design strategies aimed at convincing the strong actor to withdraw. However, in Irredentist conflicts, such as that between Israel and various Palestinian resistance groups, the strong and weak actors are close together, increasing the ability of the weak actor to threaten the strong actor's civilians and decreasing or eliminating the possibility that the strong actor will withdraw. Therefore, strong actor resolve is higher in irredentist conflicts, and the weak actor’s strategy focuses more on improving its negotiating position and winning concessions than compelling withdrawal. Testing these propositions, I find that irredentist conflicts, on average, feature significantly higher strong actor civilian fatalities and are significantly less likely to end with strong actor success than are localized insurgencies.

Additionally, prominent studies of asymmetric conflict have noted a trend towards greater weak actor success beginning in the early 20th century, attributing this pattern to the spread of a particularly successful weak actor strategy[111] or strong actors' increasing reliance on mechanized weaponry.[112] I offer an alternative explanation based on networks' ability to take advantage of geopolitical and technological transitions. To test this, I divide the sample of asymmetric conflicts into two time periods: post-WWII through the end of the Cold War and post-Cold War. Besides marking a major geopolitical transition, the latter coincides with the spread of the internet and other information technology, which enhanced networks' information acquisition, recruiting, and communication capabilities. I find that the split between small states and networks becomes more dramatic after the end of the Cold War, with powerful states succeeding more often and suffering fewer fatalities when fighting weaker states, and succeeding less often and enduring more fatalities in conflicts against networks, lending support to the argument that particular features of the information age help explain networks' relatively greater success against great powers.

Big States vs. Small States and Big States vs. Networks: Hypotheses

This section briefly introduces the main hypotheses tested in this chapter. To examine the performance of powerful states in conflicts against weaker states and networks, I utilize measures of civilian fatalities, military fatalities, conflict duration, and conflict outcome. Many studies focus on only one of these measurements, usually outcome. However, by looking at fatalities and duration in addition to outcome, the hypotheses below provide a more comprehensive examination of the

[111] Arreguin-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict.*

[112] Lyall and Wilson, “Rage Against the Machines: Explaining Outcomes in Counterinsurgency Wars.”

differences between big state-small state and big state-network conflicts, and which type of opponent is more capable against powerful countries.

Opponents that cause more civilian fatalities are more **threatening**. One of the primary responsibilities of any state is to provide civilians with security from foreign attack. While governments utilize various degrees of forceful coercion against their own citizens, any that cannot protect their citizens from foreign attack risk losing power due to popular rejection. In particular, citizens of great powers expect their government to protect them from attacks by relatively weaker actors. Therefore, I hypothesize that, compared to small states, networks tend to cause more big state civilian fatalities.

Hypothesis 1 (threat): Networks cause more civilian fatalities than small states.

Opponents that cause more military fatalities make wars more **costly**. As discussed in the previous chapter, due to the asymmetry of expectations, the ratio of casualties is not especially important in asymmetric warfare. Weak actors expect to suffer many casualties when fighting stronger opponents, while strong actor military fatalities can create political costs that weaken resolve. In wars in which the great power's survival is not at stake, those with high costs can lead domestic actors to question the conflict and advocate shifting resources to other priorities. Therefore, I hypothesize that, compared to small states, networks tend to cause more big state military fatalities.

Hypothesis 2 (cost): Networks cause more military fatalities than small states.

Opponents that prolong conflicts and prevent great powers from achieving their goals are more **challenging**. Big states fighting small states or networks expect to translate their resource advantage into rapid success. Prolonging the confrontation enables weaker actors to impose costs upon their stronger opponents which can lead to war weariness and a decision to abandon the conflict. Even if they are unable to kill many strong actor soldiers, weak actors impose financial and political costs merely by avoiding defeat and extending the resources, time and effort a big state spends in pursuit of its goals. Therefore, I hypothesize that conflicts between big states and networks tend to last longer than conflicts between big states and small states. Additionally, I hypothesize that strong actors will achieve their goals more often against small states than against networks.

Hypothesis 3A (challenge): Conflicts against networks last longer than conflicts against small states.
Hypothesis 3B (challenge): Conflicts against networks end in success less often than conflicts against small states.

Data and Research Design

To test the hypotheses described above relating to the claim that networks are better than small states at fighting great powers, I constructed an original data set of every conflict involving a nuclear-weapons state. Each opponent state is categorized as either another nuclear weapons state (big state), a non-nuclear weapons state (small state), or a non-state actor. Deliverable nuclear weapons provide a qualitative military advantage over any non-nuclear opponent, and a powerful deterrent that influences any opponent's strategic considerations. Additionally, based on 2013 figures, nuclear weapons states have the world's largest military budgets (based on total dollars, not percentage of GDP), with the US, China, Russia, and the UK making up the top four, France following at number six, and India at number eight (Japan is fifth and Saudi Arabia seventh).[113] Nuclear weapons are therefore a simple way

[113] “SIPRI military expenditure database.”

to separate big states from small states, and isolate which actors are most threatening to the United States and other powerful countries.

The data set features every post-WWII conflict involving a nuclear weapons state listed in the UCDP database, a standard resource for international relations research that includes every conflict with at least 25 battle deaths, as well as those listed in the 2008 edition of *Warfare and Armed Conflicts: A Statistical Encyclopedia of Casualty and Other Figures,* which includes conflicts with fewer than 25 battle deaths. The data set therefore includes every conflict that began after a state's first nuclear weapons test, along with any that were in progress at the time of the test, but did not conclude until after. Israel is an exception, as the country did not conduct an official test and maintains a policy of "nuclear ambiguity," but is widely believed to possess over 100 nuclear weapons. For Israel, I used January 1967 as the starting point based on a CIA assessment from early 1967 that Israel had produced bomb components and enough enriched fissile material to construct a couple of warheads.[114] These inclusion criteria resulted in a data set of 105 armed conflict dyads in which at least one side was a nuclear weapons state.

However, while India, Pakistan, and North Korea have all tested nuclear weapons, they are not included in the analysis for various reasons. First, North Korea has not demonstrated an ability to deliver a nuclear warhead over distance, and therefore does not fit the definition of a nuclear weapons state articulated above. India possesses deliverable nuclear weapons, and, since its first test in 1974 has engaged in two wars and some smaller skirmishes with a small state (pre-nuclear Pakistan), one conflict with a big state (nuclear Pakistan) and at least 26 conflicts with non-state networks, many of them domestic. Unfortunately, acquiring accurate data on Indian civilian and military casualties in these asymmetric conflicts proved especially difficult. Anecdotally, India's numerous lost-lasting conflicts with non-state actors, including insurgents in Kashmir, and relatively quick wars with

[114] Cohen, *Israel and the Bomb*, p. 298.

Pakistan, which either ended with an Indian victory or a ceasefire upholding the pre-war status quo, appear to support the claim that networks are more threatening and challenging to great powers than small states. However, without sufficient fatality data, I could not incorporate India into the quantitative study. Similarly, Pakistan fought one war against a big state since its first nuclear test in 1999, the Kargil War against nuclear India, and at least four against non-state networks, including insurgent groups in the Federally Administered Tribal Areas near the Afghan border. With no wars against a small state since becoming a nuclear power, Pakistan's experience also supports the claim that networks pose a greater threat than small states. However, without detailed fatality figures I could not include Pakistan in the data analysis below. These exclusions resulted in a dataset with 88 conflict observations used in the empirical analysis (see the appendix for a complete list).

The first thing that jumps out from a glance at this data is that only two of the conflicts are between nuclear weapons states. A border clash between the USSR and China in 1969 and the Kargil War between India and Pakistan in 1999 are the only times since World War II that the military forces of one nuclear weapons state have killed the soldiers or civilians of another. Furthermore, these big state-big state conflicts were limited and relatively quick. The Sino-Soviet border clash lasted only nine months and resulted in zero civilian deaths. Russia suffered only 58 military fatalities while killing approximately 600 Chinese soldiers. Similarly, the Kargil War was more limited than conflicts between India and Pakistan before Pakistan's first nuclear weapons test in May 1998. It lasted less than three months and caused considerably fewer deaths on both sides than the wars in 1965 and 1971, ending with a return to the pre-war status quo.

This provides strong support for the claim that powerful states in the post-World War II period have mostly checked each other. Despite this apparent success of mutually assured destruction, perhaps supplemented by economic interdependence and participation in international institutions, I do not argue that great powers are less threatening or pose less of a challenge to each other than non-state networks. As demonstrated by the final graph in chapter one portraying the relationship between resources and threat, great powers are capable of symmetric war against each other. Nuclear capabilities give them greater ability to threaten other powerful states and, coupled with large conventional military budgets, greater ability to deny other great powers success in the event of armed confrontation. Nevertheless, in 103 out of 105 conflicts involving a nuclear state, the other side has been a non-nuclear state or a non-state actor, which demonstrates the prominence of these types of conflict pairs in the post-WWII environment. Therefore, the data analysis presented below excludes the two conflicts between nuclear states, instead focusing on conflicts that involve nuclear states fighting small states or non-state networks.

Dependent Variables

The proposition that nuclear powers pose the greatest potential threat to each other is hardly novel; less intuitive is the claim that networks are more dangerous than non-nuclear states. To test this theory, I collected data on civilian and military fatalities, conflict duration, and conflict outcome and used these figures to evaluate a series of hypotheses comparing networks' and small states' ability to threaten, impose costs, and challenge nuclear weapons states. Since this project focuses on the security challenges for great powers, each of these dependent variables is measured from the perspective of the big state.

First, I collected information on civilian and military fatalities suffered by the nuclear state in each conflict. Using fatality data is uncommon in international relations research and, to the best of my knowledge, unprecedented in studies of asymmetric warfare. Most conflict studies, especially of asymmetric warfare, focus on war outcomes, while some consider conflict duration. These variables capture important aspects of warfare, but miss the costs combatants pay on their way to victory or defeat. An exception is a study by Valentino, Huth and Croco, who argue that democratic accountability leads democracies to suffer fewer military and civilian fatalities in interstate wars than non-democracies.[115] Given the prominent role imposing costs on stronger opponents plays in weak actor strategy, analyzing fatality data in addition to duration and outcome is especially appropriate for studying asymmetric conflict.

Existing data sources either pool the war-time fatalities of all sides of a conflict into a single measure, regardless of which side they are suffered by (e.g. UCDP dataset, Correlates of War dataset), or provide actor-specific fatality data but limit the scope of their coverage to only large-scale (greater than 1000 battle deaths) conflicts (e.g. Valentino, Huth and Croco 2006). It was therefore necessary to supplement existing data using a variety of sources—including academic studies, official government statistics, and media reports. Using these sources, I gathered information on civilian and military fatalities suffered by the nuclear state in each conflict. The first two dependent variables used in the analyses presented below count the total number of (1) civilian and (2) military deaths suffered by the nuclear state in each conflict. The natural log of these values is used in the analysis to account for the highly skewed distribution of both variables. Civilian fatalities range, in the dataset, from a minimum of 0 to a maximum of 3,025 (the natural log ranges from 0 to 8.015). Military fatalities, on the other hand, display much greater variation, ranging from 0 to a maximum of 58,178 (the natural log ranges from 0 to 10.971).

To measure conflict duration I coded the beginning of each conflict as the month in which strong actor forces first entered a foreign country or when weak actors first attempted an attack on strong actor civilians or military forces, whichever came first. For the end of a conflict, I used the month in which the strong actor withdrew forces or otherwise abandoned its military effort, the strong actor comprehensively achieved its main goal, or the two combatants reached a peace agreement or ceasefire. For ongoing conflicts I used July 2013 as the end date for duration purposes. The war

[115] Valentino et. al., “Bear Any Burden?”

duration dependent variable is therefore a count of the number of months a conflict lasted. It ranges from 1 to 433, with a mean of 45 months.

This coding process is fairly straightforward for most cases, except some involving Israel. For the larger Israeli-Palestinian conflict, I coded any official agreement—such as the Oslo Accords, signed in September 1993—as the end of a conflict and the next instance of violence or the start of any codenamed Israeli military operation as the beginning of a new conflict. It is possible to consider the entire history between the Israelis and Palestinians after Israel occupied the West Bank and the Gaza Strip in 1967 as one ongoing conflict, but this does not allow for evaluation of Israel's goals in each of its military operations. Alternatively, one could treat the fight between Israel and each Palestinian group as a separate dyad (Israel-PLO, Israel-Hamas, Israel-Islamic Jihad, etc.), but this creates difficulties regarding fatality data. Sometimes a specific Palestinian group publicly claims an attack against Israelis and sometimes no one does. Even more problematic, when the Israeli Defense Forces conduct a ground operation in the Palestinian territories, it is almost impossible to determine which Palestinians fired the shots or set off the bombs that killed Israeli soldiers. Therefore, I treat all Palestinian militant groups as one resistance network that has fought multiple conflicts against Israel.

Finally, to measure conflict outcome, I considered the declared military and political goals of strong actor leaders at the beginning of the conflict and then determined whether these had been achieved on a three point scale: success (2), mixed outcome (1), and failure (0). To code an outcome as a success, the strong actor needed to clearly achieve its primary goal. For example, in the Gulf War in 1991, the American-led coalition succeeded in restoring Kuwaiti sovereignty by forcing Iraq to withdraw from Kuwait. To code an outcome as mixed, the strong actor needed to partially but not entirely achieve its main goal, or achieve some tactical military success while still falling short of its primary strategic goal. For example, in the Gaza War in December 2008 and January 2009, Israel aimed to stop rocket fire from Gaza into Israel by Hamas and other Palestinian groups and eliminate their ability to fire rockets in the future. The Israelis destroyed many rockets and launchers, killed numerous Palestinian militants, and secured a ceasefire declaration from Hamas. However, while rocket fire decreased significantly after the conflict it did not cease entirely, and Hamas remained in control of Gaza and continued to import rockets and rocket parts. Finally, to code an outcome as a failure, the strong actor needed to withdraw forces before achieving the military operations' aims or make significant political concessions that ran contrary to its leaders' stated goals. For example, in 1979, the Soviet Union sent forces to Afghanistan to support the government's efforts against various rebel groups, but withdrew in 1989 without defeating the Mujahideen insurgency or securing a friendly government's rule. Any conflicts that remain unresolved as of July 1, 2013, I coded as ongoing. Ongoing conflicts are included in the fatality and duration tests, but not in the outcome analysis.

This coding scheme places the burden of success on the strong actor. Given big states' resource advantage, realist theory indicates that they should achieve their goals against small states or networks, so it is noteworthy when they do not. By contrast, many recent studies consider asymmetric conflict from the weak actors' perspective. In “Why Terrorism Does Not Work,” Max Abrahms argues that terrorism is an “ineffective means of coercion” because terrorist groups typically fail to achieve their often maximalist policy objectives.[116] Similarly, in “Assessing the Dangers of Illicit Networks,” Mette Eilstrup-Sangiovanni and Calvert Jones argue that “the prevailing pessimism about the ability of states to combat illicit networks is premature,” because networks inherently have difficulty sustaining large coordinated actions.[117] These studies convincingly dispute hyperbolic fears that terrorist networks pose an existential threat to powerful states and that insurgent networks present an insurmountable challenge. However, by taking the weak actors' perspective and considering only whether networks

[116] Abrahms, “Why Terrorism Does Not Work,” p. 51.
[117] Eilstrup-Sangiovanni and Jones, “Assessing the Dangers of Illicit Networks,” p. 8.

achieve their goals, they do not address the question of which type of opponents are relatively more capable of threatening and challenging great powers.

In the main empirical analysis presented below, the three-category outcome scale is used. The strong actor is coded as failing to achieve its aims in 16 cases (20%), as achieving a mixed outcome in 23 cases (28.75%), and as succeeding in 41 cases (51.25%). In the secondary analysis, which focuses on the effects of localized insurgencies versus irredentist conflicts in the subset of big state wars against networks, this three-category DV is collapsed into a dummy variable coded 1 if the strong actor achieves success, and zero otherwise (mixed or failure). This is done because the small sample size (N=47) prevents a multivariate analysis of a three-outcome dependent variable using multinomial logit. The two-category war outcomes variable is coded 0 (unsuccessful) in 39 cases (48.75%) and is coded 1 (success) in 41 cases (51.25%).

Key Independent Variable

The key explanatory variable in the main analysis below is the nuclear state's **Opponent Type**. The theoretical argument developed in the previous chapter, and the hypotheses laid out above, suggest that networks pose a greater threat to nuclear states than small states do, that big-states' wars against networks are more costly than those fought against small states, and that networks pose a bigger challenge to big states than small states do. The important variation in each of these relationships is the type of opponent the nuclear state faces (i.e. small state or network), and this is the key independent variable in the analysis presented below. To measure Opponent Type, I code each opponent of a big state as either a small state (coded 1) or a network (coded 2). Thirty-three cases (37.5%) involve a small state, while 55 conflicts (62.5%) are against a network.

To be coded as a small state, an actor must exercise sovereignty over a given area, openly operate out of official government buildings, control borders, and be recognized by the international community. All other actors are coded as networks. Many non-state networks exhibit some of the qualities of states, such as controlling territory, providing social services, or participating in government. For example, the Irish Republican Army was linked to a political party, Sinn Fein, representatives of which have held elective office in Northern Ireland. Hezbollah controls a section of southern Lebanon where it provides social services, and its political wing holds seats in the Parliament of Lebanon. Hamas' political wing won a majority in Palestinian legislative elections in 2006, and forcibly took control of the Gaza Strip after the Palestinian National Authority and its foreign allies rejected the election's outcome. However, while these organizations and others like them exhibit some qualities of states, none are sovereign or recognized as states internationally, and are therefore coded as networks.

Control Variables

The empirical analysis includes several control variables, which are expected to influence fatalities, conflict duration, and war outcomes. First, I control for the presence of military support for the opponent from a nuclear power. This control accounts for the possibility that, as Jeffrey Record argues, examples of weak actor success may be driven by external assistance.[118] If a small state or network utilizes a big state's resources, then the conflict features a smaller resource gap than other asymmetric wars, and the outcome may depend more on material assistance than on the weak actors' organizational type. Of the 88 big state-small state and big state-network conflicts in the data set, this check applies to four: pre-nuclear China and North Korea in the Korean War (6/1949 – 7/1953) received assistance from the Soviet Union when fighting the United States, North Vietnam in the Vietnam War (7/1959 – 5/1973) received assistance from China and the Soviet Union when fighting the United States, the Dhofar Rebellion in Oman (7/1972 – 3/1976) received assistance from China

[118] Record, *Beating Goliath*.

when fighting the United Kingdom, and the Afghan Mujahideen (6/1979 – 2/1989) received assistance from the United States when fighting the Soviet Union.

Additionally, I include standard control variables that have been shown to influence the outcome of conflict, including the nuclear state's level of democracy and military capabilities. For democracy, I use the Polity IV scale, coding any country with a score of seven or higher as a democracy; and for military capabilities, I use the CINC score from the Correlates of War project. Finally, in each of the four models (civilian casualties, military casualties, conflict duration, conflict outcome) I control for the other three factors to isolate the effect of each dependent variable (e.g. when conducting the civilian casualties test I control for military casualties, duration, and outcome).

Results

It is useful to first examine the distribution of the data and the bivariate relationships between Opponent Type and each of the dependent variables. Figures 1 through 4 below present the average civilian and military fatalities, war duration, and war outcome across the different opponent types, and provide preliminary support for the hypothesized relationships.

First, the left-hand side of Figure 1 presents the average civilian fatalities for conflicts against small states versus networks, while the right-hand side of Figure 1 presents the same relationship, but excludes conflicts in which the opponent receives military support from a nuclear state. The relationship depicted in Figure 1 provides strong preliminary support for the proposition that networks are more threatening than small states. Few small states have managed to kill big state civilians, and those who have did not kill many. By contrast, networks killed an average of 39.1 times more strong actor civilians per conflict. The data may even under-represent the relatively higher threat from networks, as the data set includes every civilian of a nuclear state killed by a non-nuclear state's forces, but does not include isolated terrorist attacks from networks that were not listed in the UCDP database or the *Warfare and Armed Conflict* encyclopedia, such as the four coordinated bombs against the London transportation system on July 7, 2005 that killed 52. The relationship remains largely the same, and supportive of the hypothesized relationship, after removing the four cases in which the weak actor received big state assistance.

Figure 1: Civilian Fatalities by Opponent Type

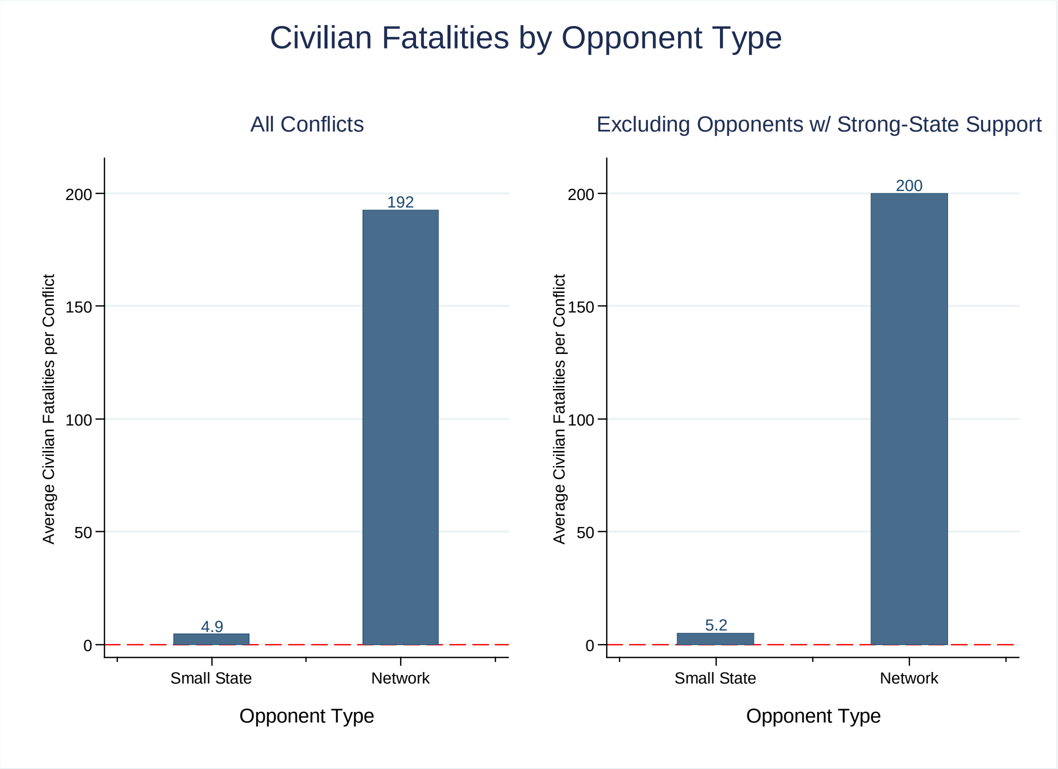


Figure 2 presents the bivariate relationship between Opponent Type and military fatalities. Interestingly, small state opponents caused, on average, more than three times as many military fatalities as networks (left-hand side of Figure 2). However, this effect reverses when the conflicts in which the weak actor received big state assistance are excluded, largely because American military fatalities in the Korean and Vietnam wars dwarf all other conflicts in the database. The United States lost 36,516 in Korea and 58,178 in Vietnam, while the total number of military deaths caused by small states in all other conflicts combined is only 16,109. This suggests that big state assistance greatly enhances small states' ability to impose costs on strong actor militaries. Meanwhile, military fatalities in the set of big state-network conflicts are more balanced. The Soviet Union lost 13,310 military personnel in Afghanistan, which is second most after France's 17,456 in Algeria. This indicates that, while external assistance helps small states kill big state soldiers, networks are more capable of imposing military costs without assistance. After accounting for strong-state support, this bivariate relationship provides preliminary support for the relationship between opponent type and military fatalities hypothesized above.

Figure 2: Military Fatalities by Opponent Type

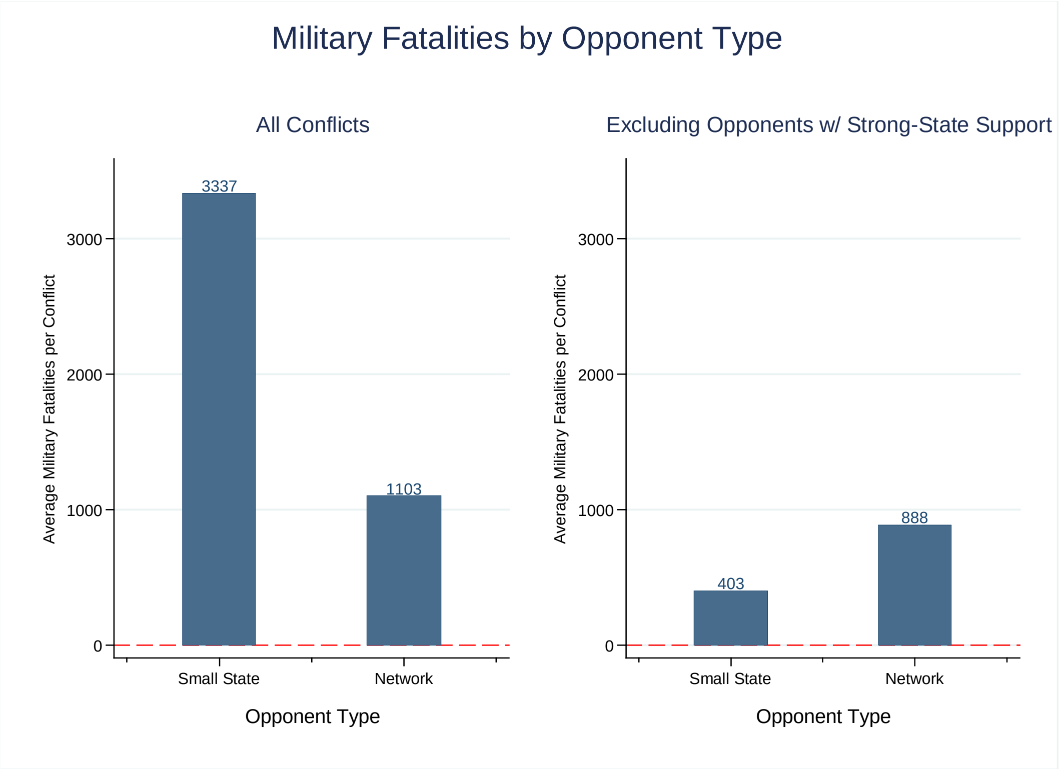
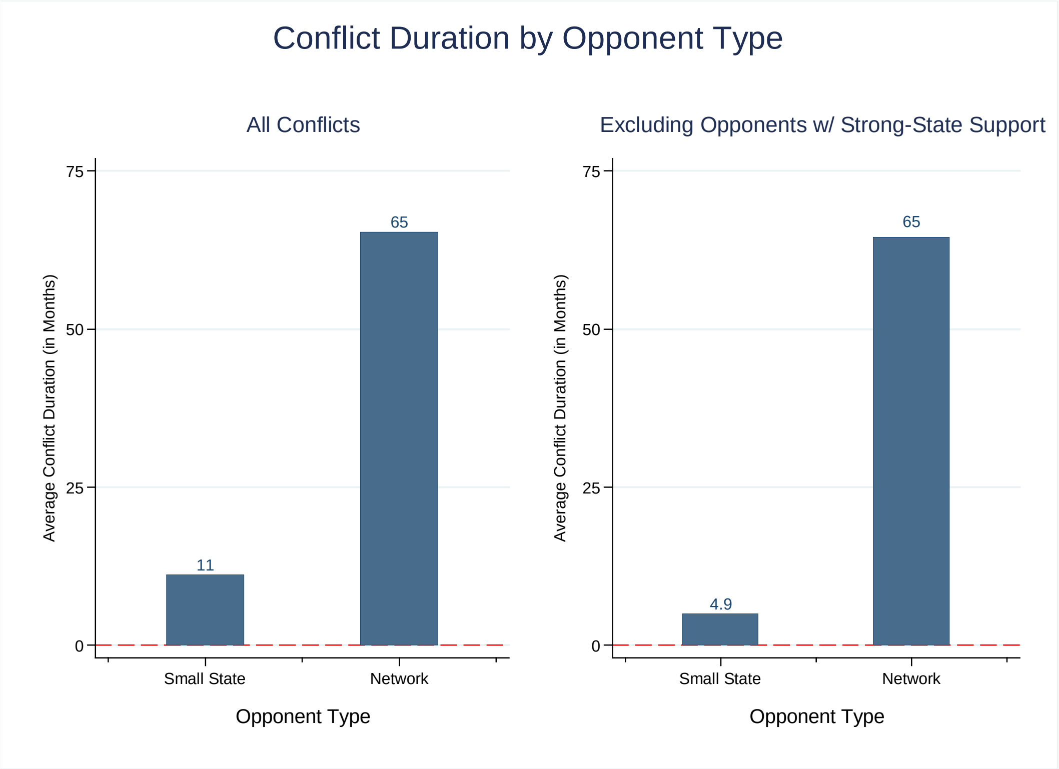


Figure 3 presents the bivariate relationship between average conflict duration and Opponent Type. Again the left-hand side of Figure 3 presents this relationship for all conflicts, while the right-hand side of Figure 3 excludes conflicts in which the opponent receives big-state support. The relationships depicted in Figure 3 once again provide strong preliminary support for the hypothesis that big states find networks more challenging than small states. Conflicts against networks last, on average, almost six times as long as conflicts against small states, a gap of four and a half years. The results are even more dramatic when excluding weak actors with strong state support. Korea and Vietnam respectively lasted 49 months and 166 months, which is considerably longer than the average conflict against a small state. Removing those two cases drops the average duration to under 5 months. The Soviet war in Afghanistan lasted 116 months, while the UK fought the Dhofar Rebellion in Oman for 44 months. The two lasted an average of 80 months, but other big state-network conflicts were sufficiently long that eliminating these two decreases the average by less than a single month.

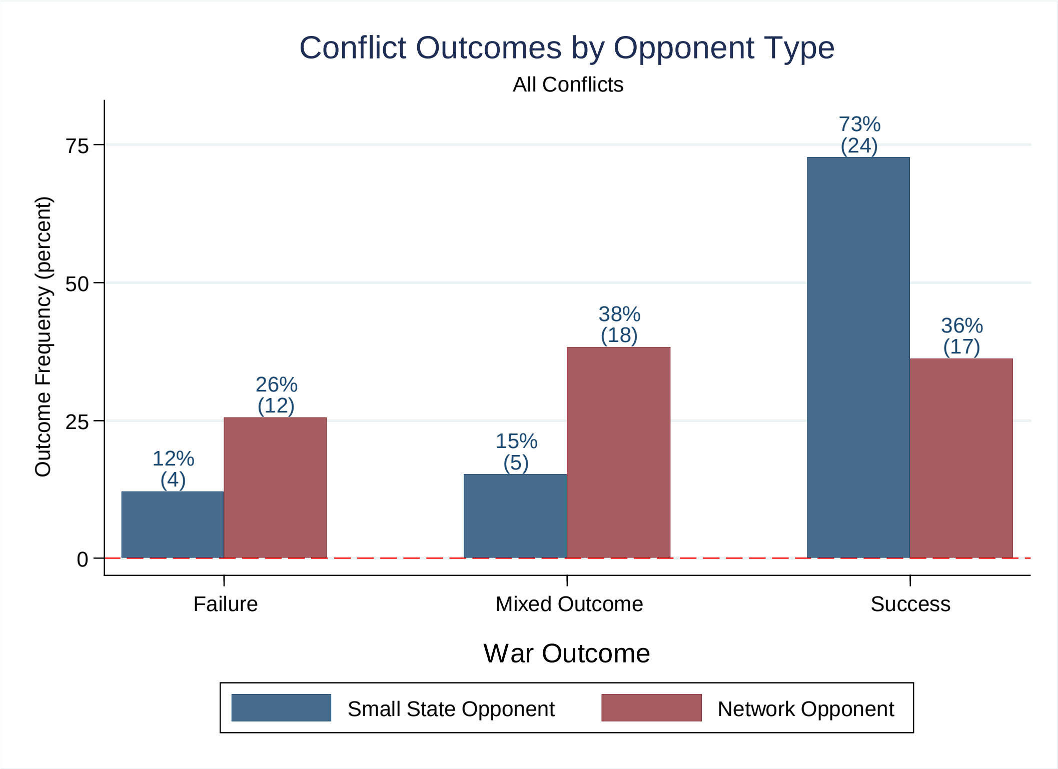
Figure 3: Conflict Duration by Opponent Type



The data on outcomes also provide preliminary support for the theory that networks are more challenging opponents for big states than small states are. Figure 4 presents the distribution of conflict outcomes for small states versus networks across all conflicts in the data set.[119] Strong actors were able to achieve their goals in 73% of conflicts against a small state, while only 12% ended in failure. By contrast, only 36% of conflicts against networks ended with success, while 26% ended in failure.

[119] The distribution excluding cases with strong state assistance is nearly identical to that presented in Figure 4, and is therefore not presented here.

Figure 4: Conflict Outcomes by Opponent Type



Multivariate Analysis

While these bivariate relationships provide relatively strong initial support for the hypotheses enumerated at the start of this chapter, further empirical tests are necessary to ensure that these relationships are statistically significant and robust to inclusion of a variety of control variables. This section presents the results of Ordinary Least Squares (OLS) regression analyses on civilian fatalities, military fatalities, and war duration, and Multinomial Logistic regression analysis on war outcomes.

Table 1 presents the results of OLS regression analyses run on the natural log of civilian casualties (model 1), the natural log of military casualties (model 2), and war duration (model 3). The key independent variable, Opponent Type, is positive and significant in all three models, indicating that big states suffer significantly higher civilian casualties and significantly higher military casualties when they fight network opponents versus small state opponents. Further, big states fight significantly longer wars when their opponents are networks rather than small states.

Table 1: OLS Results for Casualties and War Duration

	Civilian Casualties (ln)	Military Casualties (ln)	War Duration
Opponent Type	2.342***	1.497**	53.58*
	(0.443)	(0.438)	(21.88)
Big State Support to Opponent	-1.467**	3.529	78.40*
	(0.386)	(1.936)	(35.56)
Cold War	0.473	0.915	-24.82
	(0.294)	(0.955)	(16.15)
Nuclear State Democracy	-0.364	-1.564**	20.57
	(0.500)	(0.442)	(18.01)
Nuclear State Military Capabilities	-4.374	2.260	15.87
	(2.403)	(4.518)	(67.32)
Conflict Duration	0.0121**	0.0115	----
	(0.00324)	(0.00622)	
Irredentist Conflict	1.635**	0.254	16.00
	(0.448)	(1.091)	(32.12)
Interstate Conflict	2.078***	1.833	4.954
	(0.443)	(0.952)	(26.52)
Constant	-3.774***	0.867	-57.34
	(0.663)	(1.831)	(51.10)
Observations	86	86	88
R-squared	0.41	0.28	0.20

Standard errors in parentheses, clustered on Nuclear State. *p<0.10, **p<0.05, ***p<0.01.

The results of the multinomial logit analysis of war outcomes, presented in Table 2, are similarly supportive of the relationship hypothesized above. The baseline category for comparison is big-state success in the conflict. The results in the first column demonstrate that when a big state faces a networked opponent rather than a small state, failure in the conflict is significantly more likely than success. Similarly, the second column shows that a mixed outcome is also significantly more likely than success in the conflict when the nuclear state faces a network rather than a small state opponent.

Table 2: Multinomial Logit Results for War Outcome

	Success vs. Failure	Success vs. Mixed
Opponent Type	1.249* (0.686)	1.106* (0.671)
Big State Support to Opponent	0.527 (1.689)	0.0851 (1.703)
Cold War	0.477 (0.689)	-0.220 (0.462)
Nuclear State Democracy	-0.630 (0.904)	0.922 (1.178)
Nuclear State Military Capabilities	3.155 (4.457)	-3.735 (7.034)
Conflict Duration	0.0139* (0.00787)	0.0176*** (0.00488)
Constant	-3.395** (1.553)	-3.337* (1.843)
Observations	80	80

Comparison outcome category is Success. Standard errors in parentheses, clustered on Nuclear State. *p<0.10, **p<0.05, ***p<0.01.

The substantive impact of Opponent Type on each of these dependent variables, furthermore, is large (see Table 3). Moving from a small state to a network opponent increases civilian casualties from a baseline expected value of just under 10 to a post-change value of nearly 56. This is an increase in the expected number of civilian deaths of nearly 46, or a 462% increase in the number of civilians killed. Military fatalities, furthermore, increase by an average of 120 deaths when moving from a small state opponent to a network, from a baseline expected value of 167 to a post-change value of 287 military deaths. This corresponds to a 72% increase in military deaths when a nuclear state faces a network opponent rather than a small state. The substantive impact on war duration is similarly large. The baseline expected duration when facing a small state opponent of just over 9 months increases by close to 55 months when the opponent is a network, producing a post-change expected duration of close to 64 months. This represents over a 600% increase in expected war duration when moving from a small state to a network opponent.

Table 3: Substantive Results, Impact of Opponent Type

	Small-State Opponent (Baseline Value/Probability)	**Network Opponent (Post-Change Value/Probability)**	**First Difference**	**Percentage Change**
DV: Civilian Fatalities	9.95	55.92	45.97 (21.68, 98.16)	462%
DV: Military Fatalities	167.08	287.46	120.38 (66.01, 209.66)	72.1%
DV: War Duration	9.04	63.74	54.70 (40.69, 68.83)	605%
DV: War Outcome				
Failure	13.78	24.37	10.59 (-8.72, 21.57)	76.85%
Mixed	15.48	39.29	23.81 (3.84, 46.58)	153.85%
Success	70.74	36.34	-34.40 (-55.90, -9.29)	-48.63%

Note: Substantive results calculated using Clarify, holding control variables at values predicting high threat/challenge. 95% confidence intervals surrounding first differences reported. Percentage change calculated by dividing the first difference by the baseline value/probability and multiplying by 100.

The substantive results for war outcomes are similarly supportive of the hypothesized relationship. The predicted probability of big state success in war drops from over 70 percent to just 36 percent when moving from a small state to a network opponent type. This is over a 34 percentage point, or 49%, reduction in the likelihood of success. Failure and mixed outcomes, on the other hand, are more likely when the opponent is a network. The likelihood of a mixed outcome increases from about 15% to over 39%, or a nearly 154% increase in the likelihood of this type of outcome. The probability of failure, similarly, increases when moving from a small state to a network opponent, increasing the probability of this outcome type by over 10 percentage points, or nearly 77%, though this first difference just misses statistical significance at the 0.05 level.

Overall, these four tests provide relatively strong support for the main insight outlined in chapter one. The final graph depicting the relationship between resources and threat with a hump in the tail presents a more accurate portrayal than the original realist graph depicting a smoothly declining relationship between resources and capabilities. Networks appear to be more capable of threatening and challenging great powers than small states, even though small states control more resources than non-state networks.

Secondary Analysis: Situational and Strategic Variation

All state-network conflicts are influenced by the dynamics inherent to asymmetric warfare, but not all asymmetric conflicts are the same. The degree of various non-material asymmetries, such as resolve and responsibility, is partially determined by the circumstances of the conflict. Strategy is a function of preferences and incentives—what do actors want and what external conditions must they consider in pursuit of these goals?—and the strategic dynamic of a given asymmetric conflict is affected by the aims of each combatant.

With this in mind, I divided the set of conflicts between a nuclear weapons state and a non-state network into three categories based on the weak actors' main goal and the geographic proximity of the weak actor to the strong actor's main territory. This influences the ease with which weak actors can threaten strong actor civilians and the resolve of strong actors to accomplish their goals or at least achieve a mixed outcome instead of failure. Accordingly, each category of conflict presents weak actors with a different set of available strategies. This leads to testable hypotheses that complement those presented above.

Localized Insurgency (Weak Actor Goal: Expel Distant Foreigners)

Strategies in these conflicts are shaped by the strong actor's option to withdraw forces from territory claimed by the weak actor without sacrificing a piece of its homeland or directly creating a neighboring threat. Therefore, the weak actor can compel strong actor withdrawal by raising the military, monetary, and political costs of the conflict beyond the strong actor's tolerable threshold, which will lead to its government choosing to allocate resources towards other priorities. This is the most commonly studied type of asymmetric conflict, usually under the category of guerrilla wars, insurgencies, or “small wars.”[120]

Localized insurgencies are fought at considerable distance from the strong actor's main territory, perhaps across a sea or ocean. Due to this distance, and the asymmetry of resources, it is difficult for the weak actor to threaten strong actor civilians or disrupt their normal lives, with the exception of strong actor settlers, tourists, or non-military officials that travel to the area where the weak actor operates. This type of conflict includes anti-colonial wars, such as the French in Algeria, and foreign occupations by distant powers, such as the United States in Iraq. In many cases, the strong actor works with and through local government allies to control the contested territory.

The modern version of weak actor strategy in localized insurgencies draws heavily from the writings of Mao Zedong. Mao honed his version of guerrilla insurgency in response to the Japanese

[120] See, for example, Merom, *How Democracies Lose Small Wars*.

invasion of China that began with the attack on Manchuria in 1931. He utilized a three-stage strategy designed to prolong the conflict and impose escalating costs upon the Japanese to convince the invading power to withdraw. Given Japan's resource advantage, the Chinese could not prevent Japanese forces from occupying China. In the first phase, “the enemy's strategic offensive and our strategic defensive,” Mao recommended retreat deeper into China, extending Japan's forces and forcing the Japanese to spend money on the conflict. Meanwhile, Chinese fighters would stage hit-and-run raids and harass supply lines to impose costs on Japan. This would slow, but not stop, the progress of the invasion, frustrating Japanese soldiers in China and creating doubt among Japanese citizens and government officials in Japan.[121]

Mao called the second stage “strategic stalemate,” or “the period of the enemy's strategic consolidation and our preparation for the counter-offensive.” Having conquered a large amount of territory and stretched its forces, Japan had to “safeguard these areas and to make them his own by the fraudulent method of setting up puppet governments.” By surprising Japanese forces throughout occupied China with attacks behind enemy lines from guerrillas that had blended in with the civilian population, Mao's forces continued imposing costs and creating doubt among the Japanese. This also forced Japan to turn its efforts towards consolidation, allowing the Chinese to establish bases, recruit, and acquire weaponry, preparing for the third and final stage.[122]

In the third stage, Chinese forces went on the offensive, utilizing the capabilities developed during the second stage to retake territory Japan had captured.[123] Mao referred to this as an acceleration to “mobile war,” in which the guerrilla units “gradually transform themselves into regular forces.”[124] This three-stage strategy thus moved from asymmetric to symmetric warfare. Chinese

[121] Mao, “On Protracted War,” no. 36.
[122] Mao, “On Protracted War,” no. 37.
[123] Mao, “On Protracted War,” no. 38.
[124] Mao, “Problems of Strategy in Guerrilla War,” Chapter VIII, p. 181.

forces began by prolonging the conflict and imposing costs upon Japan in the first stage, acquired additional resources while eroding Japan's capabilities in the second stage, and then, in the third stage, engaged the Japanese in pitched battles while openly defending re-conquered positions. However, Japan's final defeat in China was part of the allied victory in the Pacific theater of World War II, which makes it virtually impossible to evaluate if Mao's strategy would have successfully compelled Japanese withdrawal on its own.

Nevertheless, the intermediate successes of the three-stage approach led subsequent weak actors to emulate and adapt Mao's strategy. For example, Vietnamese general Vo Nguyen Giap advocated a strategy of protracted war, first against France and then when fighting the United States.[125] The Viet Minh's effort to expel France began with isolated guerrilla attacks and advanced to mobile war, "annihilating" French forces in a conventional siege of Dien Bien Phu in 1954.[126] Similarly, North Vietnam and the Vietcong's strategy in pursuit of American withdrawal began with strategic retreat, followed by consolidation and cost imposition, and ended with a more symmetric conflict, in which a "final North Vietnamese blitzkrieg" consisting of infantry and armored units captured Saigon in 1975 as the last American forces left the country.[127]

Che Guevara adapted Mao's three-stage strategy to a domestic revolution. Che and Fidel Castro's takeover of Cuba began with a small guerrilla band conducting raids from mountainous jungles, then grew by gathering equipment and recruits while imposing costs on the forces of the Batista government, and completed with more symmetric battles.[128] Abdel Aziz al Muqrin, the late leader of al Qaeda in the Arabian Peninsula, proposed a similar three-stage guerrilla revolution against Saudi Arabia, Yemen and other Middle Eastern governments, but with a more urban focus. Unlike

[125] Giap, *People's War, People's Army*.
[126] Giap, p. 25.
[127] Summers, *On Strategy*, xiii.
[128] Guevara, *Guerrilla Warfare*.

many previous insurgency manuals, al Muqrin's explicitly advocates assassination, terrorism, and hostage-taking to impose costs on stronger opponents during the earlier stages of the conflict.[129] Che recommended against these techniques for fear of alienating the civilian population, but, in contrast to communist strategists like Mao, Giap and Che, al Muqrin argued that religious ties, demonstrations of dedication, and tactical successes would garner enough popular support for the insurgency to succeed.[130]

Many relatively weak actors fighting in localized insurgencies do not have the population of China to draw upon and face enemies with considerably more resources than the Cuban government, and therefore cannot close the resource gap enough to attempt Mao's third stage. For example, the Afghan Mujahideen utilized a compellence strategy throughout their conflict against the Soviet Union, denying the USSR victory and imposing costs until Soviet forces withdrew. Twenty-first century Afghan insurgents, some of whom fought against the Soviet Union, cannot hope to achieve material symmetry with the United States-led International Security Force, and therefore aim to emulate their predecessors by prolonging the conflict until the foreign forces leave rather than forcing a withdrawal with symmetric battles. For non-state networks resisting occupation by a distant nuclear weapons state, this strategy of extending the conflict while killing or injuring strong actor soldiers is often the best available means of imposing costs upon occupying powers and preventing them from achieving their goals.

Irredentist: (Weak Actor Goal: Gain Control of Homeland from Local Power)

Unlike the previous category, strong actors in irredentist conflicts do not have the option of complete withdrawal. In irredentist conflicts, weak actors seek to control part of the strong actor's

[129] Al-Muqrin, 'Abd Al-'Aziz, *A Practical Course for Guerrilla War.*

[130] Al-Muqrin, 'Abd Al-'Aziz, *A Practical Course for Guerrilla War*, chapter 2 “The Basic Preconditions for Conducting a Successful Guerrilla War.”

main territory, or an area adjacent to the strong actor's mainland. If successful, this could weaken the strong actor by requiring it to relinquish strategic or economically valuable territory, such as a port, a defensible border, or natural resources, and might presage further conflict by creating a potentially hostile neighboring state. The costs of failure for strong actors are greater in irredentist conflicts than in localized insurgencies, which means it is less likely that weak actors can simply impose costs until the strong actor decides to leave. Therefore, weak actor strategy often seeks to push the strong actor to a desirable negotiation point, as opposed to coercing a unilateral withdrawal.

However, few weak actors in irredentist conflicts fight for the ultimate goal of increased political representation, semi-autonomy, reduced restrictions on movement, the release of prisoners, or any other mixed outcome that results from direct negotiations or indirect bargaining with their stronger opponent. Like networks fighting localized insurgencies against foreign occupiers, weak actors in irredentist conflicts typically embrace maximalist goals. The IRA sought to liberate Northern Ireland from Great Britain; Chechen rebels seek independence from the Russian Federation; and various Palestinian groups seek an independent state in the West Bank and Gaza, with some ultimately hoping to eliminate Israel. Given the proximity of their opponent, these ambitious aims often remain unrealized. Therefore, weak actors in irredentist conflicts end up pursuing more intermediate goals, utilizing violence to improve their negotiating position and extract concessions from their stronger opponents, perhaps with the intention of resuming the struggle in pursuit of their maximalist goals if they remain unsatisfied.

The proximity of weak actors to the strong actor's territory in irredentist conflicts increases weak actors' ability to threaten the strong actor's civilians. While localized insurgents would have to travel considerable distances to launch an attack on the strong actor's homeland, weak actors in irredentist conflicts can stage cross-border raids, fire projectiles over borders, or infiltrate the strong actor's territory to attempt a terrorist attack. This heightened threat to strong actor civilians could make big states more willing to make concessions, increase their resolve, or both, leading to more mixed outcomes and fewer successes. I therefore hypothesize that irredentist conflicts will, on average, feature more big state civilian fatalities, last longer, and end in strong actor success less often than localized insurgencies.

Global Insurgency (Weak Actor Goal: General Opposition to the International Order)

In this category, a transnational movement attempts to overthrow or disrupt the general international order. This is the most expansive of goals, and virtually impossible for the weak actor to win conclusively. Compared to the other two categories, global insurgencies are more dispersed and driven more by ideology than territorial claims.

With little direct precedent, both weak and strong actor strategy for global insurgency draw upon the lessons of localized insurgency and irredentist conflict and adapt them to a larger situation. Al Qaeda, for example, seeks American withdrawal from distant territory, such as the Arabian Peninsula and Afghanistan, which resembles localized insurgencies. Additionally, al Qaeda and allied local forces aim to control territory in countries such as Pakistan and Saudi Arabia, which resembles irredentist conflicts.

Global insurgency therefore manifests itself as a series of localized insurgencies and irredentist conflicts mixed with the threat of terrorism in the strongest enemy states. It features the common strategic elements of more localized conflicts as well as elements unique to its transnational nature. While numerous non-state networks are transnational, operating in more than one country, there is only one case of global insurgency: al Qaeda and the international jihadist movement. For this reason, every hypothesis in this section considers the differences between the 27 cases of localized insurgencies and 28 irredentist conflicts in the data set. Al Qaeda's global insurgency is the focus of the next chapter.

Hypotheses

Based upon the above discussion of the differences between localized insurgencies and irredentist conflicts among the set of big state-network conflicts, I hypothesize the following:

Hypothesis 4A (threat): Irredentist conflicts cause more strong actor civilian fatalities than localized insurgencies.

Hypothesis 4B (resolve): Irredentist conflicts tend to last longer than localized insurgencies.

Hypothesis 4C (challenge): Irredentist conflicts end with strong actor success less frequently than localized insurgencies.

Key Independent Variable

In this secondary analysis, which focuses on the effects of conflict type (localized insurgency versus irredentist) among conflicts against networks, the key independent variable is a dummy variable identifying the type of conflict. This variable is coded 1 if the nuclear state is fighting a localized insurgency, and is coded 2 if the nuclear states is fighting a network opponent in an irredentist conflict.

Results

An initial analysis of the bivariate relationships between conflict type (i.e. localized versus irredentist) and civilian fatalities, war duration, and outcome provides preliminary support for hypotheses 4A, 4B, and 4C. First, Figure 5 presents the bivariate relationship between conflict type and civilian casualties. As Figure 5 shows, weak actors in irredentist conflicts, on average, kill more civilians than those in localized insurgencies. This result is not especially surprising, since irredentist conflicts, by definition, take place closer to strong actors' civilians than localized insurgencies.

Nevertheless, it demonstrates that strong actors face a greater threat to their civilians in irredentist conflicts, which both shapes weak actor strategy and could also increase strong actor resolve.

Figure 5: Civilian Fatalities in Wars against Networks

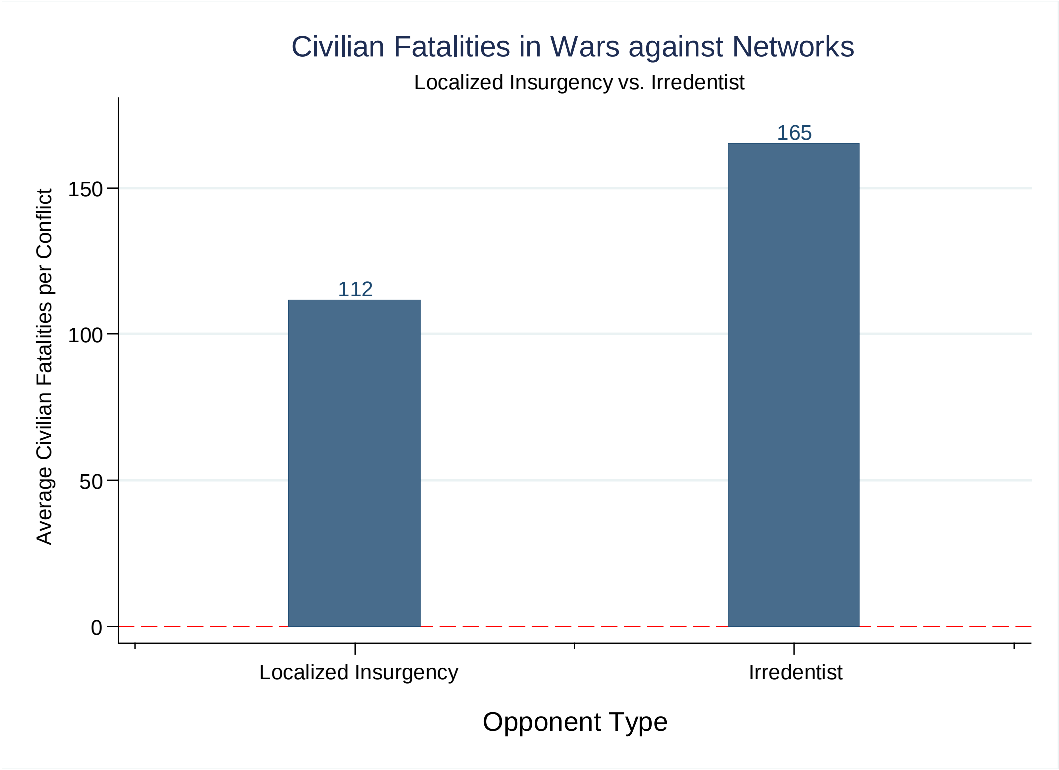
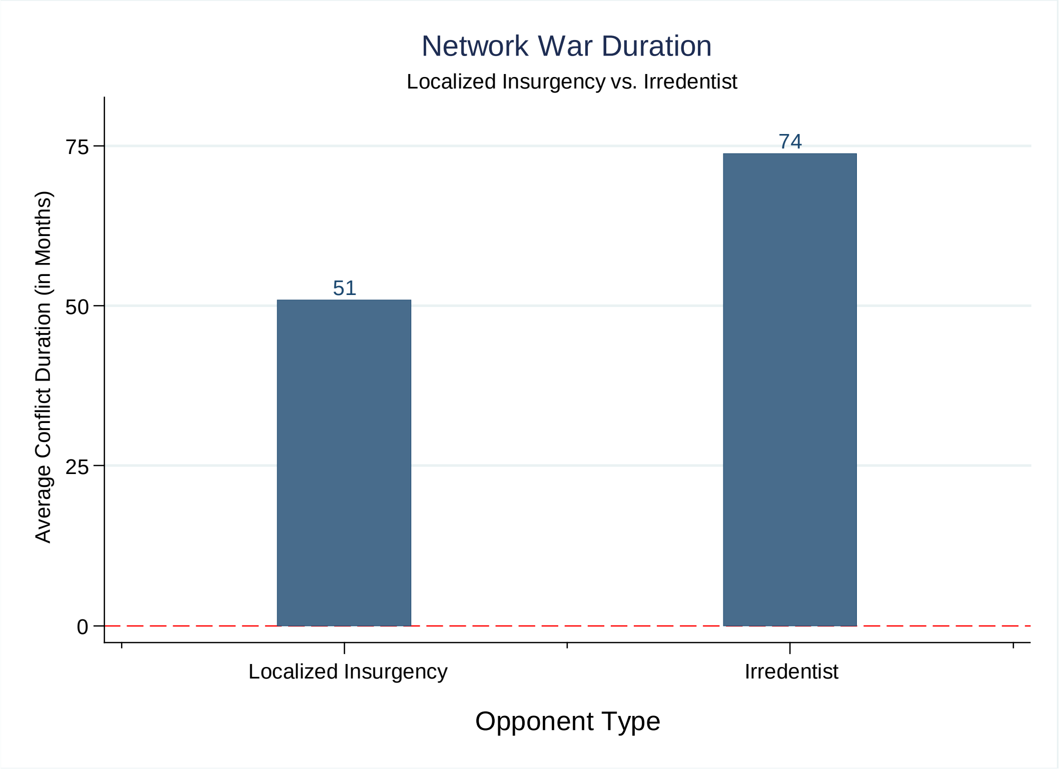


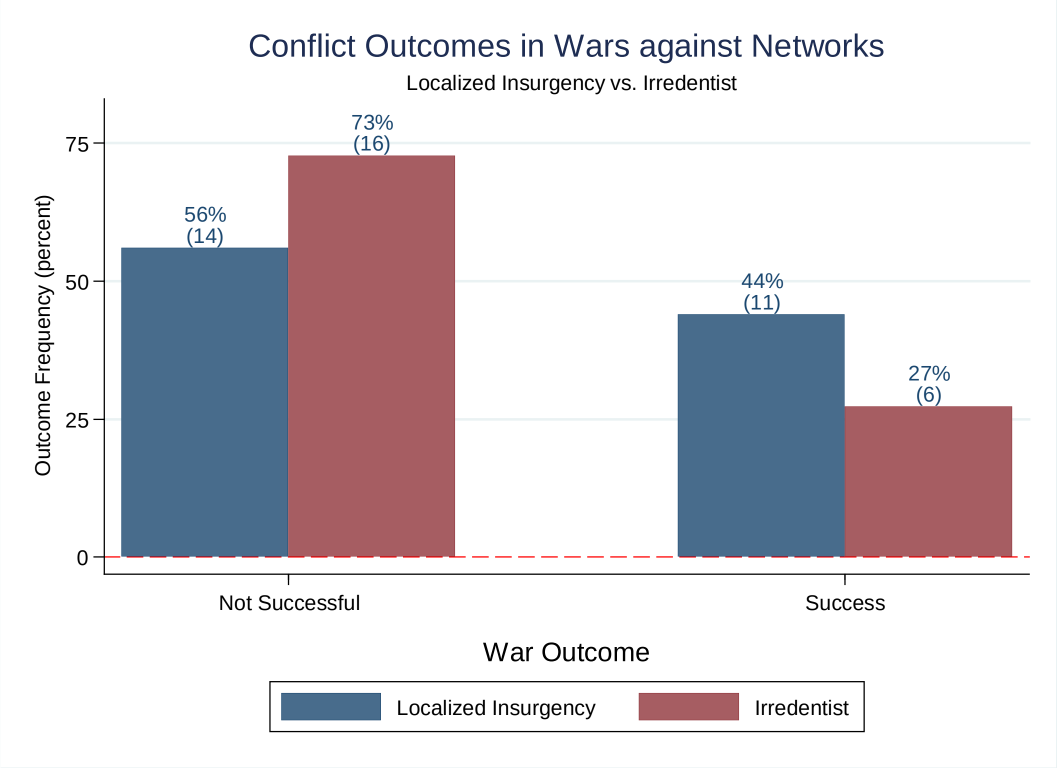
Figure 6 presents the bivariate relationship between conflict type and war duration. As with civilian casualties, irredentist conflicts are, on average, longer than localized insurgencies, which provides initial support for Hypothesis 4B. The logics are related. Strong actors are less likely to abandon their war efforts if it means that their civilians will remain in danger. Since localized insurgencies take place far from strong actors' mainland, they can withdraw forces without giving away central territory. Pulling out of a distant country removes soldiers from harm's way, and may also decrease whatever risk there is to strong actor civilians. From the weak actor's perspective, once the strong actor has left there is little to gain from attacking strong actor civilians at home and much to lose, because an attack might prompt the strong actor to reinvade. Meanwhile, once the foreign power is gone, localized insurgents can turn their attention towards domestic political control.

Figure 6: Network War Duration



By contrast, strong actors do not necessarily reduce the threat to their civilians by abandoning an irredentist conflict. Given the close proximity of the two parties, the weak actor retains the ability to attack the strong actors' civilians. The weak actor may interpret the strong actors' withdrawal as a signal of weakness, and attack again in the hopes of further improving upon an already improved position. Therefore, the strong actor is likely to have a greater interest in an irredentist conflict, accompanied by a higher public tolerance of the military, economic, and political costs incurred during the war, leading to higher strong actor resolve and longer conflicts than in localized insurgencies.

Figure 7: Conflict Outcomes in Wars against Networks



Finally, Figure 7 presents the bivariate relationship between conflict type and war outcomes, measured as success (1) versus everything else (0). The data distribution provides initial support for hypothesis 4C. Close to half (44%) of localized insurgencies end in strong state success, while only 27% of irredentist conflicts end with the stronger actor achieving its war aims. This supports the notion, developed in Hypothesis 4C, that irredentist conflicts pose a greater challenge to strong actors than localized insurgencies.

Multivariate Results

Building upon these results, this section presents the results of multivariate OLS and logistic regression models to test the impact of conflict type on civilian casualties, war duration, and war outcomes among networked opponents when controlling for a variety of other factors expected to influence these outcomes. The expectation, based upon hypotheses 4A-4C, is that moving from a localized insurgency to an irredentist conflict (i.e. increasing Conflict Type) will increase civilian casualties and war duration, but will have a negative impact on war outcomes, decreasing the likelihood of success.

Table 4 presents the results of these multivariate analyses. As expected, conflict type is positive and significant in the model of civilian casualties, indicating that strong states lose significantly higher numbers of civilians in irredentist conflicts than in wars fought against localized insurgencies. Column 2 of Table 4 presents the results for war duration. The coefficient estimate for conflict type is positive, as predicted in hypothesis 4B, but fails to reach standard levels of significance. While hypothesis 4B is not strongly supported by the empirical evidence, this non-significant result may be attributable to the relatively small sample of conflicts against networks. The non-significant result should therefore not be taken as conclusive evidence against hypothesis 4B. The final column of Table 4 presents the results for war outcome, measured as success (1) versus all other outcomes (0). The results of the logit model for war outcomes indicate, as predicted by hypothesis 4C, that strong states are significantly less likely to succeed against networks in irredentist conflicts than against networks in localized insurgencies.

Table 4: Results for Effect of Localized vs. Irredentist Networks

	Civilian Casualties (ln)	War Duration	War Outcome
Conflict Type	1.781***	30.03	-1.756**
	(0.635)	(26.02)	(0.788)
Nuclear State Democracy	-0.938	22.96	-1.069
	(1.132)	(25.45)	(0.747)
Big State Support to Opponent	-1.787**	48.69	0.680
	(0.785)	(44.71)	(2.098)
Nuclear State Military Capabilities	-9.362**	-62.08	7.015
	(4.143)	(158.2)	(5.210)
Conflict Duration (ln)	0.396***		-0.632***
	(0.136)		(0.234)
Constant	-0.498	1.210	3.786**
	(1.663)	(47.62)	(1.686)
Observations	53	54	47

Robust standard errors in parentheses. *p<0.10, **p<0.05, ***p<0.01.

Table 5 presents the substantive results for the impact of conflict type on these outcomes. The average expected number of civilian casualties in a localized insurgency is just over 30. This increases by 146 deaths, to a post-change expected value of nearly 178 civilian deaths, for irredentist conflicts. This represents a percentage increase of 490%. Turning to war outcomes, the predicted probability of strong actor success in a localized insurgency is just over 58 percent. This probability drops to under 23 percent probability of success when the strong state is fighting an irredentist conflict. This is a 35 percentage point reduction in the likelihood of strong state success, or a nearly 69% reduction in this probability. Duration is excluded from Table 5 because conflict type has no significant impact on war duration. However, the OLS results suggest that, although not statistically significant, moving from a localized insurgency to an irredentist conflict increases war duration by just over 30 months, on average.

Table 5: Substantive Results, Impact of Conflict Type

	Localized Insurgency (Baseline Value/Probability)	Irredentist Conflict (Post-Change Value/Probability)	First Difference	Percentage Change
DV: Civilian Fatalities	30.12	177.63	147.51 (17.61, 1118.16)	490%
DV: War Outcome	58.1	22.73	-35.35 (-64.63, -3.85)	-68.9%

Secondary Analysis II: Explaining the Increasing Frequency of Weak Actor Success

Multiple studies of asymmetric conflict have noticed a pattern of increasing weak actor success beginning in the early 20th century. Using a data set of asymmetric wars from 1800-2000 with over 1,000 battle deaths per year, Ivan Arreguin-Toft argues that improvements in weak actor strategy explain the trend. Analyzing the set of counter-insurgency campaigns from 1800-2005, Jason Lyall and Isaiah Wilson III argue that strong actors' increasing reliance on mechanized weaponry reduces soldiers' interaction with the population, weakening counter-insurgent strategy. My data show a related trend of decreasing strong actor success in wars against networks, but I offer an alternative explanation derived from the general theory of asymmetric warfare laid out in chapter one.

Networks, but not small states, appear especially capable of threatening, imposing costs upon, and challenging powerful states in recent decades. Given their greater organizational agility, networks can adapt more quickly than bureaucratic states to major international transitions. I therefore divide my data set into conflicts that took place during the Cold War, and those that took place after the fall of the

Berlin Wall in November 1989. The period after 1989 not only includes this geopolitical transition, but major technological transitions as well, most notably the spread of the internet.

Dividing the period of 1800-2000 into 50-year segments, Arreguin-Toft shows that an increasing percentage of asymmetric conflicts ended with weak actor victory. While weak actors won 11.8% of conflicts from 1800-49 and 20.5% from 1850-99, the weaker party emerged victorious in 34.9% from 1900-1949 and 51.2% from 1950-1999.[131] Arreguin-Toft theorizes that weak actors are more likely to win when they take the opposite strategic approach of their stronger opponents. Therefore, he asserts that "the trend toward increasing strong actor failure is suggested both by the timing of the biggest shift in outcomes favoring weak actors (1950-99), and by the logic of Kenneth Waltz's argument that actors in a competitive international system 'socialize' to similar policies and strategies."[132]

Essentially, Arreguin-Toft argues that Mao figured out how the weak can win asymmetric wars, and subsequent insurgents and guerrillas copied his tactics. "Mao's long fight for and eventual conquest of China was a model consciously imitated by Algerian rebels, the Vietminh, the Hukbalahap, Cuban insurgents, Malayan communists, and, to a large extent, Afghanistan's mujahideen."[133] According to Arreguin-Toft, when European armies socialized to direct assaults came into contact with Asian resistance networks socialized to Maoist guerrilla insurgency, as "they did with greater frequency following World War II—the strong actor lost more often."[134]

While Arreguin-Toft's theory helps explain weak actor victories in the mid-1900s, it is too limited to that time period to offer a sufficient explanation of the overall trend. His socialization theory would predict a return to material domination as more powerful actors become socialized to warfare

[131] Arreguin-Toft, p. 4.
[132] Arreguin-Toft, p. 36.
[133] Arreguin-Toft, p. 37.
[134] Arreguin-Toft, p. 37.

against weaker foes. However, though "armies learn" from fighting insurgencies, powerful states have failed to build upon the lessons of the adaptable British counterinsurgents in Malaya in the 1950s.[135] Furthermore, Arreguin-Toft limits his study to wars with over 1000 battle-related deaths per year, which leaves out dramatically asymmetric conflicts like Israel-Hezbollah, or U.S.-al Qaeda, and ignores many conflicts that are shaped by asymmetry, but did not last long enough or cause enough death to make it into his database. His sample is thus biased in favor of protracted wars, ignoring modern conflicts where the strong actor rapidly leaves when faced with asymmetric resistance, such as the United States withdrawing forces from Beirut in 1983, after losing 241 soldiers from truck bombs,[136] or withdrawing from Mogadishu in 1993, after losing 18 soldiers and two black hawk helicopters.[137] Including these quicker and smaller state-network conflicts makes the pattern more pronounced. Nevertheless, Arreguin-Toft's data still show a constant increase in weak actor victory in each 50 year period after 1800.[138] Mao began fighting in the 1920s. Strategic socialization is thus an insufficient explanation for the broader trend towards weak actor victory.

Lyall and Wilson's explanation for the pattern centers around developments in military technology and the associated effect on strong actor strategy. Their study analyzes 286 insurgencies from 1800-2005, which they define as "a protracted violent struggle by non-state actors to obtain their political objectives—often independence, greater autonomy, or subversion of existing authorities—against the current political authority."[139] Dividing this time period into 25-year segments (except for the most recent segment, 1976-2005), they find that, beginning with 1876-1900, each segment features progressively fewer strong actor victories. While counter-insurgents defeated their weaker opponents

[135] Nagl, section 2, especially pp. 103-107.
[136] "Beirut Barracks Attack Remembered," *CBS News*.
[137] "Ambush in Mogadishu," *PBS Frontline*.
[138] Arreguin-Toft., p. 4.
[139] Lyall and Wilson, "Rage against the Machines," p. 70.

in over 60% of the cases from 1901-1925, that declined below 50% in 1926-1950, below 40% for 1951-1975, and below 30% in the most recent segment from 1976-2005.[140]

Lyall and Wilson attribute this pattern to increasing strong actor reliance on mechanized weaponry. As powerful militaries began using artillery, tanks, airplanes and helicopters that executed stand-off attacks against enemy positions with shells, bombs, and missiles, they relied less and less on infantry. The result was fewer soldiers moving among the civilian population. This shift in force structure increased the lethality of modern militaries, and decreased the risk to their soldiers. However, this bias towards reducing friendly military casualties "inhibits soldiers from assuming the same risks that fence-sitting populations face daily. It therefore becomes harder to recruit reliable collaborators among local populations, further compounding information starvation. The result is a counterinsurgent that fuels, rather than deters, insurgent recruitment."[141]

Improvement in weak actor strategies and an increasing strong actor reliance on mechanization likely play a role in explaining the general trend towards weak actor success, but they do not account for the divergent performance of small states and networks. Additionally, both Arreguin-Toft's general study of asymmetric conflicts and Lyall and Wilson's more specific study of insurgencies arbitrarily divide their samples into, respectively, 50-year and 25-year segments, which seems driven by a preference for round numbers, rather than any applicable theory. To build upon these studies, and account for the distinction between small states and networks, I argue that technological and geopolitical changes in the international environment explain the recent increase in non-state network success in asymmetric warfare. Therefore, the end of the Cold War, the improvement in strong actors' ability to execute precision strikes from distance, and the spread of the internet account for the post-1989 trend of improving big state success against small states and declining success against networks.

[140] Lyall and Wilson, "Rage against the Machines," p. 69.
[141] Lyall and Wilson, "Rage against the Machines" p. 75.

End of the Cold War

The end of the Cold War dramatically altered the global geopolitical landscape. The collapse of the USSR not only removed Soviet influence from many parts of the world, but also led the United States to reorder its foreign policy. In a noteworthy example, the United States and Russia both paid considerably less attention to Afghanistan in the 1990s than in the 1980s, allowing the Taliban to win the Afghan civil war, while veterans of the Afghan resistance against the Soviet Union spread to Saudi Arabia, Bosnia, Chechnya, Sudan and elsewhere. Non-state networks in the former Yugoslavia, the Caucuses, central and south Asia, and the Middle East thus benefited from the increased freedom of movement and shifts in the global arms trade in the post-Cold War environment, as travel restrictions eased and surplus Soviet weaponry, from AK-47s to Katyusha rockets, flooded the market.

Additionally, given the difficulties the US faced in Vietnam and the USSR faced in Afghanistan, great powers may have become wary of launching wars-of-choice against weaker opponents due to the possibility that their opponent would receive external support. The end of the Cold War greatly reduced this possibility, while also freeing great powers' resources to pursue new conflicts. It is therefore possible that various big state-small state and big state-network conflicts in the 1990s and 2000s would not have happened, or would have at least happened differently, if the Cold War had continued.

Strong Actor Military Technology

The period after the fall of the Berlin wall also marks considerable advancements in military technology that enabled the most advanced states to execute precision attacks at considerable distance. Improvements in precision-guided weaponry, or “smart bombs,” allowed powerful states to fire missiles from ships hundreds of miles away or drop bombs from planes flying tens of thousands of feet in the air that could score direct hits. Stealth aircraft—such as the B-2 Spirit, which first flew in July

1989—enabled penetration of all but the most advanced air defenses; and the introduction of unmanned aerial vehicles, or “drones,” enabled reconnaissance missions and airstrikes without risking human pilots. These technological improvements empowered advanced militaries to launch strikes against weaker enemies at will, increasing their advantage over relatively weak states. However, due to the asymmetry of responsibility, non-state networks present their enemies with fewer fixed targets, partially neutralizing the advantage powerful states gained from these new weapons.

The Information Age

The post-Cold War era also coincides with the information technology revolution. The spread of the internet exponentially increased the information acquisition and dissemination capabilities of individuals. Members of non-state networks can now communicate, share tactics, debate strategy, and spread propaganda more easily than before. Insurgents and terrorists have adapted to this new technological environment, researching bomb-making techniques, approaching new recruits, and highlighting the suffering of their people without needing to reveal themselves in public, thereby decreasing their vulnerability to strong actor countermeasures. Additionally, the internet loosens networks from territory, allowing them to communicate over greater distance and grow larger than when they relied on meeting in person, sending letters, or speaking on the telephone.

Meanwhile, the internet, cable and satellite television create a global media environment, which informs people all over the world about what happens in various conflicts. This enhances weak actor strategies based on convincing strong actors to withdraw troops or make concessions. Strong actor citizens are informed of their military's difficulties in protracted conflicts, which could accelerate the development of war-weariness. Networks can highlight the actions of their stronger opponents to garner sympathy from third parties, who then add additional political pressure for the strong actor to withdraw. For example, photos of Americans torturing and humiliating Iraqi prisoners in Abu Ghraib rapidly spread around the world, leading to strenuous criticism, while strengthening the resolve and assisting the recruiting and fund-raising efforts of the Iraqi insurgency. Additionally, the global media broadcasts images from terrorist attacks and researches the attackers' motives, providing terrorist groups with elevated exposure. This increases the disruptive capacity of attacks, spreading fear among targeted populations while increasing the public's perception of the terrorists' importance.

With the end of the Cold War and advancements in weaponry that can accurately strike from distance, big states' ability to achieve their goals against small states has improved. By contrast, various non-state networks quickly adapted to the end of the Cold War and the spread of the internet and global media, developing new strategies and improving upon old techniques. Therefore, I hypothesize that big state-network conflicts will feature greater strong actor civilian and military fatalities, last longer, and end in strong actor success less frequently in the post-Cold War environment compared to those that ended before November 1989.

Hypothesis 5A (threat): Networks cause more big state civilian fatalities relative to small states in the post-Cold War period than during the Cold War.

Hypothesis 5B (cost): Networks cause more big state military fatalities relative to small states in the post-Cold War period than during the Cold War.

Hypothesis 5C (challenge): Big State-Network conflicts last longer relative to conflicts with small states in the post-Cold War era than during the Cold War.

Hypothesis 5D (challenge): Big state-network conflicts end in strong actor failure more often and strong actor success less often relative to big state-small state conflicts in the post-Cold War era than during the Cold War.

Results

An initial examination of the bivariate relationships between Opponent Type and each of the outcome variables in the Cold War versus the Post-Cold War eras provides preliminary support for hypotheses 5A-5D. Figure 8 presents the relationship between Opponent Type and Civilian Fatalities for the Cold War and post-Cold War eras. The relationship depicted in Figure 8 supports the claim that networks have become more threatening in the post-Cold War era. Big states have suffered, on average, 101 additional civilian fatalities when fighting networks after 1989 than before. At the same time, the number of big state civilian fatalities caused by small states declined from an average of 9.1 per conflict to less than one, increasing the gap between small states and networks. Networks were more capable of killing strong actor civilians during Cold War-era asymmetric conflicts than small states, but that effect has increased significantly in the period after November 1989.

Figure 8: Civilian Fatalities by Opponent Type, Cold War vs. Post-Cold War

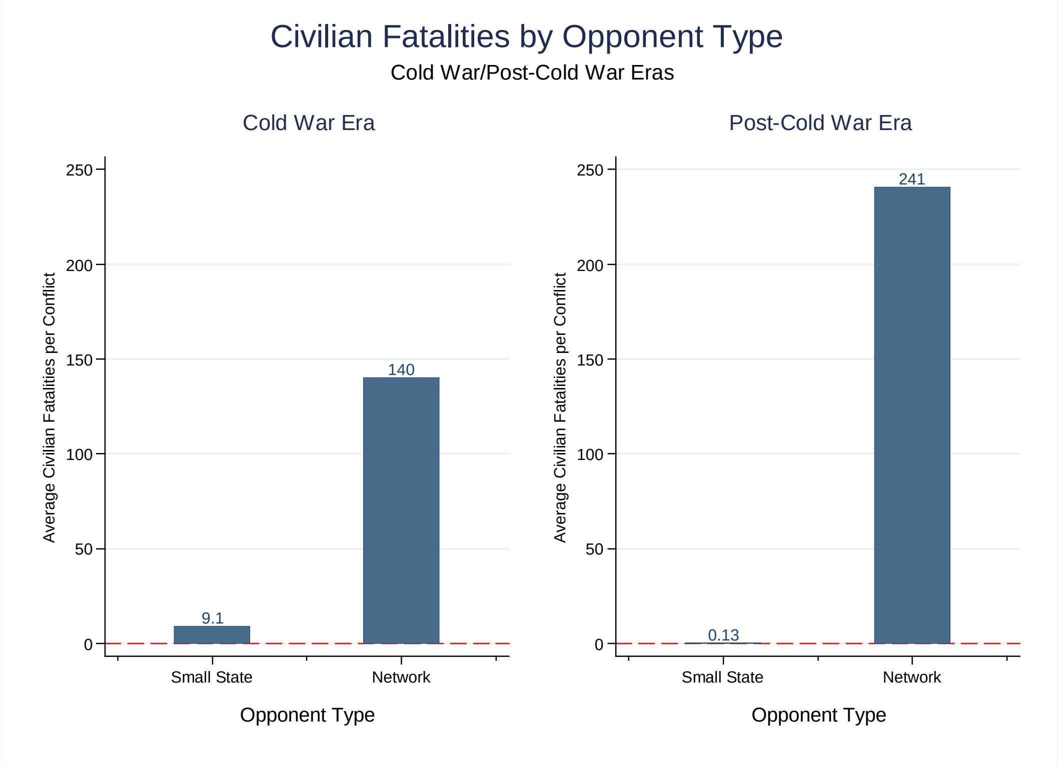


Figure 9 presents the bivariate relationship between opponent type and military fatalities in each of the relevant time periods. The data on military fatalities supports the claim that conflicts against networks have become more costly relative to conflicts against small states in the post-Cold War period. Whereas small states killed an average of 4,696 more soldiers than networks in Cold War-era conflicts, they caused an average of 648 fewer big state military fatalities compared to networks in conflicts taking place after the end of the Cold War. While the relative cost imposed by small states and networks flipped after the Cold War, it is also worth noting that the average number of military fatalities caused by both small states and networks declined in the post-Cold War period compared to conflicts that took place during the Cold War. This suggests that strong actors have altered their strategies or acquired equipment to protect military personnel from asymmetric attacks, or perhaps that medical techniques have improved so that attacks that would have killed soldiers in the Cold War era now result in injuries but not fatalities.

Figure 9: Military Fatalities by Opponent Type, Cold War vs. Post-Cold War Era

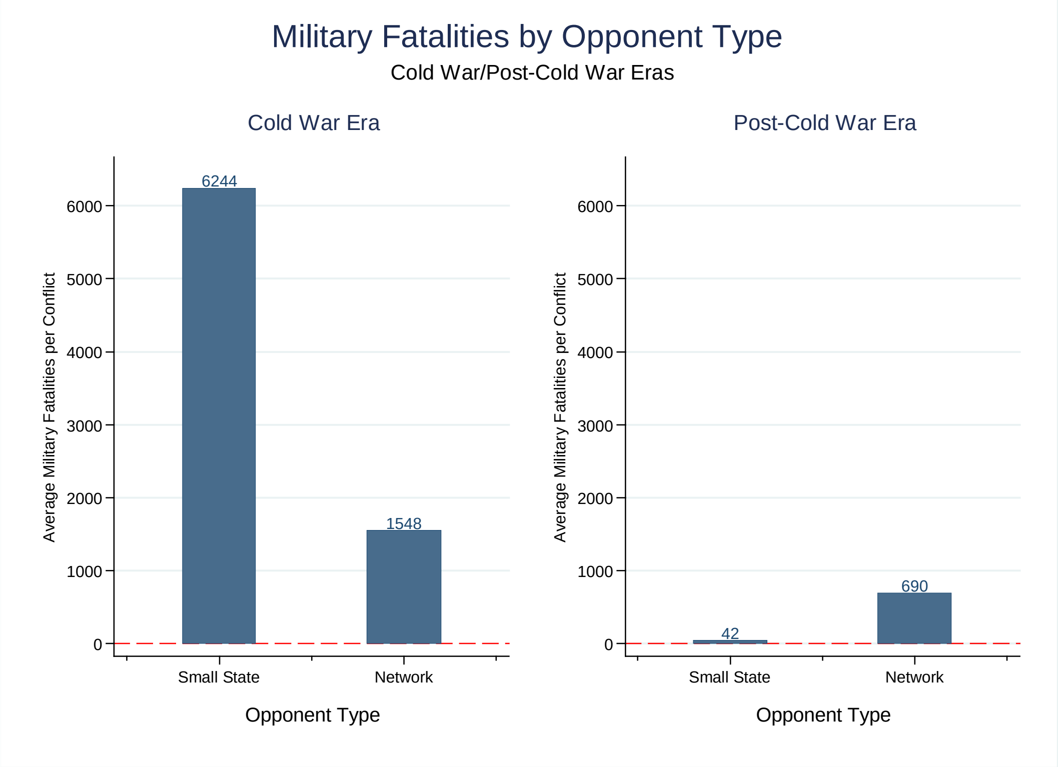
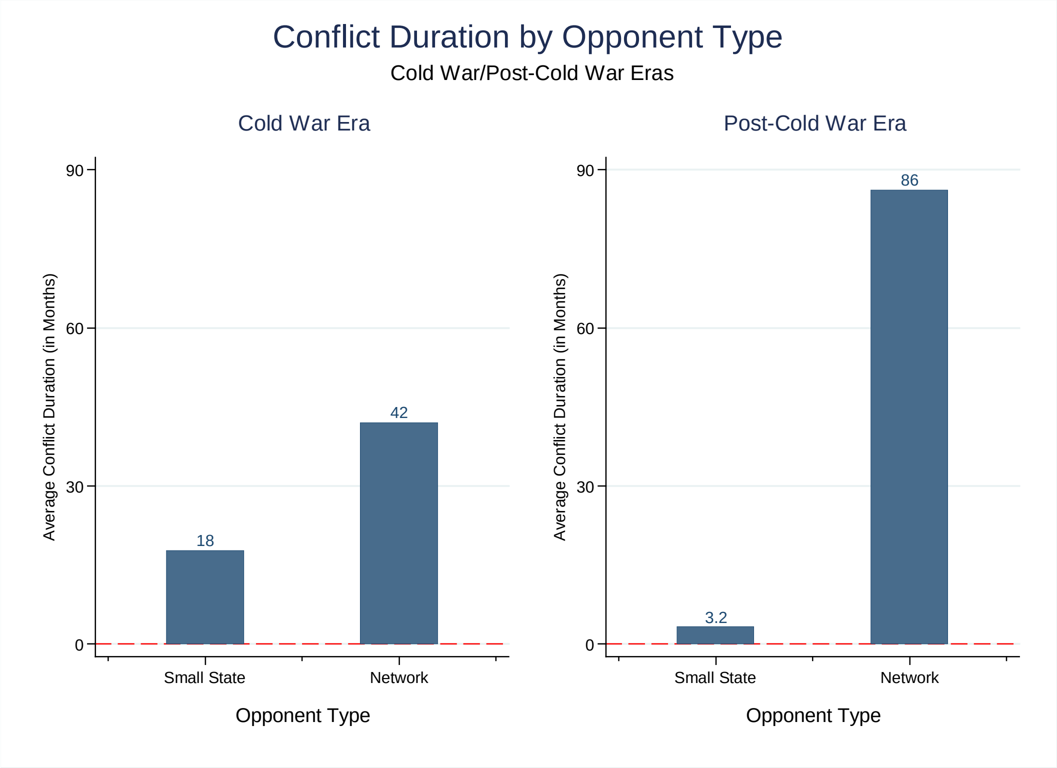


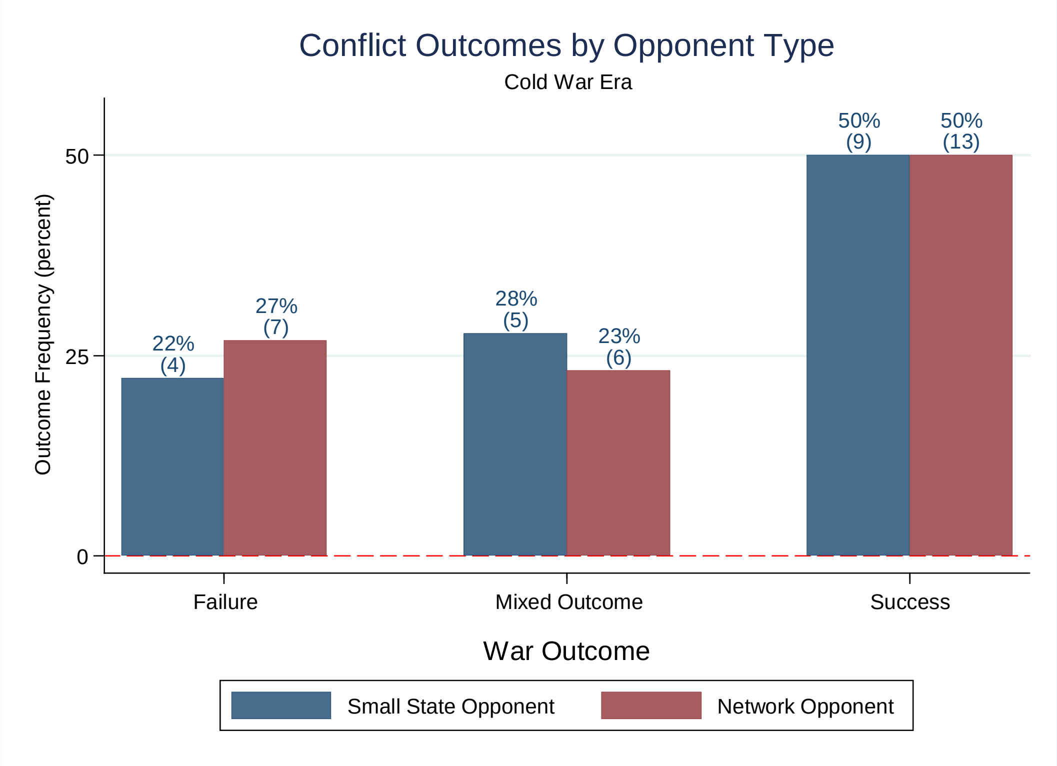
Figure 10 presents the bivariate relationship between opponent type and conflict duration during the Cold War and in the post-Cold War era. Once again, the bivariate relationship provides considerable preliminary evidence demonstrating the increased challenge posed by networks in the post-Cold War period. The average length of a big state-network conflict more than doubled, while the length of big state-small state conflicts shrunk considerably. Conflicts against networks now take almost 27 times as long as conflicts against small states, while big state-network conflicts only lasted 2.33 times as long as big state-small state conflicts in the Cold War era, lending support to the claim that relative network capabilities have improved in the information age.

Figure 10: Conflict Duration by Opponent Type, Cold War vs. Post-Cold War Era



The data on war outcomes provide the most striking illustration of the difference between Cold War era and post-Cold War asymmetric conflicts. Figure 11 presents the distribution of conflict outcomes by opponent type for cases that took place prior to 1989. During the Cold War, strong actors succeeded and failed at fairly similar rates when fighting small states and networks. Twenty-seven percent of conflicts against networks ended with the big state failing to achieve its goal, while only 22% of wars against small states ended with failure, suggesting a slight advantage for networks, but this is a fairly small difference. Meanwhile, big states achieved their goals in 50% of conflicts against both states and networks, indicating that the two types of weak actors posed a relatively equal challenge.

Figure 11: Conflict Outcomes by Opponent Type, Cold War Era

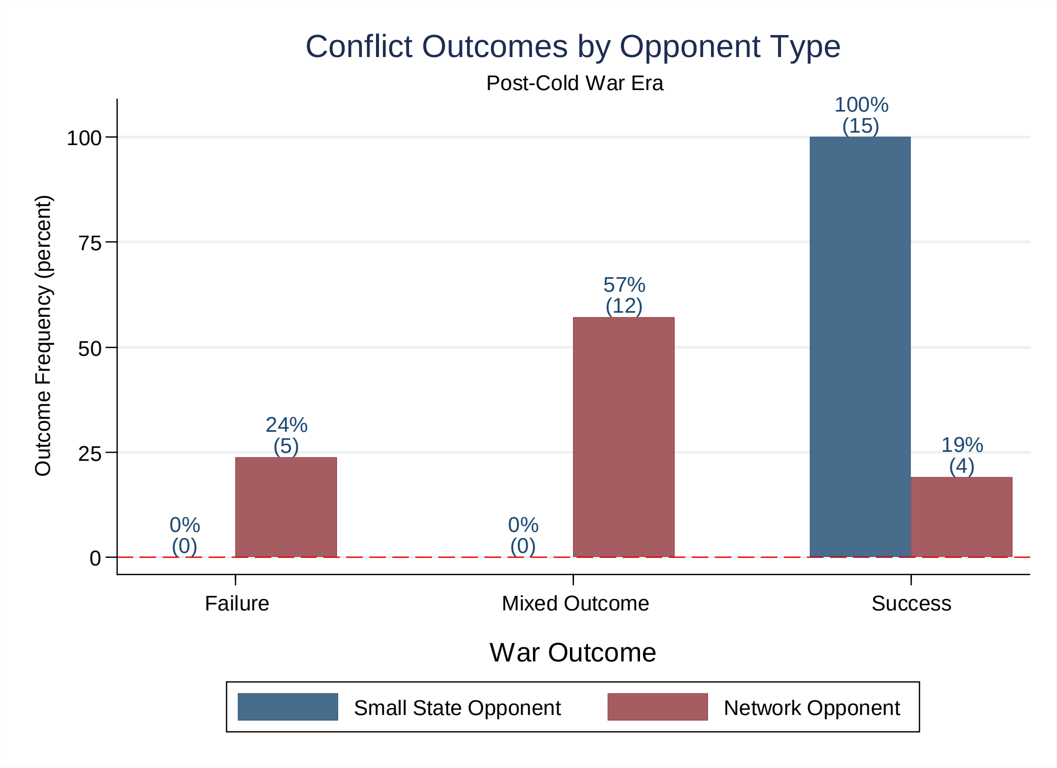


However, the picture in the post-Cold War era is dramatically different. Figure 12 presents the distribution of conflict outcomes by opponent type for conflicts that took place in the post-Cold War era. Strong actors achieved their stated aims in every single conflict against small states after 1989.

This result cannot be explained by a shift to modest goals, as the set of post-Cold War conflicts includes the US/UK invasions of Afghanistan and Iraq, which both rapidly achieved the maximalist goal of vanquishing the small state's army and overthrowing its government, as well as the Russia-Georgia war in 2008 in which the small state lost control of land it considered part of its main territory.

By contrast, strong actors achieved their goals in only 19% of conflicts against non-state networks after 1989. 24% of big state-network conflicts ended in failure, while 57% ended with a mixed outcome. This not only shows that networks have become more challenging relative to small states, but also that networks have become more challenging in the information age than they were during the Cold War. The rate of failure in conflicts against networks is fairly similar during (27%) and after (24%) the Cold War, but the rate of success declined considerably from 50% to 19%. And this does not include ongoing wars against networks in the data set that have proven challenging for great powers, such as irredentist conflicts between Russia and rebels in the Caucuses and a localized insurgency in Afghanistan the United States and United Kingdom have been unable to suppress.

Figure 12: Conflict Outcomes by Opponent Type, Post-Cold War Era



This provides additional support for the general trend towards weak actor success noted by Arreguin-Toft's study of asymmetric wars and Lyall and Wilson's study of counter-insurgency conflicts. However, those studies arbitrarily group conflicts into 50-year and 25-year segments, while this study uses a theory-driven categorization of post-World War II conflicts into two periods: post-WWII through the end of the Cold War and post-Cold War. It therefore provides evidence suggesting that networks' ability to adapt to the 21st century global environment contributes to the pattern of increasing weak actor success. Additionally, by distinguishing between big state-small state and big state-network conflicts, this study demonstrates that the decrease in strong actors' ability to achieve their goals in asymmetric warfare in the most recent period is entirely due to declining success against networks. Strong actors have actually proven more capable of defeating small state opponents, but find wars against networks more threatening, more costly, and more challenging in the information age than during the Cold War.

Multivariate Results

The preliminary evidence presented above is supplemented in this section with multivariate analysis of civilian casualties, military casualties, and war duration. It is not possible to run a statistical analysis on the war outcome dependent variable because there are no cases, in the post-Cold War era, in which a strong state either fails or experiences a mixed outcome in a conflict with a small state. In other words, there is no variation on the dependent variable in that subset of cases, and it is therefore not possible to analyze the relationship using this method. However, the fact that every case of big state-small state conflict in the information age ends in big state victory and many cases of big state-network conflict do not provides noteworthy support for the argument that the 21st century technological environment altered the dynamics of asymmetric warfare.

For each of the other dependent variables, I run an OLS model using the same set of control variables used to test hypotheses 1, 2, and 3. To account for the conditional impact of opponent type during the Cold War versus after the Cold War, I interact opponent type with the Cold War control variable. This allows me to examine whether the threats and costs faced by big states when fighting small states or networks have changed over time.

Table 6 presents the results of the analyses of civilian casualties (model 1), military casualties (model 2) and war duration (model 3). As expected, Opponent Type is a positive, significant predictor of all three outcomes. That is, moving from a small state to a network opponent increases civilian casualties, military casualties, and war duration. Because of the inclusion of an interaction term, however, the coefficient estimates for Opponent Type must be interpreted as the effect of a network versus small state opponent *only* when Cold War equals zero, or in the post-Cold War period only. It is necessary, therefore, to examine the substantive results – in particular the predicted values and first differences from these models, to more directly assess the accuracy of hypotheses 5A-5C.

Table 6: OLS Results for Impact of Opponent Type Conditional on Cold War

	Civilian Casualties (ln)	Military Casualties (ln)	War Duration
Opponent Type	3.210***	3.013***	74.72*
	(0.485)	(0.493)	(29.16)
Cold War	1.190	4.577*	72.59
	(0.847)	(1.953)	(41.99)
Opponent Type X Cold War	-0.649	-2.495*	-61.16
	(0.715)	(0.992)	(36.96)
Big State Support to Opponent	-0.548	4.275*	74.75*
	(0.441)	(1.914)	(29.76)
Nuclear State Democracy	-0.0633	-1.190**	25.51
	(0.505)	(0.344)	(18.44)
Nuclear State Military Capabilities	-4.229*	2.300	13.45
	(1.839)	(3.522)	(80.54)
Irredentist Conflict	1.708**	-0.0116	6.208
	(0.560)	(0.949)	(26.50)
Interstate Conflict	1.946**	1.262	-10.74
	(0.659)	(0.892)	(19.94)
Constant	-4.747***	-0.953	-86.56
	(0.783)	(1.976)	(53.16)
Observations	86	86	88

Standard errors in parentheses, clustered on Nuclear State. *p<0.10, **p<0.05, ***p<0.01.

Table 7 presents the predicted values and first differences for the impact of opponent type, conditional on Cold War, on civilian fatalities, military fatalities, and war duration. As the first row in Table 7 indicates, moving from a small state to a network opponent during the Cold War era resulted in a relatively small, though significant, increase in civilian fatalities by an average of 14 additional deaths. In the post-Cold War era, on the other hand, moving from a small state opponent to a network opponent results in a much larger increase in civilian fatalities of just over 44 additional civilian deaths. Importantly, the first difference for the post-Cold War era is significantly larger than that for the Cold War era, as evidenced by the fact that the upper bound of the 95% confidence interval for the Cold War era does not cross the point-estimate for the post-Cold War era. This result provides strong support for hypothesis 5A, demonstrating that networks do, in fact, cause more big state civilian fatalities relative to small states in the post-Cold War period than during the Cold War.

The second row of Table 7 presents the predicted values and first differences for military fatalities. During the Cold War, there was no significant difference between small states and networks in terms of the number of military fatalities caused. In the post-Cold War era, on the other hand, networks have caused significantly more military fatalities than small states, with an average difference of nearly 469 additional military deaths.

Finally, the last row of Table 7 presents the expected values and first differences for war duration. During the Cold War, big state wars against networks lasted approximately 26 months longer than wars against small states, a difference which is statistically significant. After the Cold War, wars against networks lasted an average of more than 83 months longer than wars against small states, also a statistically significant increase. As expected by hypothesis 5C, the first difference in the post-Cold War era is larger than that during the Cold War. Furthermore, the upper bound of the 95 percent confidence interval surrounding the first difference for the cold-war era is lower than the point estimate of the first difference for the post-Cold War era, indicating that there is a significant difference between the effects of networks versus small states in the two different time periods. Taken together, these results provide strong support for hypotheses 5A and 5C, and moderate support for hypothesis 5B.

Table 7: Predicted Values and First Differences

	Cold War Era			Post-Cold War Era		
	Small-State Opponent (Baseline Value)	**Network Opponent (Post-Change Value)**	**First Difference**	**Small-State Opponent (Baseline Value)**	**Network Opponent (Post-Change Value)**	**First Difference**
DV: Civilian Fatalities	7.25	21.25	14.0 (9.69, 20.11)	4.28	48.38	44.10 (23.39, 83.14)
DV: Military Fatalities	194.24	326.07	131.83 (-7.49, 1682)	24.22	492.8	468.58 (283.9, 747.5)
DV: War Duration	9.83	36.07	26.24 (6.69, 45.69)	3.22	86.28	83.05 (23.83, 141.7)

Conclusion

The analysis in this chapter demonstrates that networks are more formidable opponents for nuclear powers than are small states. However, this effect is especially pronounced after the end the Cold War, which indicates that changes in the international environment in the 1990s and early 2000s enhanced networks' capabilities in asymmetric warfare. In particular, advancements in computing and networking technology empowered individuals, dramatically improving their ability to acquire and disseminate information. This created new opportunities for networks that were able to adapt.

The proposition that non-state networks can rapidly adapt to major international transitions derives from the asymmetry of agility, as laid out in the previous chapter, but this does not imply that every non-state network will develop strategies that take advantage of the window created by geopolitical and technological transitions. Whether due to a lack of imagination, sclerotic ideology, poor access to new technologies, bad timing, or many other possible reasons, most networks probably do not adapt successfully. However, given networks' capacity for adaptation, some will; and those that do will present greater challenges for powerful states that have not yet adjusted to the new environment. Therefore, major geopolitical transitions and the spread of revolutionary information technology would likely both be followed by increased network success in asymmetric conflict in general, rather than improvement for every non-state actor.

For this to have merit as a theory of international asymmetric conflict, as opposed to simply an idiosyncratic explanation for the effects of the end of the Cold War and the information technology revolution, it should apply to earlier transitions as well. Along these lines, the printing press, one of the few inventions that changed the dissemination of information to a degree anywhere near the internet, was introduced to Europe in the mid-15th century and had spread throughout by the early 16th century. Among other mass produced works, the press enabled exponentially greater dissemination of the Bible, sometimes translated into common vernaculars, which likely contributed to various popular rebellions associated with the Protestant Reformation and the Wars of Religion.

For an example of a geopolitical transition, the Napoleonic Wars dislodged established power structures throughout Europe, while spreading ideas associated with the French Revolution, such as nationalism and a more modern concept of liberty. The decades after Napoleon's defeat saw numerous uprisings in various European countries, culminating in the revolutions of 1848. Similarly, the World Wars in Europe dramatically weakened many colonial powers, creating openings for independence movements and rebellions in Asia and Africa. Other studies of asymmetric conflict lend this idea some support, such as Lyall and Wilson's, which finds a significant decrease in counter-insurgent success following World War I.[142]

However, this brief glance at these historical events reveals that an increase in weak actor activity was often followed by a reassertion of strong actor control. For example, most of the revolutions of 1848 quickly burnt themselves out, or fell to reactionary forces. In the 20th century,

[142] Lyall and Wilson, “Rage against the Machines,” p. 70.

some anti-colonial rebellions faltered as departing states helped friendly regimes consolidate power, while other countries that gained independence from declining European powers fell under the influence of the United States or Soviet Union during the Cold War. The advantages non-state actors acquire by reacting more quickly to major international transitions appear to be fleeting.

This suggests that networks' relative success in the first decades after the Cold War will not last. Though networks adapted more quickly to the geopolitical and technological transitions than powerful states, strong actors will create new strategies and develop new technologies designed to counter the latest network techniques. Large bureaucratic states may take some time to adjust to new circumstances, but once they do they are able to reassert their resource advantage, until another transition creates a new opportunity for the non-state networks able to adapt most quickly. For example, the United States, United Kingdom and others have greatly enhanced their internet monitoring capabilities, decreasing terrorists' ability to communicate or research bomb-making anonymously. Additionally, as discussed in Part Two below, developments in military robotics can help states overcome some of the advantages networks acquired by rapidly adapting to the global transitions of the 1990s and developing strategies that made use of the information technology revolution. However, another transition will swing the pendulum back towards non-state networks, as they adapt new strategies that take advantage of future geopolitical and technological changes, to which states will then respond, and so on.

Summary of Data for Each Strong Actor

	Opponent Type	US	USSR/Russia	UK	France	China	Israel
Total Conflicts	Small State	10	2	7	5	3	6
	Network	7	11	13	10	0	14
Average Civilian Fatalities	Small State	0	0	0	0	0	26.17
	Network	434.57	205	55.23	289.5	0	105.86
Average Military Fatalities	Small State	9518	37.5	68.86	8.4	3481.5	672.67
	Network	991.57	2687.27	247.46	1767.1	0	155.29
Average Duration (Months)	Small State	22.7	1.5	7.29	6	4.33	7.17
	Network	76.86	47.42	84.15	74.5	0	46.36
Percent Failure	Small State	20.00%	0.00%	0.00%	0.00%	66.67%	0.00%
	Network	40.00%	30.00%	27.27%	20.00%	N/A	15.38%
Percent Mixed	Small State	10.00%	0.00%	14.29%	0.00%	33.33%	33.33%
	Network	40.00%	10.00%	18.18%	20.00%	N/A	84.62%
Percent Success	Small State	70.00%	100.00%	85.71%	100.00%	0.00%	66.67%
	Network	20.00%	60.00%	54.55%	60.00%	N/A	0.00%

Summary of Data for Each Strong Actor (Excluding Conflicts in which the Weak Actor Received Material Assistance from a Great Power)

	Opponent Type	US	USSR/Russia	UK	France	China	Israel
Total Conflicts	Small State	8	2	7	5	3	6
	Network	7	10	12	10	0	14
Average Civilian Fatalities	Small State	0	0	0	0	0	26.17
	Network	434.57	205	59.83	289.5	0	105.86
Average Military Fatalities	Small State	60.75	37.5	68.86	8.4	3481.5	672.67
	Network	991.57	1482.55	263	1767.1	0	155.29
Average Duration (Months)	Small State	1.5	1.5	7.29	6	4.33	7.17
	Network	76.86	37.42	87.5	74.5	0	46.36
Percent Failure	Small State	12.50%	0.00%	0.00%	0.00%	66.67%	0.00%
	Network	40.00%	22.22%	30.00%	20.00%	N/A	15.38%
Percent Mixed	Small State	0.00%	0.00%	14.29%	0.00%	33.33%	33.33%
	Network	40.00%	11.11%	20.00%	20.00%	N/A	84.62%
Percent Success	Small State	87.50%	100.00%	85.71%	100.00%	0.00%	66.67%
	Network	20.00%	66.67%	50.00%	60.00%	N/A	0.00%

Chapter 3: The War on Terror, Al Qaeda the Organization and Al Qaeda the Idea

The previous chapter separated asymmetric conflict into three categories: localized insurgency, irredentist, and global insurgency. That final category is a recent phenomenon, and al Qaeda is the only case that truly fits the definition. There have been some cases of transnational non-state networks engaging in asymmetric warfare in the past, with the late 19th and early 20th century European Anarchists providing a notable example. However, these earlier cases were confined to a region, while al Qaeda and its affiliates span the globe, executing attacks in North America, Europe, Africa, and various regions of Asia. This conflict is a product of globalization, enabled by the information technology revolution. In particular, the internet facilitates transnational communication and creates the space in which like-minded individuals from around the world can form a network, while the global media provides a worldwide theater for mass-mediated terrorism, providing coverage of attacks and broadcasting leaders' messages.

The organization founded by Osama bin Laden called al Qaeda ("the base") pulled off the largest terrorist attack in history, but has failed to achieve its larger goal of removing American and Western influence from the Muslim world. Following the September 11th attacks, the United States became more involved in the Middle East and Central and South Asia, not less, and significantly degraded al Qaeda's capacity, eventually killing bin Laden in May 2011. This raises the question: is the War on Terror over?

Seeking to avoid association with rendition, torture of prisoners and other unpopular actions the United States took under the rubric of fighting terrorism, the Obama administration has generally refrained from using the phrase “War on Terror.” Elements of the Bush administration first tried rebranding the conflict to avoid these negative connotations, sometimes using “Struggle against Violent Extremism” starting in 2005.[143] Though the United States has used alternative labels, including the euphemistic “Overseas Contingency Operations,”[144] counter-terrorism remains a prominent focus of American national security policy.

Al Qaeda's strategy failed to remove the United States from the Middle East because it approached a global conflict as if it were a localized insurgency. However, as the world's preeminent military and economic power, America's interest in maintaining a presence in the Middle East and supporting allied or friendly governments in Saudi Arabia, Israel, and now Iraq is greater than those of foreign powers that withdrew from distant conflicts in the face of resistance. Furthermore, when al Qaeda attacked New York and Washington, it demonstrated the capacity and desire to directly threaten American civilians. This made the conflict more closely resemble a scaled-up irredentist conflict than a localized insurgency, and the United States responded accordingly, resolving to continue the War on Terrorism until achieving success, or at least a mixed outcome preferable to the status quo.

Bin Laden's group has been severely weakened, and it is unclear if it will survive his death, but the international jihadist movement he helped catalyze lives on. This loosely connected group of organizations and individuals resembles a violent version of a transnational activist network.[145] The various nodes—from fairly large groups like al Qaeda in the Arabian Peninsula to self-starters like the Boston Marathon bombers—share an ideology and the general goal of resisting what they perceive to be a Western war on Islam. The ideology behind international jihad predates al Qaeda and overlaps somewhat with opposition to Israel, but the September 11th attacks and the subsequent American-led invasions of Afghanistan and Iraq galvanized it. The internet facilitates communication between

[143] Schmitt and Shanker, “Washington recasts terror war as 'struggle.'”
[144] Wilson and Kamen, “'Global War on Terror' Is Given New Name.”
[145] See Keck and Sikkink, *Activists Beyond Borders*.

adherents and sympathizers, and gives them access to both the arguments of radical clerics advocating violence and information teaching them techniques to carry it out. Meanwhile, the global media provides coverage of distant conflicts and national actions taken in the name of fighting terrorism, creates an international audience that inflates the impact of terrorist attacks, and frequently refers to any self-stylized jihadists as “al Qaeda,” increasing their perceived importance and unity.

The result is a globalized insurgency of which few members pursue goals beyond the general idea of resistance. Various individuals and organizations that share the jihadist ideology think globally, but act locally. This loose network is less capable of concentrating power than a more tightly organized group, but more adaptable and harder to eliminate.

The War on Terrorism

In response to 9/11 the United States declared a War on Terror, but it has never been entirely clear what that means. The most open-ended interpretation is an ambiguous struggle similar to the War on Poverty or War on Drugs: a problem that can be reduced with effort but never solved entirely. However, unlike the wars on poverty and drugs, primary responsibility for the War on Terror fell to the American military and an expanded and more militarized intelligence community. Those organizations, tasked with the national security of the United States, typically operate against clearly defined enemies, but terror is an emotion and terrorism is a tactic, neither of which can be vanquished.

The US government's “National Strategy for Combating Terrorism,” released in February 2003, is somewhat more specific, but still quite broad. “The intent of our national strategy,” it declares, “is to stop terrorist attacks against the United States, its citizens, its interests, and our friends and allies around the world and ultimately, to create an international environment inhospitable to terrorists and all those who support them.”[146] While the document acknowledges that victory will not be clearly marked by a formal surrender, it does present a desirable end-state at which point the war will be won, envisioning that “through the sustained effort to compress the scope and capability of terrorist organizations, isolate them regionally, and destroy them within state borders, the United States and its friends and allies will secure a world in which our children can live free from fear and where the threat of terrorist attacks does not define our daily lives.”[147] This is grandiose, but it points to clear goals: reducing the scope and capacity of known terrorist groups, improving vigilance and homeland security to decrease vulnerability to terrorism, and coordinating international efforts to advance these goals through intelligence sharing, freezing terrorists' finances and denying them safe haven.

However, it became clear in the war's first years that the United States did not intend to target every terrorist group that threatens a friend or ally. At the time of the National Strategy's publication, the US State Department listed 36 “Designated Foreign Terrorist Organizations,” but the United States did not devote military and intelligence efforts towards combating all of them. Groups focused on single countries that had not killed Americans or directly threatened American interests, such Aum Shinrikyo in Japan, Basque Fatherland and Liberty (ETA) in Spain, and Sendero Luminoso (Shining Path) in Peru fell outside the scope. Critics accused the United States of waging a war on Islam, noting that the groups targeted by the United States all espoused Islamist ideologies. In a poll of four Muslim majority countries (Morocco, Egypt, Pakistan, Indonesia) conducted from December 2006 to February 2007 by World Public Opinion, 79% said that a goal of US foreign policy is to “weaken and divide the Islamic world,” which ranged from 73% of respondents in Indonesia to 92% in Egypt.[148]

Contributing to this perception was the “second phase” of the War on Terror, in which the Bush administration pivoted to rogue states. In a speech on September 12, 2001, President George W. Bush

[146] “National Strategy for Combating Terrorism,” p. 11.
[147] “National Strategy for Combating Terrorism,” p. 12.
[148] “Muslims believe US seeks to Undermine Islam.”

linked al Qaeda to the Taliban government providing them sanctuary in Afghanistan, claiming "we will make no distinction between the terrorists who committed these acts and those who harbor them."[149] When the Taliban did not respond to America's demand to arrest and extradite bin Laden, a US-led multinational coalition worked with the Afghan Northern Alliance to depose the Taliban and dislodge al Qaeda from its sanctuary.

However, US policy soon shifted from retaliation to preemption. Identifying terrorists armed with weapons of mass destruction as potentially the most serious threat facing the United States, Bush declared that "we must prevent terrorists and regimes who seek chemical, biological or nuclear weapons from threatening the United States and the world."[150] The president labeled North Korea, Iran and Iraq an "Axis of Evil" and accused them of "arming to threaten the peace of the world."[151] These states, Bush argued "could provide [WMD] to terrorists, giving them the means to match their hatred."[152] Because of this possibility, the United States would oppose rogue regimes, using military force preemptively if necessary.[153]

This culminated in the invasion of Iraq and overthrow of Saddam Hussein. In a September 12, 2002 speech to the United Nations, President Bush argued that Iraq was pursuing nuclear weapons and that this was a risk the UN could not afford because "if an emboldened regime were to supply these weapons to terrorist allies, then the attacks of September 11th would be a prelude to far greater horrors."[154] Bush accused Iraq of sheltering and supporting terrorist organizations, though he never explicitly tied Saddam Hussein's government to al Qaeda or the September 11th attacks in any formal speech. Other administration officials, most notably Vice President Dick Cheney, asserted that Saddam

[149] Bush, "Bush addresses nation."
[150] Bush, "State of the Union Address" January 29, 2002, p. 3.
[151] Ibid.
[152] Bush, "State of the Union Address" January 29, 2002, p. 4.
[153] See, for example, "National Security Strategy of the United States of America," September 2002, p. 6.
[154] Bush, "Remarks at the United Nations General Assembly," September 12, 2002, p. 4.

Hussein worked with al Qaeda.[155] However, while Iraq had provided some support to non-state networks fighting against Turkey, Iran and Israel, there was no evidence linking the Iraqi government to al Qaeda or any other terrorist group that had killed Americans.[156] Unlike the Taliban, Saddam Hussein's regime did not impose a strict interpretation of Sharia law, making Iraq a potential target for al Qaeda rather than a likely ally. Nevertheless, the primary public justification for the invasion of Iraq was the possibility that Iraq could provide anti-American terrorists with weapons of mass destruction in the future.

Pre-war UN weapons inspections found, and post-invasion searches confirmed that Iraq did not have an active nuclear or biological weapons program,[157] and administration officials revealed that the Bush administration saw the overthrow of Saddam Hussein as a priority before September 11th,[158] but the interpretation of the War on Terrorism that targets rogue regimes lives on in the concept of the Long War. This term, popularized by General John Abizaid, acts as a general policy guideline for the Pentagon in the post-Cold War world.[159] Whereas the United States sought containment of the Soviet Union and opposition to communism after World War II, now America's general geopolitical goal is to prevent disruption of the globalizing international order.[160] The main actors interested in or capable of disrupting this order are rogue states and terrorist groups, independently or in concert, and opposing them provides a general strategic direction for the United States that's an alternative to the framework that places China as a “near-peer” competitor akin to the USSR. Following this policy, the United States would act globally to counter terrorist groups (e.g. drone strikes against suspected al Qaeda

[155] “Cheney Reasserts Al Qaeda Links to Saddam Hussein's Iraq.”

[156] “Terrorism Havens: Iraq.”

[157] “CIA's final report: No WMD found in Iraq.”

[158] Suskind, *The Price of Loyalty*.

[159] Graham and White, “Abizaid Credited With Popularizing the Term 'Long War.'”

[160] See Carafano and Rosenzweig, *Winning the Long War* and, even though he doesn't use the phrase “Long War,” the strategic writings of Thomas P.M. Barnett in *The Pentagon's New Map* and *Blueprint for Action*.

operatives) and overthrow or contain rogue states pursuing weapons of mass destruction (e.g. sanctions, covert activity, and possibly future military action against the Iranian nuclear program).

This is the broadest interpretation of the War on Terror, incorporating goals above and beyond the prevention of terrorist attacks. At the other end of the spectrum is the narrowest interpretation: a war against al Qaeda, the organization responsible for the September 11th attacks. This rubric treats the response to September 11th as similar to law enforcement, aiming to arrest (if possible) or kill the individuals who planned, perpetrated, and assisted with the attacks.

That task has been mostly accomplished. The original 19 hijackers died in the attacks, and Mohammed al Qahtani, the alleged "20th hijacker" was captured in Afghanistan in 2001 and imprisoned in Guantanamo Bay. (Qahtani was unable to participate in the attacks because he arrived at Orlando International Airport in Florida on August 3, 2001 having used a one-way ticket, and US immigration denied him entry out of suspicion that he intended to become an illegal immigrant). Khalid Sheikh Mohammed, named the "principal architect of the 9/11 attacks" by the 9/11 Commission Report was captured in Pakistan on March 1, 2003 and remains in US custody.[161]

The United States alleged that five senior members of al Qaeda, including Khalid Sheikh Mohammed, were "fully aware of the operation's details,"[162] and all five are dead or in custody. Mohammed Atef, the military chief of al Qaeda, was one of the "principle decision makers" and recruiters for the 9/11 attacks;[163] and was killed by a US drone strike near Kabul, Afghanistan in November 2001.[164] Abu Turab al Urduni, who trained the 9/11 attackers in hijacking, disarming air marshals, explosives, and basic English, was also killed in Afghanistan in 2001.[165] Ramzi bin al Shibh, who facilitated communications between the attackers and al Qaeda's leaders, was captured in Karachi,

[161] "The 9/11 Commission Report."

[162] "Substitution for Testimony of Khalid Sheikh Mohammed, p. 24."

[163] Ibid.

[164] "Taliban confirms death of Osama bin Laden's military chief in U.S. Strike."

[165] "Substitution for Testimony of Khalid Sheikh Mohammed, p. 24."

Pakistan in September 2002, and held by the CIA in Morocco before being transferred to Guantanamo Bay in 2006.[166] And Osama bin Laden, the leader of al Qaeda, was killed by US forces in Abbottabad, Pakistan on May 2, 2011.

However, the War on Terror was always about more than bringing the individuals responsible for 9/11 to justice. Regardless of the label used for the conflict, there is a near-consensus among American and allied military and political leaders that preventing future al Qaeda attacks is a worthwhile national security goal. But that goal is more expansive than countering bin Laden's organization; it also includes combating the international movement he helped catalyze.

Al Qaeda the Organization

Al Qaeda's war against the United States began shortly after its founding in 1988. The minutes of the original meeting in Peshawar, Pakistan—which was attended by Osama bin Laden, Ayman al Zawahiri, and Sayyed Imam al Sharif, better known as Dr. Fadl[167]—vow to advance the cause of Islam and do not mention America, but the United States became al Qaeda's main target within a few years. Bin Laden, like many Arabs and Muslims (and others) had long criticized the United States for its support of Israel, advocating a boycott of American products in a 1986 speech because "the Americans take our money and give it to the Jews so they can kill our children with it in Palestine."[168] However, bin Laden's choice to make America the focus of al Qaeda's jihad grew out of his reaction to the Saudi decision to accept the United States' protection in the Gulf War.

After Iraq invaded Kuwait in August 1990, Saudi Arabia feared that Saddam Hussein's army might next push on to capture northern Saudi oil fields. Bin Laden, fresh off his participation in the successful expulsion of Soviet forces from Afghanistan, used his family connections to contact the

[166] "Binalshibh to go to third country for questioning."
[167] Wander, "A history of terror: Al-Qaeda 1998-2008."
[168] Bergen, *The Longest War*, p. 18.

Saudi royal family and offer to protect Saudi Arabia from a potential Iraqi attack. The Saudis turned him down, opting for American help instead. Accepting assistance from the world's preeminent military power over that of a group that helped compel invaders to withdraw after a decade of insurgency makes eminent strategic sense, but bin Laden was infuriated by the presence of 500,000 American troops, some of them women, in the land of Islam's two holiest cities. To bin Laden, his followers, and various Muslim clerics in Saudi Arabia and elsewhere, the Saudi government had willingly allowed an infidel army to invade Muslim land. In their interpretation, these foreign forces were "crusaders," and their presence "in the sanctuary of Islam posed a greater calamity than the one that Saddam was already inflicting on Kuwait."[169]

Unwelcome by the Saudis, bin Laden fled to Pakistan and then shifted al Qaeda to Sudan, where he first developed a plan to attack Americans. Still angry over the presence of American forces in Saudi Arabia, bin Laden interpreted the American mission in Somalia that began in December 1992 as evidence that the United States intended to colonize Muslim lands. Al Qaeda's first attack on an American target was against two hotels in Yemen that housed US Soldiers bound for Somalia. The bombs killed two tourists, but no Americans.[170]

This attack was unsuccessful, but the American intervention in Somalia shaped al Qaeda's strategy. The United States pulled out of Somalia in response to losing 18 soldiers in Mogadishu in October 1993 while trying to capture a Somali warlord, in what became known as the Black Hawk Down incident. Similarly, in 1983, the United States withdrew forces from Lebanon after a truck bomb attack on a marine barracks killed 241 American servicemen. To bin Laden and other al Qaeda strategists, this demonstrated that America is weak, and will quit when faced with resistance. "The youth were surprised at the low morale of the American soldiers and realized more than before that the

[169] Wright, *The Looming Tower*, p. 182.
[170] Wander, "A history of terror: Al-Qaeda 1998-2008."

American soldier was a paper tiger and after a few blows ran in defeat," bin Laden told an interviewer in reference to the withdrawal from Somalia. "And America forgot all the hoopla and media propaganda about being the world leader and the leader of the new world order, and after a few blows, they forgot about this title and left, dragging their corpses and their shameful defeat."[171]

Drawing on his experience fighting in the successful localized insurgency against the Soviet Union in Afghanistan, bin Laden crafted a strategy based on attacking American targets to compel an American withdrawal from the Middle East. In 1996, bin Laden left Sudan under pressure from the government, and established a new base of operations in Afghanistan. From there, in August 1996, he issued a "Declaration of War against the Americans Occupying the Land of the Two Holy Places," referring to Mecca and Medina in Saudi Arabia. It argues that "the people of Islam had suffered from aggression, iniquity and injustice imposed on them by the Zionist-Crusaders alliance and their collaborators" and declares that all Muslims have a religious duty to attack Jews and Americans.[172]

Al Qaeda began carrying out this strategy with attacks on American targets in Africa. On the morning of August 7, 1998, truck bombs exploded at the American embassies in Nairobi, Kenya and Dar es Salaam, Tanzania. The explosions killed 223 people, including 12 Americans. In response, the United States launched cruise missiles at al Qaeda training camps in Sudan and Afghanistan. These caused some damage, but only further convinced bin Laden that the United States would not be willing to put its soldiers at risk and therefore lacked the stomach for a protracted conflict.

The next major al Qaeda attack was scheduled for the turn of the millennium, on or around January 1, 2000. The plan consisted of near-simultaneous attacks on four locations in Jordan targeting American and Israeli tourists, an attack on Los Angeles International Airport, and an attempt to sink the *USS Sullivans*, a destroyer refueling in Aden harbor off the coast of Yemen. Jihadists had executed

[171] Zernike and Kaufman, "The Most Wanted Face of Terrorism."
[172] Bin Laden, "Declaration of War against the Americans Occupying the Land of the Two Holy Places."

terrorist attacks in the United States before—most notably a team led by Ramzi Yousef set off a truck bomb below the North Tower of the World Trade Center in 1993 that killed six[173]—but the LAX plot was the first time someone acting at al Qaeda's direction attempted an attack on US soil. Jordanian intelligence thwarted the first plot, US Customs and Border Protection thwarted the second by catching a would-be LAX bomber crossing the Canadian border with bomb-making material, and the attack against the *Sullivans* failed when the boat intended for a suicide attack sank under the weight of the explosives onboard.[174]

The attack against the *Sullivans* failed, but a successor attempt against the *USS Cole* succeeded on October 12, 2000. The suicide boat attack killed 17 sailors and injured another 39. This success proved a significant victory for al Qaeda, as "camps in Afghanistan filled with new recruits, and contributors from the Gulf States arrived carrying Samsonite suitcases filled with petrodollars."[175] Furthermore, the United States did not retaliate, possibly because less than a month remained until the Bush-Gore presidential election, because President Clinton was focused on negotiating Israeli-Palestinian peace, or because the CIA was uncertain as to bin Laden's location.[176] Regardless, this further convinced al Qaeda's leaders that they could benefit from attacking American targets.

Al Qaeda next struck on September 11, 2001, killing 2,996 in the largest terrorist attack in history. Bin Laden's strategic intent behind 9/11 was likely a combination of three possibilities. Either the United States would be frightened and withdraw support for Saudi Arabia and Israel, much as it had withdrawn from Somalia in 1993; the United States would not react, as in the aftermath of the *Cole* bombing, or would respond with a limited strike as it had in response to the embassy attacks, and al

[173] "First Strike: Global Terror in America."
[174] Loeb, "Planned Jan. 2000 Attacks Failed or Were Thwarted; Plot Targeted U.S., Jordan, American Warship, Official Says."
[175] Wright, *The Looming Tower*, p. 374.
[176] Ibid.

Qaeda would gain recruits and funding;[177] or perhaps the attacks would bait the United States into invading Afghanistan, where bin Laden believed the mujahideen could win as they had against the Soviet Union.[178] On October 3, 2001, in anticipation of an American invasion of Afghanistan, bin Laden wrote a letter to Taliban leader Mullah Omar explaining his conviction that "a U.S. campaign against Afghanistan will cause great long-term economic burdens which will force America to resort to the former Soviet Union's only option: withdrawal from Afghanistan, disintegration, and contraction."[179]

9/11 was thus a tactical success for al Qaeda, but a strategic failure. The attacks demonstrated that the United States was vulnerable which likely pleased and motivated jihadists around the world, but the aftermath did not go as bin Laden hoped. It took barely one month for the United States to depose the Taliban, which had both provided al Qaeda with sanctuary and represented the closest thing to the organization's vision of a true Islamic government. Almost 12 years after the original invasion, the United States and the UN-sanctioned International Security Force has not been able to defeat the Afghan insurgency. However, Hamid Karzai, the appointed leader of the Afghan Transitional Administration, won national presidential elections in 2004 and 2009. Despite expressing a desire to negotiate with insurgent groups, he shows no interest in supporting al Qaeda or the international jihadist cause and agreed to an "Enduring Strategic Partnership" with America.[180] Meanwhile, the United States, which plans to withdraw forces from Afghanistan in 2014,[181] does not appear on the verge of economic or political collapse.

American and allied Afghan forces mostly drove al Qaeda from Afghanistan, and the United States continued pursuing its core members as they fled to Pakistan and elsewhere. The central

[177] Bergen, *The Longest War*, p. 5.
[178] Wright, *The Looming Tower*, p. 375.
[179] Bergen, *The Longest War*, p. 10.
[180] "Enduring Strategic Partnership Agreement between the Islamic Republic of Afghanistan and the United States of America."
[181] Yellin, "Obama strongly considers withdrawing all troops from Afghanistan in 2014."

organization has not been able to execute another attack against an American target, claiming only a June 2002 attack on a synagogue in Tunisia that killed 19,[182] and some bombings in Pakistan. Many of the senior members are dead or in custody.

Bin Laden's death could mean the end of the group he founded. Accounts from inside al Qaeda show that bin Laden “exercised near-total control” of the organization. Senior members had to swear a religious oath to him personally, and he could overrule a consensus position among the rest of the leaders by himself.[183] This role persisted after the invasion of Afghanistan and throughout al Qaeda's subsequent time underground. Materials captured in the 2011 raid on bin Laden's compound revealed that he continued orchestrating his group's operations, contacting operatives through couriers.[184]

Former lieutenant Ayman al Zawahiri has formally taken the leadership role of post-bin Laden al Qaeda, but most accounts describe him as uncharismatic, “a poor speaker, argumentative, and a know-it-all.”[185] Bin Laden's reputation was almost precisely the opposite: charismatic in person, admired for forgoing the life of luxury his family's wealth could afford him in favor of a modest, pious existence, and especially well-spoken in public, from wedding speeches to formal recorded addresses intended for a global audience.[186] Given the role personal inspiration and devotion played in al Qaeda under bin Laden, Zawahiri may not be able to guide the organization back to a similarly prominent position.

Bin Laden made multiple strategic errors. He underrated both the importance of great power material assistance to the mujahideen's victory over the USSR as well as the developments in strong actor military technology in the years since the Soviet Union withdrew, including laser-guided precision missiles and unmanned aerial vehicles. He overrated the importance the Afghan war played

[182] “Al-Qaeda claims Tunisia attack.”
[183] Bergen, *The Longest War*, pp. 24-25.
[184] Hashim, “The Bin Ladens' life on the run.”
[185] Musharbash, “A New Path for Al-Qaida: Zawahiri Confirmed as Bin Laden's Successor.”
[186] Bergen, *The Longest War*, p. 25.

in the collapse of the USSR, ignoring the role of internal economic and political problems, and therefore believed that the United States would suffer a similar collapse if it tried to occupy Afghanistan. Perhaps most importantly, he built his strategy around theories of localized insurgency, when the war he wished to undertake more closely resembled a large-scale irredentist conflict.

The key feature of a localized insurgency is the strong actor's ability to withdraw without sacrificing a central national interest, and this goal seemed to drive bin Laden's thinking. He noted attacks that killed American soldiers, precipitating withdrawal from Beirut and Mogadishu, and miscalculated that a larger attack against American civilians would lead to a larger withdrawal from the greater Middle East. However, the United States' support for Saudi Arabia, Israel, and other friendly Middle Eastern governments, and interest in guaranteeing the normal flow of the world's oil supply, is considerably larger than America's commitment to peacekeeping missions in Lebanon or Somalia. When al Qaeda attacked American military and diplomatic targets abroad, it utilized a transnational version of a localized insurgency strategy. However, by killing many civilians on US soil, al Qaeda galvanized American resolve in a manner similar to strong actors fighting irredentist conflicts, leading to the War on Terrorism.

Al Qaeda the Idea

Bin Laden's strategy may have weakened his organization and failed to reduce American influence in the Middle East or Central and South Asia, but there is one area where he seems to have succeeded: spreading international jihadism and turning the cause into a global movement. The ideas behind fundamentalist Muslims violently resisting Western influence and overthrowing insufficiently religious regimes predate al Qaeda, but bin Laden's speeches, the September 11th attacks, and America's subsequent invasions of Afghanistan and Iraq spread the ideology and increased the number of adherents. Numerous organizations have taken up the al Qaeda label, only some of which received support from bin Laden's central group. Additionally, individuals from North America, Europe, North and East Africa, the Middle East, the Caucuses, and Central, South, and Southeastern Asia have committed violence in the name of jihad.

Abdullah Azzam, a Palestinian theologian, has been called the Father of Global Jihad.[187] In reaction to the Soviet invasion of Afghanistan—the first time since World War II that a non-Muslim state had invaded a majority-Muslim country—Azzam issued a fatwa (religious ruling) called "Defense of the Muslim Lands" instructing Muslims that their first obligation, after faith, was to fight against aggression by non-Muslims.[188] Azzam called on Muslims from around the world to help expel foreigners from Muslim lands, primarily the Soviets from Afghanistan and the Israelis from Palestine. This call to jihad resonated around the world, "inspiring men from Algeria to Brooklyn to travel to Pakistan and Afghanistan" to fight the Soviets.[189] One of these men was Osama bin Laden.

Azzam died from a car bomb explosion on November 24, 1989, but his ideas live on. His assassin remains unknown, though various parties have suspected competing Afghan warlords or mujahideen leaders, the CIA, Mossad, or operatives working for Ayman al Zawahiri.[190] Azzam's legacy, however, is considerable. In addition to mentoring bin Laden, Azzam helped found both Hamas, the Palestinian group that now controls Gaza, and Lashkar e Taiba, the group based primarily in Pakistan-administered Kashmir that executed the 2008 Mumbai attacks.[191]

In line with Azzam's call to fight defensive jihad, these organizations focus on expelling non-Muslims from what they believe to be Muslim lands, but al Qaeda's goals are more expansive, shaped by the ideas of Ayman al Zawahiri. An Egyptian doctor, Zawahiri led Egyptian Islamic Jihad in its

[187] Riedel, "The 9/11 Attacks' Spiritual Father."
[188] Azzam, "Defense of the Muslim Lands."
[189] Bergen, *The Longest War,* p. 14.
[190] Bergen, *The Osama bin Laden I know*, p. 97.
[191] Riedel, "The 9/11 Attacks' Spiritual Father."

fight against the Egyptian government. Following the teachings of Sayyid Qutb, a leader of the Egyptian Muslim Brotherhood imprisoned and later killed by the Egyptian government, Zawahiri strongly opposed both the secular rule of Gamal Abdel Nasser and the peace agreement with Israel signed by Nasser's successor Anwar Sadat. Qutb argued for offensive jihad, writing that those "who attempt to defend the concept of Islamic jihad by interpreting it in the narrow sense of the current concept of defensive war... lack understanding of the nature of Islam and its primary aim."[192] This led Zawahiri to believe that jihad required more than fighting against foreign forces occupying Muslim countries. He argued that jihadists should overthrow governments throughout the Middle East, which would both purify Islamic society and strengthen it for a fight against the West.[193] Zawahiri officially merged Egyptian Islamic Jihad into al Qaeda in 1998.

The intellectual justification for jihadist violence against fellow Muslims and secular or insufficiently religious regimes comes from Dr. Fadl. Fadl wrote "The Essential Guide for Preparation," which al Qaeda used as both a training manual and motivational tool. The Guide asserts that Muslims must always be in conflict with non-believers and that rewards await those who fight, or assist the fighters, in the afterlife. This argument resonated in part due to Fadl's reputation as an accomplished religious scholar. In the Guide, Dr. Fadl denounces many Middle Eastern governments as apostate, arguing that "the way to end the rulers' unbelief is armed rebellion." Many Arab governments banned the book and arrested anyone caught with a copy.[194]

Bin Laden combined Azzam's notion of defensive jihad against foreigners, Qutb and Zawahiri's desire for offensive jihad against apostate Muslim governments, and Fadl's justifications for worldwide attacks against non-Muslims into a two-stage strategy. He agreed that jihadists needed to purify the Muslim world by overthrowing secular and corrupt governments, but asserted that this "near enemy"

[192] Qutb, *Milestones*, quoted in Bergen, *The Longest War*, p. 24.
[193] Wright, *The Looming Tower*, pp. 43-47.
[194] Wright, "The Rebellion Within," p. 2.

could not be defeated until the United States, the "far enemy," was forced to withdraw its support.[195] Bin Laden's 1996 fatwa declaring war reflects Azzam's teachings by arguing "clearly after Belief there is no more important duty than pushing the Americans out of the holy land."[196] However, he also accused the Saudis of collaboration, writing "instead of motivating the army, the guards, and the security men to oppose the occupiers, the regime used these men to protect the invaders, further deepening the humiliation and the betrayal."[197]

The focus on the United States, and narrative of persecution at the hands of non-Muslim governments, helped unite various adherents of the jihadist ideology and catalyze the larger movement. Individual groups could put aside their doctrinaire religious disagreements and specific local political aims and unite behind the general goal of resisting the global conspiracy against Islam. Furthermore, explaining the misfortunes of local jihadist organizations as the product of a concerted effort by the world's most powerful states absolved those organizations of blame. The decisions of various regional groups to adapt the al Qaeda moniker, as well as Zawahiri's formal incorporation of Egyptian Islamic Jihad into al Qaeda, demonstrate the appeal of bin Laden's unifying idea.

In public statements, especially post-9/11 addresses intended for a global audience, bin Laden calmly laid out his arguments in the manner of a statesman. For example, in a videotaped message delivered to al Jazeera in October 2004, bin Laden explained that al Qaeda targeted the United States because of its support for Israel's 1982 invasion of Lebanon and other aggressive actions that resulted in the deaths of innocents. Portraying September 11th as self-defense, bin Laden spoke directly to the American people, saying that "your security is in your own hands. Any nation that does not attack us will not be attacked." Asserting the political nature of his cause, bin Laden asked "contrary to what Bush says and claims – that we hate freedom – let him tell us then, 'Why did we not attack

[195] Bergen, *The Longest War,* pp. 23-24.
[196] Bin Laden, "Declaration of War against the Americans Occupying the Land of the Two Holy Places."
[197] Ibid.

Sweden?'"[198] Bin Laden surely knew that multiple audiences would hear this message and aimed his arguments at supporters as well as opponents. The speech both threatens and extends an offer of peace to Americans, reassuring supporters that they are not fanatics, nihilists, or crazy conspiracy theorists, but rational actors responding to aggression.

The jihadist thinker who most clearly articulates the vision of a global resistance movement goes by the nom de plume Abu Musab al Suri. His manifesto, *The Global Islamic Resistance Call*, published online in January 2005, critically evaluates the history of the jihadist movement and proposes a strategy based on decentralized cells linked primarily by shared sympathy and ideology. Al Suri argues that "al Qaeda is not an organization, it is not a group, nor do we want it to be. It is a call, a reference, a methodology." Bin Laden's organization, therefore, would only be "a stage in the development of the worldwide Islamist uprising."[199]

Al Suri's writings demonstrate a forward looking understanding of the movement's strategic situation and the appeal of information technology. He openly criticized bin Laden for relying on geographically fixed training camps that could be hit with guided missiles, as was the case in response to the 1998 embassy bombings. By contrast, al Suri's doctrine calls for autonomous cells without overt bases or traceable organizational ties.[200] He sees the internet as essential to cultivating the group consciousness necessary for autonomous cells to operate with a shared grand strategy, and his ideas are accordingly popular in the online forums that terrorism analyst Thomas Hegghammer calls the "town square of" jihadism.[201] Al Suri's writings are featured on the website of the Global Islamic Media

[198] "Bin Laden: 'Your security is in your own hands.'"
[199] Lia, *Architect of Global Jihad*, p. 7.
[200] Ibid., p. 6.
[201] Gardner, "The growth of 'online jihadism.'"

Front, one of the largest online distributors of jihadist works, and have been downloaded tens of thousands of times from the online library known as the Pulpit of Monotheism and Jihad.[202]

In addition to advocating a decentralized strategy, al Suri is a vocal proponent of weapons of mass destruction. This comes from an understanding of the disadvantages associated with an asymmetry of resources and the ability of WMD to provide a partial equalizer. In "The Muslims in Central Asia and the Coming Battle of Islam," al Suri writes that "the difference in armament and number between Muslims and their enemies, between the oppressed and the strong has never been larger... The military logic shows us that it is almost absurd to launch a classical confrontational war to restore the balance of power." Therefore, he argues that jihadists "must attempt to acquire weapons of mass destruction (nuclear, biological, bacteriological) in exactly the same way as the aggressive oppressive world represented by the Jews and the West possess these weapons."[203] While radical clerics have issued fatwas providing religious justification for WMD use against non-Muslim civilians,[204] al Suri emphasizes the strategic logic of WMDs as a force equalizer. Additionally, if those responsible for a WMD attack follow al Suri's advice and avoid revealing themselves as much as possible while shunning fixed training camps, efforts to deter or retaliate against them would be especially difficult. Both deterrence and retaliation require known targets.

Al Suri thus represents the next generation of jihadist thinkers, who see al Qaeda more as an idea than an organization. His strategy is that of global insurgency, mixing in elements of localized insurgency and irredentist conflict with an online community of loosely connected autonomous cells to create a transnational resistance network. Eliminating this diffuse movement will be difficult, but the decentralization will limit its ability to concentrate power. Given the resources and expertise necessary to construct, acquire, or operate working weapons of mass destruction, al Suri's visions of a loosely

[202] Lia, *Architect of Global Jihad*, p. 15.
[203] Quoted in Lia, *Architect of Global Jihad*, p. 307.
[204] Al Fahd, "The Legal Status of Using Weapons of Mass Destruction against Infidels."

connected network of autonomous cells and an al Qaeda armed with WMDs are somewhat contradictory.

The Global Jihadist Network

The various organizations and individuals united by this ideology function similarly to a network of issue activists. In *Activists without Borders*, political scientists Keck and Sikkink define a transnational advocacy network as a collection of "actors working internationally on an issue, who are bound together by shared values, a common discourse, and dense exchanges of information and services."[205] Similarly, the international jihadist movement does not need to be centrally controlled to act as a transnational network. Like groups of activists, jihadists are committed to a common cause and share information to help each other advance the cause with separate actions.

This can be seen in the pattern of post-September 11th suicide bombings. The worldwide incidence of suicide attacks has skyrocketed since 2001, especially in the Middle East and South Asia. There were four times as many suicide bombings from September 11, 2001 through the end of December 2005 than in the entire period from 1968 through September 10, 2001. Individuals espousing jihadist ideology are responsible for more than 85% of the suicide attacks in the 21st century, but few belonged to the same organization or received direction from the same leaders. As Scott Atran argues, "most suicide terrorists today are inspired by a global jihadism which, despite atavistic cultural elements, is a thoroughly modern movement, filling the popular political void in Islamic communities left in the wake of discredited Western ideologies co-opted by corrupt local governments."[206]

In line with al Suri's vision, numerous jihadist groups now consider themselves branches or affiliates of al Qaeda. A committee established by the UN Security Council to sanction "individuals,

[205] Keck and Sikkink, *Activists without Borders,* introduction.
[206] Atran, "The Moral Logic and Growth of Suicide Terrorism," p. 139.

groups, undertakings and other entities associated with Al-Qaida," lists 224 individuals and 64 separate groups as of July 11, 2013.[207] Among the largest groups are the Organization of al Qaeda in the Islamic Maghreb (North Africa), which changed its name from the Salafist Group for Preaching and Combat in 2007 and primarily seeks to overthrow the governments of Algeria and Mali; Jemaah Islamiyah, a group based in Southeast Asia responsible for the October 12, 2002 bombing of a Bali nightclub that killed 202 and injured an additional 204, for which they received funding from bin Laden's group; Lashkar e Taiba, the group primarily based in Kashmir that attacked Mumbai in 2008; the Islamic International Brigade, which fights Russia in the Caucuses; al Shabaab, which controls part of Somalia and officially joined al Qaeda in 2012; al Qaeda in Mesopotamia (Iraq); al Qaeda in the Arabian Peninsula; and others. Most of these groups focus on a particular country or region, acting as localized insurgents or irredentists; but all of them espouse a jihadist ideology, and inspire, advise, and occasionally assist each other.

However, sharing an ideology does not mean they agree on tactics. For example, al Qaeda in Mesopotamia, which was founded as Jamaat al Tawhid wal Jihad by the Jordanian Abu Musab al Zarqawi, gained notoriety for brutal attacks against Iraqi Shiites in an attempt to stoke an Iraqi civil war. Concerned that Zarqawi's videotaped beheadings harmed al Qaeda's reputation, Ayman al Zawahiri wrote Zarqawi a letter asking him to change his methods. After praising the efforts of al Qaeda in Mesopotamia and stressing the importance of the Iraqi theater to the global jihadist cause, Zawahiri wrote "if we look at the two short-term goals, which are removing the Americans and establishing an Islamic amirate in Iraq, or a caliphate if possible, then, we will see that the strongest weapon which the mujahideen enjoy – after the help and granting of success by God – is popular support from the Muslim masses in Iraq, and the surrounding Muslim countries."[208] Zarqawi did not

[207] "Al-Qaida Sanctions List."

[208] "Letter from al-Zawahiri to al-Zarqawi."

heed this request, continuing to alienate Iraqis by bombing and beheading Shia Arabs, and directing three simultaneous suicide attacks at hotels used by foreign diplomats in Amman, Jordan on November 9, 2005. The attacks killed 60 people and injured 115 more, including many attendees of a Palestinian wedding, among them the fathers of both the bride and groom.

This incident illustrates the difficulty of coordinating actions across various nodes of the network and how that can be detrimental to the movement's grand strategy. While Zawahiri emphasized the necessity of popular support, Zarqawi seemed motivated primarily by hatred for Shiites and his native Jordan. Popular revulsion at Zarqawi's tactics likely contributed to many Iraqi insurgents' and their supporters' decision to turn on al Qaeda in Mesopotamia, including the Sunni Arab tribal leaders behind the Sons of Iraq. Beginning in 2005, these militias began fighting against al Qaeda and working to stabilize as part of a movement known as the Sunni Awakening.

While most al Qaeda affiliates focus on local conflicts, al Qaeda in the Arabian Peninsula (AQAP) has attempted attacks against the United States in addition to pursuing an irredentist conflict against the governments of Yemen and Saudi Arabia. AQAP recruited Umar Farouk Abdulmutallab, the son of a prominent Nigerian banker, and sent him to blow up a passenger jet bound for Detroit on December 25, 2009 with the plastic explosive PETN sown into his underwear. The "underwear bomber" failed to ignite the explosives properly and was subdued by passengers.[209] AQAP attempted a larger attack using PETN in October 2010, hiding the explosive in printer cartridges placed in packages in the cargo container of two passenger jets bound for the United States. Officials from the United Arab Emirates and United Kingdom discovered the packages when the planes stopped, respectively, at Dubai International and East Midlands airports. The bombs were designed to explode in midair when the planes were close to landing, destroying the aircraft and raining debris down on a major US city,

[209] "FACTBOX-Al Qaeda's Yemen-based wing."

possibly Chicago.[210] Though unsuccessful, these instances demonstrate that attacks on Western cities could come from any ambitious jihadist group, even one focused on an insurgency against a local government.

AQAP also played a role in inspiring self-starters in the United States. Anwar al Awlaki, an American imam who preached a fundamentalist ideology at mosques in the US and then UK, moved to Yemen in 2004 and became a prominent member of al Qaeda in the Arabian Peninsula. Awlaki maintained an active presence online, posting sermons and writing a blog that advocated anti-American violence, frequently in English. The most popular sermons received over 40,000 views on YouTube.[211]

Awlaki offered his email address to his online followers. Among those who contacted him was Nidal Malik Hasan, a US Army medical officer who practiced psychiatry. Awlaki and Hasan exchanged at least 18 emails before Hasan shot and killed 13 while injuring an additional 29 at Fort Hood in Texas on November 5, 2009, due to anger over the US military presence in Iraq and Afghanistan. While AQAP recruited and sent the underwear bomber, Awlaki did not instruct Hasan to attack; Hasan's questions in the emails were found to be consistent with his psychiatric research.[212] Rather, Awlaki's message inspired Hasan to come up with the attack himself.

Other self-starters include Faisal Shahzad, who tried and failed to set off a car bomb in Times Square on May 1, 2010, and claimed to be influenced by Awlaki's sermons and writing, though the two did not have direct contact.[213] Bilal Abdullah, a British-born doctor of Iraqi decent, crashed a Jeep loaded with propane canisters into Glasgow International Airport on June 30, 2007 in an “al Qaida inspired” attack that only managed to kill his driver.[214] More recently, Tamerlan Tsarnaev, who, along with his brother Dzhokhar, killed three in the Boston Marathon bombing on April 15, 2013, followed

[210] “Parcel bomb plotters 'used dry run,' say US officials.”
[211] Madhani, “Cleric al-Awlaki dubbed 'bin Laden of the Internet.'”
[212] Egerton, “Imam's e-mails to Fort Hood suspect Hasan tame compared to online rhetoric.”
[213] Dreazen and Perez, “Suspect Cites Radical Imam's Writings.”
[214] “Hospital staff stunned as doctors are questioned.”

the video postings of Gadzhimurad Dolgatov, a Dagestani jihadist who went by Abu Dujana.[215] These self-starters were inspired by jihadist ideology, and tried to attack Western targets despite never receiving training or instructions from a terrorist organization, demonstrating the reach of the global jihadist network.

This interpretation runs the risk of conflating disparate threats into a single entity. The various organizations and self-starters who consider themselves part of a global jihadist movement may act like a loosely connected activist network, but they do not receive central direction and many of the groups and individuals never communicate or come into contact with each other. Therefore, those who compare the fight against jihadism to the Cold War against communism are making both an analytical and strategic error. As John Nagl put it, “we are facing a number of different insurgencies around the globe—some have local causes, some of them are transnational. Viewing them all through one lens distorts the picture and magnifies the enemy.”[216]

Nevertheless, as al Suri envisioned, a network of autonomous cells is carrying on the jihadist mission. They are not centrally controlled and some of them are just localized insurgencies or irredentists that use the al Qaeda moniker. However, many operate transnationally, and some pose a threat to the US, UK, and other Western countries. Organized groups, like al Qaeda in the Arabian Peninsula, and self-starters, like the Boston Marathon bombers, will continue planning attacks in the name of the global jihadist movement, threatening local governments and civilians, as well as the soldiers, government officials, and civilians of distant powers.

[215] Dewey, “The obscure Russian jihadist whom Tamerlan Tsarnaev followed online.”
[216] Quoted in Wilson and Kamen, “'Global War on Terror' Is Given New Name.”

Conclusion

The al Qaeda organization suffered a number of serious, possibly fatal blows. Many members have been killed, and the rest are on the run. By most accounts, Zawahiri lacks bin Laden's charisma, and has been unable to reconstitute the organization. However, the international jihadist cause al Qaeda championed shows no sign of disappearing. This global activist network of organizations and individuals is adaptable and resilient. Due to the limited size of each node and a lack of coordination between them, this network will continue to have difficulty concentrating power. However, it is likely to remain at least a low-level threat for the foreseeable future.

Part 2:

Robotics

Chapter 4: Asymmetric Warfare and the Robotics Revolution

This dissertation presents a cyclical theory of international asymmetric warfare, in which non-state networks adapt more quickly than powerful states to systemic technological or geopolitical change. States are larger, more bureaucratic organizations, with more permanence and inertia; they thus experience an institutional drag that can delay adaptation to external change, especially in the absence of a pressing need, such as an existential threat from a rival great power. This creates a window in the wake of major shifts in the global system in which non-state networks capable of threatening great powers can spring up before the states fully adapt. However, given time, powerful states can marshal their resources and reduce the asymmetric threat by producing technological, strategic, and political advancements.

In the post-Cold War world, the prevailing international system is a global, near-universal, commercial alliance among states, featuring eight nuclear powers.[217] As long as they remain at peace with each other, communicating, trading, and participating in international institutions, the greatest threat to nuclear states individually, and the international system as a whole, is disruption by non-state networks. Many networks fighting irredentist conflicts and localized insurgencies adapted quickly to the information age, enhancing their capabilities by utilizing new communications technologies. Additionally, the internet and global media created an environment in which globalized insurgency is possible; while the political, economic, and cultural changes associated with globalization motivate some individuals to violently resist the international order.

[217] US, Russia, UK, France, China, India, Pakistan, and Israel. Does not include states that possess nuclear technology, but lack nuclear weapons. Also does not include North Korea, because its estimated stockpile of nuclear weapons is less than 10, and, unlike the other nuclear weapons states, it lacks the missile technology to strike from distance.

States have responded to these challenges by gradually adapting to the information technology-enhanced strategies and transnational nature of many 21st century non-state networks, especially al Qaeda and its affiliates. National security and intelligence agencies share more information with each other, track and freeze financial transfers used to support terrorist and insurgent organizations, and monitor their websites. These efforts demonstrate states' ability to marshal their resources to counter threats enabled by technological shifts. However, while new technologies create new capabilities and strategic opportunities, the dynamic often works in reverse, with strategic need driving technological change.

States, unlike networks, possess the resources necessary to drive technological advancement. While networks may adapt more quickly, and design idiosyncratic strategies in response to major shifts in the technological environment, they cannot possibly afford long-term research programs or production facilities for high-tech inventions. Therefore, developing new technologies is a significant way for states to utilize their resource advantage to counter the threat posed by non-state networks. This inherently takes more time than developing new ways to utilize existing, commercially available technology, but has the potential to provide longer lasting, more decisive benefit.

To counter the asymmetric threat from non-state networks in the 21st century, the world's most powerful states should and will direct an increasing amount of security resources to robotics and automated systems. Robots are machines that can perceive their surrounding environment and recognize changes in it, process this information and make decisions in response, and act upon the external environment without constant human direction.[218] By contrast, a computer can processes information and choose among options, but not act upon the surrounding physical environment, while a non-robotic machine can change its external environment, but does not make decisions. Robots come

[218] See Finkelstein, "Military Robotics: Malignant Machines or the Path to Peace?" p. 5-6, for a more technical version of this definition.

in many types, ranging from fairly simple varieties that perform repetitive tasks on factory assembly lines, to complex aircraft that can autonomously survey a large area and fire missiles at a target. All technologically advanced militaries now utilize automated systems, which demonstrates the widespread belief in their usefulness.[219]

As the robotics revolution continues to advance, it will likely have an increasing impact on strategies of asymmetric warfare. Whereas internet-era communications technology can enhance non-state networks' capabilities by increasing their ability to exploit the non-material asymmetries in which they have an inherent advantage, advancements in robotics and information processing have the potential to help states reduce weak actor advantages derived from non-material asymmetries, especially information, resolve, and responsibility. Using robots, advanced militaries can gather and process more information, risk fewer lives, and protect more locations than with human soldiers alone.

Robots and the United States Military

As the most advanced military in the world, with an annual budget greater than all other nuclear powers combined,[220] the United States has prioritized robotics. Responding to Congressionally mandated austerity and the winding down of wars in Iraq and Afghanistan, the Department of Defense released a document in January 2012 outlining a 22% reduction in total defense expenditures from the 2010 peak.[221] All of this reduction comes from personnel and manned systems; the budget protects or increases funding for unmanned platforms. The new budget projections reduce active army personnel from 570,000 to 490,000, and reduce active Marine personnel from 202,000 to 182,000, while retiring and divesting planes designed to airlift troops.

[219] Rawnsley, “It's a Drone's World. We Just Live in it.”
[220] SIPRI Military Expenditure Database.
[221] “Defense Budget Priorities and Choices.”

This reduction in ground capacity and mobility could be expected following the end of two foreign occupations, but the budget reduces manned naval and aerial capacity as well. It retires seven Navy cruisers early, while removing two Littoral Combat Ships and eight Joint High Speed Vessels from future acquisition plans. Additionally, it recommends disestablishing six (out of 60) Air Force tactical fighter squadrons. However, the new budget funds the equipment and personnel necessary for 65 Predator and Reaper drone patrols, "with a surge capacity of 85," up from the 2011 total of 61. It also protects or increases the funding for Gray Eagle, the Army's unmanned air system, and "sea-based unmanned intelligence, surveillance and reconnaissance (ISR) systems such as Fire Scout," all in the name of "counter-terrorism operations."[222] This is consistent with personnel training over the last few years; since 2009, the Air Force has trained more pilots to fly unmanned aircraft than manned fighters and bombers combined.[223] DoD's priorities are clear: over the next decade, the United States military will become a more roboticized force.

Advances in robotics, along with developments in computing—namely, increased networking, information processing, and cyber capabilities—have the potential to grant the US military significant strategic advantages. While robots undoubtedly would be useful in the event of a relatively symmetric interstate war, their effect on international asymmetric warfare will be more immediately dramatic. Other powerful states are also developing robotic military technology, and no developments appear likely to overthrow the nuclear balance in the near future. Non-state networks, however, lack the resources to develop or acquire advanced automated systems, and new innovations in unmanned technology have already made significant contributions to America's counterinsurgencies in Iraq and Afghanistan, and in the global conflict against al Qaeda.

[222] "Defense Budget Priorities and Choices," p. 10.
[223] Pincus, "Air Force to Train More Remote than Actual Pilots."

Robots in Combat

In the 21st century, robots have taken on more combat-related tasks, including some of the most dangerous. With mobile machines of various shapes and sizes turning corners and entering rooms ahead of soldiers, removing wounded troops from combat zones, and searching roads for explosives ahead of human-carrying vehicles, powerful militaries can undertake risky missions with less risk to soldiers' safety. Fewer casualties decreases a major source of the strong actor's political costs of war, making the asymmetry of resolve less of an advantage for weak actors. This undermines weak actors' primary strategy in localized insurgencies, in which protracted war and steadily mounting costs create political disputes within strong actors that eventually lead them to abandon the conflict. For example, the American anti-war movement in response to the protracted conflict in Vietnam would almost certainly have been weaker if American casualties were significantly lower, with robots reducing the need for a draft.

In the United States, as with other countries, public support for a given conflict tends to decrease as casualties rise, with the notable exception of wars against perceived existential threats, such as World War II.[224] Along these lines, it is unsurprising that approval ratings for the war in Afghanistan have steadily decreased, from 90% approving at the start in 2001, to slightly over half of those polled approving in the mid-2000s, to only 36% approving in 2011.[225] Meanwhile, American casualties rose from an annual average of 50 from 2002-2004, to 104 from 2005-2007, and then as high as 499 in 2010 and 418 in 2011.[226]

By contrast, approval for attacks from unmanned aerial vehicles (UAVs) has remained high among Americans. A Washington Post-ABC news poll conducted in February 2012 found that 83% of

[224] Mueller, *War, Presidents, and Public Opinion*.

[225] Data an average of polls from Gallup, CNN and Opinion Research Corporation, and Fox News and Opinion Dynamic. See: Wayner, “American Approval Rating (Percent) of War in Afghanistan.”

[226] Data from “Operation Enduring Freedom” at *iCasualties.org*.

Americans approve of “the use of unmanned 'drone' aircraft against terrorist suspects overseas.”[227] The 2012 “Global Attitudes Survey,” released by the Pew Global Attitudes Project in June 2012, found majorities from most countries disapproving of American drone strikes, with the notable exception of the United States, where 62% of respondents approved and only 28% disapproved.[228] The gap in the two surveys most likely reflects the specific language of each question—the Washington Post-ABC News poll specified drones strikes against “terrorist suspects overseas” while the Pew survey did not use the word “terrorist”—rather than a significant drop in approval over a few months. Regardless, both of these polls demonstrate that a solid majority of Americans support the use of drone strikes, and that millions of Americans who oppose the war in Afghanistan nevertheless support continuing the campaign of UAV attacks there and elsewhere.

This indicates that the American public supports the use of force against suspected members of terrorist and insurgent organizations, except when the effort results in mounting American casualties. Therefore, with an increasingly roboticized military, the United States will be increasingly able to use force abroad without generating much public disapproval at home. This will make America, and other powerful states that utilize drones and other unmanned military platforms, less vulnerable to the Maoist strategy of protracted war, while also raising ethical questions regarding the ease with which governments are willing to use force absent potential public disapproval.

Ground-based Robots

Aerial drones get the most publicity, but ground-based robots are revolutionizing 21st century warfare as well. Whether rolling around on wheels or treads, or, in a recent development, walking around on legs, unmanned ground-based systems can enhance the capabilities of soldiers in the field.

[227] “Washington Post-ABC News Poll,” February 4, 2012.

[228] “Drone Strikes Widely Opposed, Global Opinion of Obama Slips, International Policies Faulted,” *Pew Global Attitudes Project*.

As of early 2013, the United States has developed or acquired robots that can remove wounded troops from battlefields, carry supplies over difficult terrain, detect and remove explosives, shoot firearms with precision, knock mortars and rockets out of the sky, and locate the origin of gunfire. Many of these have already been utilized successfully in active combat theaters.

The US government has awarded numerous grants to developers of semi-autonomous robots for non-killer tasks. For example, the Battlefield Extraction-Assist Robot, or BEAR, from Vecna Robotics, is designed to carry wounded soldiers to safety without risking others' lives. It can lift up to 500lbs, navigate uneven terrain, climb stairs, and autonomously determine how best to lift objects of various shapes and sizes.[229] The BEAR was invented in 2005, and Vecna received a grant in excess of $1 million from the US Congress to further its development in 2007. As of late 2012, it is undergoing testing at the US Army Infantry Center Maneuver Battle Lab at Fort Benning, where soldiers are growing accustomed to its glove-controller, which recognizes hand gestures, and developing tactics for extracting wounded soldiers in simulated battle conditions.[230]

Another large ground robot currently undergoing testing is the Legged Squad Support System (LS3) from Boston Dynamics, known as the BigDog, which acts as a robotic pack mule. Unlike the BEAR and most other ground-based robots which move around on wheels or treads, the BigDog walks on four legs, allowing it to traverse more difficult terrain. With a variety of sensors, a gyroscope, and an on-board computer constantly making adjustments, the robot maintains its balance much like a person or an animal. In demonstration videos, it slips on ice and regains its balance without dropping any of its cargo, all without human assistance.[231] By absorbing the shock of the impact of each leg

[229] See Atwood and Klein, “Vecna's Battlefield Extraction-Assist Robot BEAR,” or “High Performance Hydraulics for Industrial Applications.”

[230] Ruppert, “Battlefield Extraction-Assist Robot to Rescue Wounded on Battlefield.”

[231] “BigDog Overview.”

with the ground, it can recycle some energy from one step to the next, extending operating time between charges.

The LS3 is about 3 feet long, 2.5 feet tall, weighs 240lbs, and looks eerily like a headless four-legged animal. In separate tests, the BigDog demonstrated that it can run at 5 mph, climb slopes up to 35 degrees, walk across rubble, through mud, snow, and water, and carry a maximum load of 340 lbs.[232] It also has the ability to follow a human leader without directional input, and, in 2013, Boston Dynamics added a robotic arm which is capable of lifting (and throwing) heavy objects such as cinder blocks.[233] Funded by the Defense Advanced Research Projects Agency (DARPA), the BigDog began undergoing military tests in 2012, and could be deployed as early as 2014. In video from tests in the summer of 2012, the LS3 prototype demonstrates that, if knocked down, it can automatically right itself, stand up, and continue walking. Early versions were noisy, but the latest prototype is “roughly 10 times quieter than when the platform first came online, so squad members can carry on a conversation right next to it, which was difficult before,” according to DARPA program manager Lt. Col. Joe Hitt.[234] A robotic pack mule like the BigDog would allow soldiers to bring heavier equipment into rougher terrain, and lighten the load carried on their backs, making them simultaneously more mobile and better equipped.

Currently, the United States and other advanced militaries make extensive use of smaller, multipurpose robots, like the PackBot by iRobot, which looks like a camera and robotic arm mounted on a series of treads. Over 2,000 PackBots have been deployed to Iraq and Afghanistan, where they enter buildings or peer around street corners ahead of soldiers, reducing the risk to personnel.[235]

[232] “BigDog – The Most Advanced Rough-Terrain Robot on Earth.”
[233] “Dynamic Robot Manipulation.”
[234] Pfeiffer, “DARPA Unveils Robotic Mule.”
[235] “Ground Robots – 510 PackBot.”

Weighing approximately 7 to 18 kilograms—give or take, depending on accessories—the PackBot can be carried in a backpack (hence the name).

Most importantly, PackBots can detect and dispose of explosives, especially improvised explosive devices (IEDs). Of 2,617 International Security Force fatalities in Afghanistan from October 2001 through the end of 2012, 1,337 have been due to IEDs, for a total of 51.09%. However, the percentage has steadily declined, from a peak of 60.98% (of 451) in 2009 to 58.41% (of 630) in 2010, 51.22% (of 492) in 2011, and 42.31% (of 312) in 2012.[236] Part of this decline may be due to shifting insurgent and counter-insurgent tactics, but a significant portion is likely due to deployment of the PackBot 510 EOD model beginning in late 2007. EOD stands for Explosive Ordinance Disposal, and the new model can drag larger objects and lift up to 13.6kg with its arm in a compact position and 4.5kg with its arm extended, twice the capability of its predecessors, with a grip that is three times as strong.[237] Additionally, these robots feature “Fido” sensors that can detect explosive vapors on a level comparable to highly-trained bomb sniffing dogs.[238]

The decline in the percentage of coalition casualties caused by IEDs coincides with the deployment of thousands of EOD robots, beyond the 2,000-plus PackBots deployed to Afghanistan and Iraq. The larger Talon robot, developed by Foster-Miller and produced by QinetiQ, weighs approximately 52 to 71 kilograms, depending on accessories, and includes chemical, gas, temperature, and radiological sensors. With its larger size, the Talon is less portable that the PackBot, but features a more powerful robotic arm, capable of manipulating heavier objects, dragging up to 113kg, and lifting up to 34kg with its arm retracted and 13kg when extended.[239] As of the beginning of 2012, Talon's

[236] “Operation Enduring Freedom,” iCasualties.org.
[237] “iRobot PackBot 510 with Engineer Kit.”
[238] “PackBot Tactical Robot.”
[239] “Talon Specifications.”

makers boast of “more than 20,000 successful EOD missions in Iraq and Afghanistan.”[240] The Talon, PackBot, and other robots with explosive ordinance disposal capabilities—such as the Wheelbarrow bomb disposal robot, made by Northrup Grumman primarily for the United Kingdom, and the tEODor, made by Cobham primarily for the Spanish Armed Forces—reduce the ability of weak actors to injure or kill strong actors' soldiers, thereby weakening their overall strategy. Less fear of IEDs allows military units to advance further and faster, while decreasing the rate at which strong actors' accrue costs in prolonged conflicts.

In addition to planted explosive devices, automated systems help protect soldiers against explosive projectiles. After IEDs, some of the most successful insurgent weapons against American and allied forces in Iraq and Afghanistan have been rockets and mortars. Insurgents occasionally fire these relatively inaccurate projectiles at US bases from nearby residential neighborhoods, thereby discouraging long-range retaliatory fire. The shooters, therefore, often have time to abandon their location before ground forces can respond, making the possibility of retaliation insufficient to deter rocket and mortar fire. To counter this threat, the Army and Marines have employed Counter Rocket, Artillery, and Mortar technology (C-RAM).[241]

In response to an operational needs statement from the Multinational Corps in Iraq, Raytheon adapted its MK15 Phalanx Close-In Weapons System for land use.[242] Since the 1980s, the US Navy has mounted Phalanxes on ships to protect against anti-ship missiles and aircraft. The system utilizes radar—and, more recently, infrared, and electro-optical sensors—to spot incoming projectiles, and then fires up to 4,500 rounds per minute from a swiveling Gatling gun to destroy them before they can reach the ship. Though attached to a fixed position on various vessels, the Phoenix is considered a robot because it “autonomously perform[s] its own search, detect, evaluation, track, engage and kill

[240] “Armed, Aware and Dangerous.”
[241] Singer, *Wired for War*, p. 38.
[242] “Counter Rocket, Artillery, and Mortar (C-RAM).”

assessment functions."[243] After tests demonstrating a 60-70% success rate in shooting down incoming mortars, the land-based version known as Centurion was first deployed to Iraq in 2005, where it was installed at bases and government installations, including the Green Zone and Camp Victory.[244] Unlike the ship-mounted Phalanx, which uses depleted uranium shells, land-based C-RAMs employ incendiary rounds to avoid civilian exposure to radioactive material, and explode in mid-air to reduce the risk that ammunition that misses the target will harm personnel or civilians.[245] Before deployment, the military required Centurion to demonstrate an ability to neutralize incoming threats while minimizing collateral damage.[246]

While the original Centurion can protect an area of up to 1.2 square kilometers from a fixed position, the latest C-RAM technology aims for greater range, improved tracking, and mobility.[247] In 2010, Raytheon successfully demonstrated a Mobile Land-Based Phalanx Weapon System (MLPWS). This mobile C-RAM system, mounted on the back of a heavy tactical truck, met the 60-70% success rate of its stationary antecedent while maneuvering through 28 miles of paved and off-road conditions.[248] It could provide useful protection against mortars and rockets to mobile convoys, reducing the threat of ambushes, and also rapidly provide C-RAM defense to forward positions.

An alternative C-RAM system, which boasts a greater success rate against mortars and rockets, was recently developed by Rheinmetall for the German military to protect bases in Afghanistan. The Modular Automatic and Network capable Targeting and Interception System, or MANTIS for short, was first deployed in 2011, and includes six 35mm automatic guns, two sensor units capable of recognizing approaching missiles from 3km, and a ground-based control unit. Instead of hurling a hail of bullets at incoming projectiles, the system fires air-burst shells that separate into 152 tungsten

[243] "MK 15 – Phalanx Close-In Weapons System (CIWS)."
[244] "Counter Rocket, Artillery, and Mortar (C-RAM)."
[245] Singer, *Wired for War*, p. 38.
[246] "Counter Rocket, Artillery, and Mortar (C-RAM)."
[247] "A Laser Phalanx?"
[248] "Raytheon's Mobile Land-Based Phalanx Weapon System Completes Live-Fire Demonstration."

projectiles, each of which weigh 3.3 grams. The central control unit analyzes information from the sensors to determine the flight path and velocity of incoming targets, and then programs the ammunition using an electronic timer. When the MANTIS' ammunition approaches its target, it bursts into a metal cloud obstructing the projectile's flight path, which increases the chances that it will destroy the incoming rocket or mortar compared to other land-based C-RAM systems. The entire process—detection, analysis, counter-fire—takes approximately 4.5 seconds.[249]

To improve range and reduce operating costs, Raytheon is developing a variant of the Phalanx that would use lasers instead of bullets. By using a focused fiber-optic beam, a C-RAM system could triple the range of earlier models and eliminate the cost of ammunition. However, despite successful tests at shorter distances, in which a laser-based C-RAM destroyed incoming 60mm mortars at 550 yards, numerous technical problems remain. Lasers require considerable power to operate, and sometimes have difficulty maintaining full strength in unfavorable weather conditions, such as fog or rain. The delicate technology may degrade from exposure to salt spray at sea, or sand in deserts, and destroying targets with lasers at a greater distance creates additional risk of collateral damage. Unlike incendiary shells, which detonate after a set distance, lasers could go through the target, creating a risk for friendly or civilian aircraft in the area.[250]

Minimizing civilian casualties is essential for C-RAM to provide strategic value in asymmetric warfare. If insurgents fire mortars or rockets from populated areas, and the C-RAM system knocks the projectiles out of the air without destroying them, they could harm civilians or destroy civilian property. From the insurgents' prospective, both outcomes are strategically beneficial: either the projectile gets through the C-RAM defenses and has the opportunity to strike counterinsurgent soldiers or equipment, or the C-RAM knocks down the projectile in a civilian area, potentially angering the

[249] "NBS MANTIS Air Defense Protection System, Germany."
[250] "A Laser Phalanx?"

population against the counterinsurgents. Both exploit the asymmetry of resolve, as they impose costs on the strong actor and motivate the weak actor. By contrast, a C-RAM system that protects soldiers without causing harm to local civilians benefits strong actors by reducing the asymmetry of resolve from both directions.

Unsurprisingly, in addition to those that to protect soldiers and save lives, some modern military robots possess offensive capabilities. The Special Weapons Observation Reconnaissance Detection System, or SWORDS, is a weapons system that can be mounted on a Talon robot. SWORDS replaces Talon's gripping arm with a gun mount that can hold any weapon weighing less than 300lbs, including an M-16, a .50-caliber machine gun, an antitank rocket launcher, or a 40mm grenade launcher.[251] In testing, it directly hit bull's-eyes up to 2,000 meters away every time it was fired from a stationary position.[252]

The robot achieves greater accuracy than even the best human snipers by eliminating human error. A Talon does not breathe, react to surprises, fear counter-fire, or depend on muscle control, thus providing a more stable platform for weapons than any person could. Furthermore, the SWORDS system matches its zoom lens camera to a weapon's optics, allowing soldiers to see exactly what the weapon is looking at on a monitor, instead of needing to align their eye with the gun sight.[253] Therefore, by using robots instead of human soldiers on the front lines in uncertain, dangerous situations, like urban warfare against an insurgency, strong actors not only reduce the risk to their soldiers, but could reduce collateral damage as well.

Futuristic developments over the next decade or two will likely produce ground-based robots increasingly capable of combat-related tasks traditionally handled by human soldiers. As of 2012, unmanned ground systems can carry supplies, remove wounded soldiers from the battlefield, pick up

[251] Singer, *Wired for War*, p. 30.
[252] “Armed Robots March into Battle.”
[253] Singer, *Wired for War*, p. 31.

smaller items, dispose of explosive ordinance, and fire weapons at a target. Soon, these functions will be joined by hunter-killer robots designed to track down and incapacitate human targets.

Adapting the BigDog's ability to walk on legs, Boston Dynamics created an anthropomorphic two-legged robot called PETMAN. It is human-sized and shaped, and can walk, twist, squat, and do push-ups. The company currently sells PETMAN as “an anthropomorphic robot for testing chemical protection clothing.”[254] By moving like a person and simulating human physiology, “controlling temperature, humidity and sweating when necessary,”[255] the PETMAN can provide realistic conditions for testing protective clothing.

Even though the PETMAN looks eerily like a prototype of the hunter-killer robot from the movie *Terminator*, humanoid robot soldiers are likely still a long ways off.[256] PETMAN can walk on a treadmill and return to its original path when pushed, but it cannot move as smoothly or as quickly as a person. On video, its jumping-jacks and push-ups appear stunted, and it lacks the ability to rapidly switch motions, such as from walking to crawling.[257] More importantly, no currently designed robot possesses anywhere near the adaptability or decision-making capabilities of human beings. With engineering improvements, a humanoid robot could move faster or more smoothly than the current incarnation of the PETMAN, but the lack of high-functioning artificial intelligence means that human soldiers are in no danger of being replaced by robots in the near future.

However, the ideal hunter-killer robot to assist human soldiers in a limited task may not be humanoid. In the *Terminator* movies, the robot resembles a person because it aims to infiltrate human society and track down a specific target. It looks human to avoid detection, and interacts with people to acquire information. Appearing and acting indistinguishable from a real person is far beyond the

[254] “PETMAN – BigDog Gets a Big Brother.”
[255] Ibid.
[256] Yirka, “Makers of infamous BigDog robot unveil human version.”
[257] “PETMAN – BigDog Gets a Big Brother.”

capabilities of current robotic technology, and human soldiers will remain central to military tasks, especially the population-interaction elements of counterinsurgency, for the foreseeable future. However, a ground-based hunter-killer robot could help human soldiers catch a fleeing suspect.

In pursuit of this goal, DARPA granted a contract to Boston Dynamics to adapt the BigDog into a cheetah-like robot that can track down human prey. Like the BigDog, the Cheetah-bot stands on four legs, but the aim is to create a faster, more agile robot capable of making tight turns so that it "can zigzag to chase and evade."[258] It could have non-combat uses as well. For example, DARPA and Boston Dynamics foresee this fast, four-legged robot assisting rapid emergency response teams, reaching victims of a fire or vehicular accident before human first responders. In a 2012 demonstration, the Cheetah-bot reached a maximum speed of 28.3 mph galloping on a treadmill, which is faster than Olympic sprinters.[259]

As ground-based robots increasingly protect soldiers from hostile fire and take on some of the most dangerous combat-related tasks, including battlefield extraction, explosive ordinance disposal, and front-line advancement on enemy positions, the ability of weak actors to kill strong actor soldiers will likely decrease. With fewer soldiers returning home in body bags, strong actors would face less domestic political pressure to negotiate unfavorable settlements or abandon protracted conflicts. Additionally, the increased precision of robot-fired weaponry could decrease civilian casualties without reducing military effectiveness. By shooting more accurately and never acting out of fear for their own safety, robots like the SWORDS system or a futuristic hunter-killer could decrease the harm to civilians that fuels both weak actor resolve and political pressure from human rights' groups and antiwar advocates. Therefore, ground-based robots have the potential to increase the likelihood of strong actor

[258] Rawnsley, "Darpa's Cheetah-Bot Designed to Chase Human Prey."

[259] "Cheetah Robot runs 28.3 mph, a bit faster than Usain Bolt."

success in asymmetric conflicts by narrowing the asymmetry of resolve, undermining a key element of weak actor strategy.

Aerial Robots

In addition to ground-based robots, the US military and intelligence community makes extensive use of flying robots known alternatively as unmanned aerial vehicles (UAVs) or unmanned aerial systems (UASs), commonly referred to as aerial drones. Most drone missions involve reconnaissance, but some UAVs, like the Predator and Reaper, use missiles to attack targets on the ground. According to GlobalSecurity.org, there are 77 different UAV models in use, discontinued, or currently in production.[260]

Unmanned aircraft are almost as old as manned airplanes, with the first attempts at remote-controlled planes coming in World War I. The Hewitt-Sperry Automatic Airplane project aimed to create a "flying bomb," and flew the unmanned N-9 model for the first time in 1917. An explosives laden unmanned airplane, the N-9 was more of a precursor to cruise missiles than modern UAVs. The earliest unmanned aircraft using a jet engine, the Firebee by the Ryan Aeronautical Company—which became Teledyne Ryan after a merger in 1969, and was purchased by Northrup Grumman in 1999—first flew in 1955, and was used primarily for training aircraft gunners. Later versions, including the Ryan Lightning Bug, were designed for reconnaissance, and the United States first flew Lightning Bugs in August 1964 to gather information over China and Vietnam.[261]

Expanding UAV use in combat, Israel utilized adapted Firebees as decoys to distract Syrian aerial defenses in the 1973 Yom Kippur War. In 1982, in advance of a strike on Syrian positions in the Bekaa Valley, Israel sent a squadron of UAVs that broadcast signals like regular planes, prompting

[260] "Unmanned Aerial Vehicles."
[261] Wagner, *Lightning Bugs and Other Reconnaissance Drones.*

Syrian anti-aircraft fire. The Israelis then followed with a wave of manned aircraft that destroyed the air defenses using radar frequencies revealed by the anti-aircraft batteries' attacks on the drones.[262]

However, in the Post-Cold War world, UAV use has expanded dramatically, most notably for targeted killings. The Predator drone, manufactured by General Atomics Aeronautical Systems, comes in two versions: the RQ-1 for surveillance and reconnaissance, and the MQ-1, which includes combat capabilities. Operational since 1994, the Predator first flew missions in Bosnia in 1995, in support of forces under the auspices of NATO and the United States.[263] It can fly up to 25,000 feet, and remain in the air up to 40 hours. The original version, used in the former Yugoslavia, was flown remotely by a pilot and sensor operator, sometimes accompanied by payload specialists, sitting in a van near the runway of the drone's operating base. Direct radio signals controlled takeoff and landing, just like a remote-controlled model airplane. Once airborne, communications between UAV and pilot shifted to the military's satellite network, which often caused delays of a few seconds between a pilot's command and the drone's response.[264]

By the beginning of the 21st century, improvements in communications technology allowed pilots to fly unmanned aircraft from thousands of miles away, without noticeable delay. The US has two main UAV programs operating out of two command centers: CIA pilots fly drones from the agency's headquarters in Langley, Virginia, near Washington D.C., while the US military's UAV pilots operate out of Creech Air Force Base in Nevada.[265] Both bases are over 6,000 miles away from Afghanistan, Pakistan, Somalia, or Yemen, where the planes fly and execute various missions, including missile strikes.

[262] Singer, *Wired for War*, p. 56.
[263] "Predator RQ-1/MQ-1/MQ-9 Reaper – United States of America."
[264] Coll, *Ghost Wars*, p. 529.
[265] Pitzke, "How Drone Pilots Wage War."

The Predator was the first UAV to be controlled via satellite data link, the first to support manned aircraft with target laser designation, and the first to fire air-to-ground missiles.[266] As a result, it is also the first flying robot in history to kill a person outside of a war zone. In February 2001, an MQ-1 Predator successfully fired a Hellfire-C laser-guided missile in flight tests at Nellis Air Force Base in Nevada.[267] In November 2002, a CIA-controlled Predator destroyed a jeep in Yemen with a Hellfire missile, killing six men, including Ali Qaed Senyan al Harthi, a member of al Qaeda linked to the bombing of the USS Cole off the coast of Yemen on October 12, 2000.[268] Since then, the MQ-1 Predator—and the Predator B, a successor aircraft also known as the MQ-9 Reaper—have played an increasing role in American counter-terrorism and counterinsurgent efforts.

The Reaper is a larger, more powerful version of the Predator, specifically designed to strike enemy targets. According to Air Force General T. Michael Moseley, "the Reaper represents a significant evolution in UAV technology and employment. We've moved from using UAVs primarily in intelligence, surveillance and reconnaissance roles before Operation Iraqi Freedom, to a true hunter-killer role with the Reaper."[269] First flown in 2001, the Reaper features a 900-horsepower engine, compared to the original Predator's 119hp, and can carry 15 times the ordinance, fly twice as high, and achieve a maximum velocity at least twice as fast as the earlier model.[270] General Atomics is developing an even faster version, the Predator C, or Avenger, which first flew in April 2009, but as of 2012, remains in an expanded test program.[271]

In the 21st century, the United States has increasingly utilized missiles fired from Predator and Reaper drones to strike targets linked to al Qaeda or Afghan insurgent networks. The US does not officially acknowledge these attacks because they are part of a covert program, so there are no publicly

[266] "Predator UAS."
[267] "Predator RQ-1/MQ-1/MQ-9 Reaper – United States of America."
[268] "CIA 'killed al-Qaeda suspects' in Yemen."
[269] Quoted in "'Reaper' moniker given to MQ-9 unmanned aerial vehicle."
[270] "Predator B UAS."
[271] "Predator C Avenger."

available statistics from the American military or intelligence services that oversee the strikes. However, compiling news reports of drone attacks can provide reasonable estimates. From 2004 through January 2013, American drones launched approximately 337 attacks in Pakistan,[272] along with approximately 65 strikes in Yemen,[273] and 3 to 9 in Somalia.[274]

The totals are approximate because, given the lack of official statistics, reports occasionally conflict regarding whether the strike came from a UAV or a manned aircraft, or whether American or local government forces were responsible. For example, according to diplomatic cables revealed by WikiLeaks, Yemeni officials claimed responsibility for American airstrikes to avoid a public outcry over the government granting foreign forces permission to launch attacks against Yemeni citizens on their territory, with Yemeni President Ali Abdullah Saleh telling American General David Petraeus, then commander of US forces in the Middle East, that "we'll continue saying the bombs are ours, not yours."[275] The figures thus represent confirmed American drone strikes, which could be considered a low-end estimate. Alternative sources, especially those critical of American UAV campaigns, like the Bureau of Investigative Journalism's "Covert War on Terror" project, compile data on any possible drone strike, estimating 362 attacks in Pakistan, and up to 93 in Yemen, which effectively provide high-end estimates.[276]

Of the three locations, Pakistan features the best international press coverage and has received the most scholarly attention. The Year of the Drone project, led by Peter Bergen at the New America Foundation, provides a comprehensive study of UAV attacks in Pakistan. The project "draws only on accounts from reliable media organizations with deep reporting capabilities in Pakistan, including the New York Times, Washington Post, and Wall Street Journal, accounts by major news services and

[272] "Year of the Drone."
[273] "Obama Covert War in Yemen."
[274] "Covert War on Terror."
[275] Allen, "WikiLeaks: Yemen Covered Up US Drone Strikes."
[276] "Covert War on Terror."

networks—the Associated Press, Reuters, Agence France-Presse, CNN, and the BBC—and reports in the leading English-language newspapers in Pakistan—the Daily Times, Dawn, the Express Tribune, and the News—as well as those from Geo TV, the largest independent Pakistani television network."[277] Using these sources, Bergen's team compiles drone attacks in Pakistan through January 2013 as follows:

Year	Drone Strikes	Estimated Total Deaths		Estimated Militant Deaths		Percentage Civilian Deaths[278]		Est. Militant Leader Deaths
		Low	High	Low	High	Low	High	
2004-2007	9	89	112	81	103	8.98%	8.04%	3
2008	33	274	314	134	165	51.09%	47.45%	11
2009	53	369	725	266	502	27.91%	30.76%	7
2010	118	607	993	581	939	4.28%	5.44%	12
2011	70	378	536	362	500	4.23%	6.71%	6
2012	48	222	349	194	317	12.61%	9.17%	6
2013 (Jan)	6	37	44	37	44	0.00%	0.00%	4
Total	337	1976	3073	1655	2570	16.24%	16.37%	55

The United States first employed UAVs in Pakistan in 2004, but the drone campaign began in earnest in 2008. The number of strikes escalated from 33 in 2008, to 53 in 2009, and peaked at 118 in 2010, followed by 70 in 2011 and 48 in 2012. The initial rise indicates an increasing reliance on UAV strikes to target various insurgent networks operating along the Afghanistan-Pakistan border, along with remaining members of al Qaeda. The increasing number of attacks is coupled with a decreasing percentage of civilian deaths, which suggests better intelligence and improving skill regarding drone

[277] "Year of the Drone."

[278] Low percentage of civilian deaths calculated using the low estimated total deaths and low estimated militant death figures. High percentage of civilian deaths calculated using the high estimated total and high militant death figures. As a result, in some years, the percentage of civilian deaths calculated by using the low estimates is greater than that calculated by using the high estimates.

usage.

The declining number of UAV strikes and associated deaths after 2010 demonstrates the effectiveness of the campaign, as fewer targets become available. While this could be due to successful elimination of a significant percentage of fighters, the decline could also indicate that insurgents have adjusted their behavior to reduce their vulnerability to aerial attacks. The estimated number of militant leader deaths in 2011 (6) and 2012 (6) are fewer than any since 2007, and insurgent leaders have said that the drone strikes have driven them underground.[279] This therefore suggests that the drone campaign in Pakistan has disrupted insurgent operations in the Afghanistan-Pakistan theater by killing fighters and leaders, and denying the remaining members the ability to operate openly.

Meanwhile, the drone campaign in Yemen has escalated, with more UAV attacks in 2011 and 2012 than in all previous years combined. While Yemen was the site of the first extrajudicial targeted killing by UAV—the Predator-launched strike against Ali Qaed Senyan al Harthi in 2002—the American drone campaign began focusing on Yemen after al Qaeda in the Arabian Peninsula (AQAP) claimed responsibility for the attempted “underwear bombing” on December 25, 2009, in which Umar Farouk Abdulmutallab attempted to detonate a plastic explosive called PETN that was sown into his underpants while on board a Northwest Airlines flight from Amsterdam to Detroit. Beginning with an attack on a suspected AQAP training camp in December 2009, the United States launched approximately 27 drone strikes through June 2012,[280] and at least 27 more in the following seven months, with 6 attacks in January 2013 alone.[281]

As of January 2013, the strikes have killed an estimated 765-1080 people in Yemen, 743-1006 of whom the New America Foundation identified as militants. This presents an estimated civilian

[279] Khan, “Pakistani Taliban: US Drone Strikes Forcing Militants Underground.”
[280] Bergen and Rowland, “Obama Ramps Up Covert War in Yemen.”
[281] “Obama's Covert War in Yemen.”

casualty rate of 2.87% to 6.85%, which is similar to the rate in Pakistan from 2010 through early 2013 (5.63% to 6.35%), providing further evidence of the UAV teams' ability to target selectively. The strikes have killed at least 41 senior members of AQAP, including the American-born cleric Anwar al Awlaki on September 30, 2011, and the organization's head of media, Ibrahim al Bana on October 14, 2011.[282] In addition to assisting in the planning of operations, al Awlaki was considered the public face of AQAP, broadcasting the group's message in sermons on the internet, and directly communicating with and motivating Abdulmutallab, Fort Hood shooter Nidal Malik Hasan, and others.[283]

While the United States can point to individual successes, like killing al Awlaki, it is unclear if the drone campaign is succeeding strategically. Yemen expert Gregory Johnsen reports that al Qaeda in the Arabian Peninsula has grown from 200-300 militants in 2008 to more than 1,000 fighters as of 2012, with expanded control in southern Yemen. “In parts of Abyan and Shabwa provinces,” he stated, “the organization controls towns in which it has established its own police departments and court systems. It is providing water, electricity and services to these towns. In short, AQAP now sees itself as the de facto government in the areas under its control.”[284] This demonstrates UAVs' ability to kill wanted individuals, but casts doubt on the strategy of targeted killings as a method of successfully neutralizing militant groups. It is possible that anger in response to attacks increases popular support for militant movements and improves their recruiting, though this blowback effect is almost certainly due to violations of sovereignty and the damage and casualties the attacks cause, not the fact that the strikes come from unmanned systems rather than manned aircraft.

Much like ground-based robots, aerial drones allow militaries to execute missions at reduced risk to personnel. This leads to fewer strong actor deaths, and, correspondingly, less political cost.

[282] Ibid.
[283] Madhani, “Cleric al-Awlaki Dubbed 'bin Laden of the Internet.'”
[284] Quoted in Bergen and Rowland, “Obama Ramps Up Covert War in Yemen.”

States, of course, do not want unmanned aerial systems to crash, get shot down, or destroyed, because of the cost of the equipment and the risk that enemies will learn more about proprietary technologies; but there is no danger that a human pilot will be killed or captured and exploited by enemy forces. Drones are expensive, but cost considerably less than manned aircraft, primarily because they do not include equipment necessary to accommodate a person, such as a cockpit, ejection seat and parachute, or air pressure control. For example, according to the Pentagon's requested budget for fiscal 2012, each F/A-18E/F Fighter costs $93.4 million, while the next generation F-35 Joint Strike Fighter and F-22 respectively cost $133.6 million and $345.9 million per plane. However, each Reaper costs a relatively cheap $30.3 million, which includes the ground control equipment, satellite uplink, and the drone itself. Each RQ-1 Predator costs only $4.03 million.[285]

These manned aircraft are not yet obsolete, because they offer far superior air-to-air combat capabilities. Unlike fighter jets such as the F-18 or F-22, Predators and Reapers lack the ability to engage in aerial dogfights against enemy airplanes. The drones are capable of carrying air-to-air missiles, which they could fire at opposing aircraft, but they lack the speed, maneuverability, and situational awareness to challenge fighter jets.[286] In December 2002, before the start of the Iraq war, an MQ-1 Predator gathering information over Iraq was fired upon by an Iraqi MiG-25 Foxbat. As the MiG's missile approached the Predator, the drone's pilot launched an air-to-air Stinger missile in response, but did not connect. The Predator was destroyed.[287]

Since 2002, there have been no reported incidents of UAVs firing upon enemy aircraft. Due to the absence of air threats in the Iraq and Afghanistan wars, and Predators' limited carrying capacity, the

[285] "Analysis of the Fiscal Year 2012 Pentagon Spending Request."

[286] Pardesi, "Unmanned Aerial Vehicles/Unmanned Combat Aerial Vehicles: Likely Missions and Challenges for the Policy- Relevant Future."

[287] "Dogfight between MQ-1 Predator drone and MiG-25 Foxbat."

United States outfitted its unmanned combat aerial systems exclusively with ground attack weapons;[288] but in the future, the United States and other advanced nations will likely develop UAVs capable of aerial combat. A 2009 Air Force study mapping out the future of unmanned aircraft envisions a class of UAVs called "MQ-Mc," which would be capable of any Air Force mission, including dogfighting and nuclear strikes, by 2030.[289] Meanwhile, the Navy is already designing experiments, which may take place as early as 2015, in which two teams, each made up of as many as 50 small "aerial battle bots," will engage each other to develop tactics for unmanned air-to-air combat.[290] Besides costing less than manned aircraft, and eliminating the risk to human pilots, unmanned planes have the potential to be more maneuverable, because human pilots can lose consciousness from the g-force of rapid turns at supersonic speeds.

However, air-to-air combat capabilities are not especially important to state-network warfare. Due to their resource advantage, powerful states can easily maintain air superiority over non-state opponents. The primary threat to strong actor aircraft comes from surface-to-air attacks from anti-aircraft weaponry, such as shoulder-launched missiles, rather than enemy fighter jets. Every fixed-wing or rotary aircraft lost by the United States and allies in Iraq or Afghanistan was due to accident or ground-based fire. Therefore, while unmanned aerial vehicles with the ability to engage other aircraft in dogfights would provide strategic advantages in a symmetric conflict between powerful states, UAVs with information gathering and ground attack capabilities are sufficient for conflict against non-state networks.

In asymmetric warfare, the lack of human pilots brings advantages beyond decreased risk to personnel and lower monetary cost. Robotic airplanes do not need to eat, sleep, or use the bathroom. Ground-based drone operators have the opportunity to attend to bodily needs, or change shifts due to

[288] Axe, "Predator Drones Once Shot Back at Jets... But Sucked At It."
[289] "Unmanned Aircraft Systems Flight Plan."
[290] Terdiman, Daniel, "Drone dogfights by 2015? U.S. Navy preps for futuristic combat."

fatigue. As a result, UAVs can remain in the air for far longer than any manned aircraft, with pilots constantly operating at peak capacity. This allows them to be more selective about the timing of attacks. Due to limited flight time and concern for personal safety, the pilot of a manned plane is more likely to fire on a target when the opportunity arises. Unmanned planes, by contrast, can remain in the air for 36 hours or more, allowing them to wait for greater certainty about a target's identity, and for targeted individuals to be isolated from non-combatants.

The result is fewer civilian deaths relative to attacks from manned aircraft. As the following table shows, an increasing reliance on drone strikes coincided with a significant decrease in civilian casualties in Afghanistan. According to statistics from United States Air Force Central Command, weapons fired from unmanned aircraft increased by 42% from 2011 to 2012, going from 5.45% of total airstrikes to 12.37%. Meanwhile, civilian casualties (including both deaths and injuries) declined by 42%, while civilian deaths from airstrikes declined by 46%. Though 2012 featured fewer total weapons released by aircraft, this cannot explain the decline in civilian casualties, as the rate of both total civilian casualties and civilian deaths per airstrike decreased.

Year	All Weapon Releases from Aircraft[291]	Weapon Releases from UAVs[292]	Percentage of Weapon Releases from UAVs	Civilian Casualties from Air Attacks[293]		Civilian Casualties Per Weapon Release	
				Casualties	Deaths	Casualties	Deaths
2010	5102	279	5.47%	306	171	6.00%	3.35%
2011	5411	294	5.43%	353	235	6.52%	4.34%
2012	4092	506	12.37%	204	126	4.99%	3.08%

[291] See: Dobrydney, David, “Combined Forces Air Component Command Airpower Statistics.”
[292] Ibid.
[293] “Afghanistan: Annual Report 2012 Protection of Civilians in Armed Combat.”

In addition to large drones, like the Reaper, the US employs smaller unmanned aerial vehicles that help ground forces attack with greater precision, potentially reducing the risk to strong actor soldiers and nearby civilians. For example, the Switchblade, from AeroVironment, is "a Non Line of Sight (NLOS) weapon" that measures only two feet long and weighs a little over two pounds.[294] It launches out of mortar-like tube, whereupon its wings unfold and its camera switches on.[295] Alternatively, it can launch from the 70mm rocket tubes used on army helicopters.[296] Together, the launch tube and drone weigh 5.5lbs, and can be easily carried by one soldier.[297] Using a hand-held controller that receives video and GPS coordinates, an operator can guide the Switchblade and then crash it into a target in a kamikaze attack.

This provides soldiers in the field with a valuable method of attacking distant targets without having to call in airstrikes. The Switchblade utilizes a quiet electric motor, which allows it to sneak up on targets,[298] can remain in the air for 20 to 40 minutes,[299] has an effective range of 10 kilometers, and is capable of suspending its attack sequence and loitering.[300] While Predators and Reapers fire 100-pound Hellfire missiles, or drop 500-pound GPS guided bombs,[301] the Switchblade carries an explosive similar to a hand grenade.[302] It therefore causes far less collateral damage to bystanders or property. After successful tests in 2011, the US Army ordered over 100 Switchblades,[303] awarding AeroVironment with a series of contracts that total $10 million for the drones and associated services, such as training.[304]

[294] "Switchblade – Miniature Loitering Weapon."
[295] Hennigan, "Pentagon to soon deploy pint-sized but lethal Switchblade drones."
[296] Dunnigan, "Switchblade Enters Service."
[297] "Switchblade – Miniature Loitering Weapon."
[298] "UAS Advanced Development: Switchblade."
[299] Dunnigan, "Switchblade Enters Service."
[300] "US Military Bringing a Switchblade to A Gun Fight."
[301] Hennigan, "Pentagon to soon deploy pint-sized but lethal Switchblade drones."
[302] Dunnigan, "Switchblade Enters Service."
[303] Dunnigan, "Switchblade Enters Service."
[304] "U.S. Army Awards AeroVironment $5.1 Million Order for Switchblade Loitering Munition Systems and Services."

In many ways, the Switchblade represents a culmination of the century-old effort to create a flying bomb. While missiles are capable of quickly traveling great distances, and the modern varieties can shift direction mid-air and be guided towards a target, they cannot hover or return to base. The Switchblade, however, can loiter and land, giving operators the ability to pause an attack to reconsider, or call it off and reuse the equipment later. Additionally, the cameras allow soldiers to pursue fleeing suspects and confirm a target's identity at close range before initiating the attack sequence.

The Switchblade is ideally suited for urban warfare, as it greatly improves attacks against covered positions, and grants soldiers the ability to strike enemies firing from rooftops or windows without destroying entire buildings. Firing mortars, lobbing grenades, or calling in airstrikes risk collateral damage, while advancing on the enemy's position places soldiers at risk. Additionally, as soldiers advance, they often utilize covering fire, which could accidentally hit bystanders. The Switchblade, however, can maneuver around objects and strike directly around corners, over walls, at fortified positions or enemies hiding from a soldier's line of sight. This decreases the ability of weak actors to exploit the asymmetries of resolve and expectations by operating in populated areas, because small kamikaze drones like the Switchblade improve the ability of strong actors to respond to enemies firing from covered or hidden positions without risking extensive civilian casualties.

In addition to unmanned attack aircraft, the United States military has begun using pilotless helicopters to deliver supplies in combat theaters. Beginning in December 2011, two modified K-MAX helicopters, built by Kaman and modified for autonomous flight by Lockheed Martin, have been delivering goods to American marine outposts in Afghanistan. These experimental missions have been such a success that the program has been extended twice and remains running.[305]

The K-MAX can carry up to 6,000 pounds at sea level, which is more than its empty weight, and more than 4,000 pounds at an altitude of 10,000 feet, attached to a steel cable. With its "four-hook

[305] "Robocopter arrives."

carousel," the helicopter can drop off supplies in multiple locations on one mission.[306] In the first two months, the K-MAXs delivered over 100,000lbs of cargo on over 50 unmanned resupply missions.[307] Within six months, the helicopters delivered over one million pounds of food, fuel, and equipment.[308]

Unlike the Predator and other fixed wing UAVs, which are usually piloted by remote control, the unmanned K-MAX often flies autonomously. The helicopter typically flies along a pre-programmed course to a forward operating base using GPS coordinates, where a human on the ground directs the drop with a remote control. Using a variety of sensors, it is able to drop its cargo or land in total darkness.[309] However, with a new development the K-MAX can deliver cargo without human intervention. Using a beacon approximately the size of a hockey puck developed by Lockheed Martin to mark the drop point, an unmanned K-MAX autonomously deposited cargo within three meters of its target on ten out of ten demonstrations in April 2012.[310] The beacons are scheduled for further tests in April 2013.

Whether partially or completely autonomous, robotic helicopters provide two main advantages to strong actors fighting an insurgency: bypassing land-based supply routes and reducing the risk to helicopter pilots. Ground forces, especially those stationed in remote locations, require a steady supply of food, fuel, ammunition, and replacement parts for equipment. Traditionally, armies convoy materials to forward troops with long, ground-based supply lines, along which vehicles and, in rougher terrain, pack animals, could be attacked. Supply line disruption is a common insurgent technique, because convoys are rarely as well armed as combat troops, and regular routes allow those with knowledge of the territory to set up ambushes. Helicopter-based supply lifts reduce the need for ground-based supply lines, which reduces insurgents' ability to ambush convoys, kill personnel, deny

[306] McLeary, "Marines extend Afghan deployment of cargo UAV."
[307] McLeary, "K-MAX Chugging Along in Afghanistan."
[308] McLeary, "Marines extend Afghan deployment of cargo UAV."
[309] "Robocopter arrives."
[310] Sanborn, "Beacon improves UAVs cargo-delivery accuracy."

materials to troops in the field, and, perhaps most importantly, capture supplies. Switching from ground-based to aerial supply missions would make Che Guevara's favored technique of supplying his forces with captured material much more difficult.

Automated helicopters increase the feasibility of an aerial alternative to ground-based supply lines. Like fixed-wing UAVs, the automated K-MAX does not get fatigued or hungry, and can thus remain in flight longer than manned aircraft. As with other drones, robotic helicopters eliminate any physical risk to human pilots. However, this is arguably more important for helicopters than airplanes, because helos fly lower and slower than planes, making them more vulnerable to ground-based anti-aircraft fire.

Therefore, as with ground-based robots, both fixed-wing and rotary UAVs reduce strong actors' disadvantage regarding the asymmetry of resolve from both directions. Using unmanned airplanes and helicopters reduces strong actor casualties, thereby slowing the rise of war-weariness and the associated political pressure to abandon protracted conflicts. Additionally, drones' ability to wait longer than manned aircraft before striking reduces the risk of collateral damage, generating less anger among both strong and weak actor constituencies. As a result, the strong actor faces fewer political costs, and the weak actor experiences less of a boost to resolve.

In a study of drone strikes in Pakistan from March 2004 through June 2010, Patrick Johnston and Anoop Sarbahi find that drone strikes correlate with a decrease in both the frequency and lethality of militant attacks.[311] This suggests that the drone campaign in Pakistan has reduced militants' capacity, and that the negative reaction among Pakistanis is insufficient to replenish the capabilities of insurgent networks. If the drone strikes increased the resolve of people in the Federally Administered Tribal Areas along the Afghanistan-Pakistan border, if anger over the attacks effectively created more

[311] Johnston and Sarbahi, “The Impact of US Drone Strikes on Terrorism in Pakistan.”

insurgents than the strikes eliminated, then we would expect to see the opposite result from a study like Johnston and Sarbahi's.

Robots and Information

While drone strikes garner more publicity, considerably more UAV flight time is devoted to gathering information. For example, in Afghanistan from 2009-2011, the United States conducted more than four times as many spy sorties as strike missions.[312] Robots do not attack in fundamentally different ways from humans; UAVs fire the same types of missiles that are attached to manned aircraft, and ground-based bots fire the same types of weapons that human soldiers carry or mount on manned vehicles. However, a robot can gather far more and more detailed information than a person by employing daylight cameras, infrared, radar, and other sensors. Furthermore, machines can process more information, more quickly, and from more sources at once. The rapid advancement of robotics and information technology show no signs of slowing, which has, and will continue to have, a dramatic impact on asymmetric warfare by helping relatively strong actors overcome asymmetries of information.

Intelligence, Surveillance, and Reconnaissance (ISR) Unmanned Aerial Systems

While the earliest unmanned aircraft were attempts to create flying bombs, the United States began developing the forerunners of modern UAVs to replace spy planes. In 1960, the Soviet Union shot down an American U-2 over Sverdlovsk (now Yekaterinburg) that was using high-resolution cameras to photograph military installations and other strategically important sites on Soviet territory. The pilot, Francis Gary Powers, managed to eject and parachute down safely, but was captured by

[312] Shachtman, “Flying Spy Surge: Surveillance Missions Over Afghanistan Quadruple.”

Soviet forces, along with the remains of the mostly intact U-2. The incident caused considerable embarrassment for the United States, and led to the release of KGB colonel Vilyam Fisher in a prisoner exchange for Powers. Within days of Powers' capture, the United States launched Red Wagon, a classified UAV program.[313]

American UAVs began flying reconnaissance missions in the 1960s over Vietnam and China, using primarily Ryan Lightning Bugs. The US Air Force's 100th Strategic Reconnaissance Wing flew 3,435 UAV missions during the Vietnam War, losing 554 unmanned planes. In Congressional testimony, USAF General George S. Brown explained the logic simply: “The only reason we need [UAVs] is that we don't want to needlessly expend the man in the cockpit.”[314]

The modern UAV successor to large, high-endurance spy planes like the U-2 is the RQ-4 Global Hawk made by Northrup Grumman. The RQ designation identifies the Global Hawk as an intelligence gathering platform, in contrast to the MQ designation that identifies the Predator and Reaper as combat systems. First tested in June 1999, the Global Hawk can fly extremely high, up to 65,000 feet, and remain in the air for as long as 35 hours. With a maximum speed approaching 400 mph, the Global Hawk can fly 1,200 miles to a target area, observe the area for 24 hours, and then return to base. The drone is almost entirely autonomous. Once it is programmed where to fly and what area to observe, the Global Hawk can autonomously taxi, take off, fly, gather information about the target area, return, and land. Ground-based operators, primarily at Beale Air Force Base in California, monitor the UAV remotely and can redirect the plane or its sensors as they wish.[315]

21st century intelligence, surveillance, and reconnaissance (ISR) systems like the Global Hawk utilize a variety of methods of gathering information. In addition to high resolution cameras that provide photographs and video, ISR drones carry infrared sensors, which observe heat, rather than

[313] Wagner, p. xi, xii.
[314] Wagner, p. 208.
[315] “RQ-4 Global Hawk.”

visible light, allowing them to identify hot objects like people, vehicles, anti-aircraft batteries, electricity generators, and computer servers. Synthetic-aperture radar, which has also been used by spacecraft to observe the surface of planets and other celestial objects, utilizes the motion of the aircraft and a varied series of sound waves to provide a detailed map of terrain, including land formations, buildings, and other objects.[316] Complimenting these are electro-optical sensors, which gather information about a given object by analyzing the spectrum of electromagnetic energy—infrared, visible light, and ultraviolet—it reflects and absorbs. Much as space telescopes can determine the chemical make-up of distant stars by the electromagnetic energy they emit, electro-optical sensors on ISR drones can determine the type and strength of fuel coming out of the back of a missile, as well as distinguish between objects that appear similar in photographs, such as natural terrain and artificial camouflage.[317] Beginning in 2007, some UAV models feature the Airborne Signals Intelligence Payload system (ASIP), which tracks and identifies radar and other types of electronic and communication signals.[318] The infrared, radar, electro-optical, and electronic signals sensors can gather information day or night, regardless of cloud cover.

Utilizing these sensors in combination, the Global Hawk can conduct a wide-area search observing an entire region, or focus on a single target using its "high-resolution spot mode."[319] In 24 hours, it can image a 40,000 square-mile area, approximately the size of Illinois, and relay this information in near-real time using satellite and ground-based communication systems.[320] Northrup Grumman boasts that Global Hawks logged over 350 hours of flight time in the Iraq War, collecting

[316] "What Is Synthetic-Aperture Radar?"
[317] Lum, "The Measure of MASINT."
[318] "RQ-4 Global Hawk," p. 4.
[319] Singer, *Wired for War*, p. 36.
[320] "RQ-4 Global Hawk", p. 4.

over 4,800 images, and locating surface-to-air (SAM) missile batteries, SAM transporters, and Iraqi tanks.[321]

Unlike the Global Hawk, the RQ-170 Sentinel from Lockheed Martin is outfitted with stealth technology, making it better suited for gathering information against targets that possess air defense capabilities. Introduced in 2007, the Sentinel is operated primarily by the Air Force and the CIA, and much of its specifications remain classified. In contrast to other drones, the Sentinel is a flat "flying wing," and looks like a smaller version of the B-2 stealth bomber. Because it utilizes jet propulsion, the Sentinel can probably fly considerably faster than propeller powered UAVs like the Predator, and reach heights of 50,000 feet.[322] The Sentinel was photographed over Afghanistan in 2007, earning it the nickname "the Beast of Kandahar,"[323] and played a role in the operation that killed al Qaeda leader Osama bin Laden. It is widely assumed that the Sentinel possesses an array of sensors similar to that of other ISR drones like the Global Hawk, with the possible addition of nuclear material "sniffing" sensors that can detect radioactive isotopes at a distance.[324] With its role in providing ground forces with real-time battlefield intelligence, along with suspected spying missions over Iran and North Korea, this stealth UAV demonstrates both the rapid advancement of drone technology, and the increasing usefulness of unmanned systems.

In 2010, the United States began outfitting reconnaissance drones with the next generation of ISR cameras, the Wide Area Airborne Surveillance System from the Sierra Nevada Corporation. Nicknamed Gorgon Stare, after the unblinking monsters from Greek mythology, the system uses nine electro-optical and infrared cameras to observe up to 100 square kilometers at once.[325] The images are sufficiently detailed that the system can send up to 65 different views to different users on tablets or

[321] "RQ-4 Global Hawk," p. 2.
[322] "Lockheed Martin RQ-170 Sentinel Unmanned Aerial Vehicle."
[323] Dsouza, "RQ-170 Sentinel 'Beast of Kandahar.'"
[324] "Lockheed Martin RQ-170 Sentinel Unmanned Aerial Vehicle."
[325] "Gorgon Stare."

laptops, allowing some users to zoom in on a small section while another user simultaneously looks at a wider area. According to Maj. Gen. James O. Poss, the Air Force's assistant deputy chief of staff for intelligence, surveillance and reconnaissance, “Gorgon Stare will be looking at a whole city, so there will be no way for the adversary to know what we're looking at, and we can see everything.”[326] Gorgon Stare thus provides a significant advancement from one-camera systems that could capture video images of a single target, like a building or an intersection.

The Air Force plans to mount Gorgon Stare on Reaper UAVs, and reportedly began using it in a limited capacity in Afghanistan beginning in December 2010.[327] At least eight have been ordered, at a cost of $17.5 million each. The system weighs 1,100 pounds, and, because of its weight and configuration, would be mounted on Reapers that are not also carrying weapons.[328]

However, Gorgon Stare disappointed in tests in late 2010 by the 53rd Wing of the Air Combat Command at Eglin Air Force Base, which deemed the system “not operationally effective” and “not operationally suitable.”[329] It successfully tracked vehicles, but could not reliably follow smaller objects, most notably people. Gorgon Stare sometimes failed to seamlessly join the images from multiple cameras, creating blind spots and leading the system to lose track of objects as they left an individual camera's frame. Limited bandwidth combined with huge amounts of data caused delays in relaying information to the ground. Most egregiously, even when it successfully tracked objects, a software error occasionally generated “a faulty coordinate grid,” sending an inaccurate location to operators. This could lead forces acting on the information to lose an object of interest by arriving at an incorrect location, or, disastrously, attacking a civilian or friendly target.[330] These problems led one

[326] Nakashima and Whitlock, “With Air Force's Gorgon Drone 'we can see everything.'”
[327] “Gorgon Stare.”
[328] Nakashima and Whitlock, “With Air Force's Gorgon Drone 'we can see everything.'”
[329] Clark, “Gorgon Stare Blinks A Lot.”
[330] Ibid.

tester to deem Gorgon Stare only "55 to 65 percent reliable,"[331] which is insufficient for regular use in the field, especially regarding information that is acted upon in real-time.

These difficulties are technical, rather than conceptual, and will almost certainly improve as imaging and data transfer technology continue to progress. A promising alternative is a system based on a single, extremely powerful camera rather than a series of integrated sensors like Gorgon Stare. The Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), developed by BAE systems, utilizes the world's highest resolution video camera.[332] At 1.8 gigapixels, it can spot a 6-inch object from 17,000 feet in the air.[333] The picture is so detailed that the ARGUS-IS can provide over 60 independent "electronically steerable" windows that zoom in on a component of the larger image. Instead of directing a camera to change its focus, a computer system focuses on an aspect of the recorded image, either providing continuous footage of a fixed area, or automatically keeping a specific target in the window.[334] Therefore, unlike Gorgon Stare, the ARGUS-IS does not lose track of an object as it moves from one sensor area to another.

However, like other Wide Area Airborne Surveillance Systems, the ARGUS-IS collects a huge amount of information, potentially creating data transfer delays. The ARGUS-IS can store up to one million terabytes of data per day, recording the equivalent of 5,000 hours of high-definition video.[335] Such a large amount of data requires considerable bandwidth to transfer from the aircraft to a ground base where analysts can view the videos.

One potential method to smooth this process is through an aerial command center, known as Integrated Sensor Is Structure (ISIS).[336] Directed by DARPA and the United States Air Force Research Laboratory, the ISIS project aims to develop a high-altitude airship that would carry sensors, including

[331] Ibid.
[332] Beizer, "BAE to Develop Surveillance System."
[333] Gallagher, "Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?"
[334] "Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System (ARGUS-IS)."
[335] Gallagher, "Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?"
[336] "Integrated Sensor Is Structure (ISIS)."

a radar with a range of 600 kilometers, and could link to ISR drones. While the ARGUS-IS films from a maximum height of 20,000 feet,[337] the ISIS blimp will fly over 60,000 feet, out of the range of most anti-aircraft weapons. Additionally, from that height, it could track aerial objects along with those on the ground. Held aloft by helium, and powered, at least in part, by solar energy, the airship could remain aloft for long stretches of time, perhaps multiple years. In April 2009, DARPA awarded a $400 million contract to Lockheed Martin and Raytheon to produce a prototype ISIS system, which is expected in 2014.[338]

A functional ISIS system could address some of the technical problems of Gorgon Stare. Like the ARGUS-IS, the ISIS system uses a single radar and sensor array covering a wide area, so it would not lose track of an object as it moved from one sensor area to another; though its high-altitude position would reduce the ability to provide detailed visual imagery to observers. As a blimp flying at high-altitude, ISIS could communicate more easily with a satellite, improving upon ARGUS-IS or Gorgon Stare's difficulties with data transmission. Additionally, the airship could function as an informational mothership, gathering data from other ISR platforms in the area, and relaying that information to analysts on the ground. By combining data from the sensors of Gorgon Stare, the high definition video of ARGUS-IS, and the powerful radar of the ISIS in one ISR command center, battlefield commanders and intelligence analysts could gather a detailed portrait of a designated area.

This would help address the technical problem of delayed data transmission, but not the conceptual problem of the bottleneck created by data analysis. A fully operational Gorgon Stare, ARGUS-IS, or alternative Wide Area Airborne Surveillance System, could produce visual, infrared, and electro-optical information about a 100 square kilometer area, covering an entire town or a significant portion of a large city. (For reference, Baghdad covers 734 square kilometers). These

[337] Hoffman, “PBS Features DARPA'S ARGUS-IS.”
[338] Trimble, “Lockheed Martin to Build the Mother of All Airborne Radars.”

systems produce an immense amount of data, requiring dozens of human observers to monitor a sparsely populated area, and hundreds to watch and analyze an urban center bustling with activity. Air Force officials working on the ARGUS-IS project have reached out to sports broadcasters and reality show producers seeking advice on how to monitor many simultaneous video feeds.[339]

The United States already has difficulty keeping up with the demand for airborne surveillance, especially in active theaters like Afghanistan. ISR sorties undertaken by manned and unmanned aircraft quintupled over Afghanistan, from approximately 500 per month in the first quarter of 2009, to over 1,500 per month in mid-2010,[340] to over 2,500 per month in the first nine months of 2011.[341] Analyzing the data from each of these sorties requires considerable manpower, even though the information is relatively focused because an officer explicitly selected a target for surveillance. A Wide Area Airborne Surveillance System could reduce the number of flights necessary to gather the same amount of information, but the true advantage of Gorgon Stare or ARGUS-IS is the ability to observe many targets at once, including areas that users do not know are important in advance. However, to accomplish this would require observers to actively monitor every piece of information the system acquires, whether or not they possess a corroborating reason to pay attention. Highlighting this problem at a conference in November 2010, General James E. Cartwright, the vice chairman of the Joints Chiefs of Staff, lamented that “an analyst sits there and stares at Death TV for hours on end, trying to find the single target or see something move. It's just a waste of manpower.”[342]

This demonstrates that current technologies cannot yet overcome the asymmetries of information and responsibility inherent in asymmetric warfare. Relatively weak actors, such as insurgents in Afghanistan, have a plethora of targets to choose from; attacking civilians or local

[339] Hoffman, “PBS Features DARPA'S ARGUS-IS.”
[340] Nakashima and Whitlock, “With Air Force's Gorgon Drone 'we can see everything.'”
[341] Shachtman, “Flying Spy Surge: Surveillance Missions Over Afghanistan Quadruple.”
[342] Nakashima and Whitlock, “With Air Force's Gorgon Drone 'we can see everything.'”

government officials in any populated area disrupts normalcy, while attacking strong actor forces or anyone working with them in any location imposes a cost on the counterinsurgents. Relatively strong actors have to protect all of these targets at once, without knowing where insurgents will attack, or, in many cases, who is an insurgent and who is a civilian. Human intelligence can close the information gap by providing strong actors with the identities and plans of some insurgents. However, without good humint to direct analysts' focus, ISR systems just gather a flood of information that may or may not be important. Given the limited ability of operators to monitor all of this data at once, they might not learn that a particular piece of information is relevant until after an attack.

Therefore, it would be extremely valuable if advancements in information gathering were accompanied by advancements in information processing. Instead of numerous human analysts staring at live video feeds, just in case something might happen, computer software could monitor many feeds simultaneously, and alert human analysts if something happens that requires their attention. This would allow a few people to monitor a large area, since no human attention would be wasted on locations where nothing is moving.

As of yet, comprehensive software capable of autonomously monitoring a large area does not exist, though there have been considerable advancements in the field of computer vision, which indicates that such a software package is possible. Computer vision seeks to teach machines to replicate the human ability to distinguish and understand components of visual imagery. While humans have little difficulty picking out the components of pictures or videos, computers require complex algorithms to identify various objects as distinct from the background. It is especially challenging to teach a computer to recognize the same object from multiple angles, at multiple scales, or when partially obscured.[343]

[343] See Sonka et. al., *Image Processing, Analysis, and Machine Vision*.

Computer vision already plays a significant role in ISR systems. Object recognition and motion tracking allow systems like the ARGUS-IS to keep a visual window focused on a person or vehicle as it moves through the larger image. This requires distinguishing the object from a constantly changing background and from similarly shaped objects that enter the frame. However, while the system can autonomously follow a designated item, a human operator must first select a target for the system to track.

Before long, software will be able to identify and track objects with less human direction. In 2012, Google received a patent for software that autonomously identifies objects in videos on YouTube, its video sharing site. Instead of asking users to label objects in their videos, the software utilizes a database of "feature vectors," such as color, shape, texture, and movement, to compare various objects across videos and label them automatically.[344] Such software presages a program that could watch "Death TV for hours on end" in support of, or in place of human analysts.

Developing software capable of monitoring the input from a Wide Area Airborne Surveillance System would free up considerable manpower and could significantly reduce the disadvantage strong actors face from the asymmetries of responsibility and information. To prevent disruption, counterinsurgents need to protect many potential targets at once. In larger areas, this becomes cost prohibitive for strong actors, since it is almost impossible to know when and where weak actors will attack. Oil pipelines, power lines, railroads, and other infrastructure are thus attractive targets for insurgents, because it is difficult to defend all of them at once, and a breach anywhere along the route can significantly disrupt the flow of resources, electricity, or goods. However, a computer, monitoring video and infrared sensors, could effectively watch an entire length of pipeline or railroad, alerting human operators to suspicious activity, such as people approaching a remote area at night. If soldiers are unable to arrive in time to prevent the attack, the computer could track any people leaving the area

[344] Fingas, "Google lands patent for automatic object recognition in videos."

following an explosion, allowing soldiers to intercept them before they can blend back in to the civilian population.

Due to the asymmetry of information, attacking strong actor soldiers as they move along roads is among the most successful insurgent tactics. Given their size, convoys of strong actor troops or supplies are fairly conspicuous. It is therefore far easier for insurgents to know the route of a convoy than for counterinsurgents to know the location of ambushes or explosives hidden next to or buried under a road. A Wide Area Airborne Surveillance System could monitor roads in front of convoys, spotting people that may not be visible to soldiers traveling along the road, and use object recognition to autonomously search for weapons. Additionally, if computer vision software can learn to recognize basic actions in addition to objects, cameras could monitor every stretch of road in a given area, alerting human operators when it spots someone potentially planting explosives. The action in question may be innocuous, and the system might not be able to recognize every type of explosive device, but it could alert a human analyst to the suspicious activity, who could then zoom in closely and review the video.

Meanwhile, the data gathered by airborne ISR systems, including Gorgon Stare and ARGUS-IS, could be utilized for after-the-fact analysis. With Wide Area Airborne Surveillance systems and ISIS blimps capturing images of everything within an area of interest, there would be a record of every IED explosion, every attempted ambush, and every outdoor movement of people and vehicles. This would enable analysts to review a visual record of any event of interest. They could closely analyze a single event to identify mistakes and develop countermeasures, or analyze multiple events of the same type, looking for patterns.

For example, after an IED explodes under a patrolling vehicle, or is successfully dismantled by an Explosive Ordinance Disposal team—perhaps with the assistance of a ground-based EOD robot—analysts could review video from the bomb's location. They could run the video back to the point when an insurgent placed the IED, and then both follow him to his next location or reverse the video further to discover his previous location, thereby potentially finding where the bomb was made. Real-time analysis would be more valuable, by enabling ground forces to arrive quickly when an insurgent plants a bomb, arrest the bomber, and dispose of the ordinance before it can harm anyone. Nevertheless, the opportunity to discover insurgent hideouts, bomb-making factories, and weapons caches demonstrate the vast potential of Wide Area Airborne Surveillance systems, even while real-time data analysis remains a bottleneck.

Smaller Information-Gathering Robots

In addition to ISR sensor systems mounted on Global Hawks, Sentinels, Predators, and other large UAVs, the military utilizes smaller robots to gather information. On the ground and in the air, these robots operate on the tactical level, improving soldiers' battlefield awareness. This can reduce strong actors' informational disadvantage in asymmetric war, especially in urban environments, as soldiers move along roads, through alleyways, and into buildings.

The RQ-11 Raven, made by AeroVironment, is a small unmanned aerial system that carries video, electro-optical, and infrared cameras, enabling it to gather information day and night. Weighing between 4.2 and 4.8 pounds with a wingspan of 4.5 feet,[345] it uses an electric motor to fly up to a maximum of 15,000 feet above sea level, though it more frequently operates and achieves maximum performance around 500 feet above the ground, and can remain aloft for up to 90 minutes. With a flying speed between 28 and 60 mph, the Raven's range is effectively 10 kilometers. The three cameras transmit information to a ground control station, which can display the images in real-time or store them for future analysis. Together, a Raven and its ground control station cost approximately $250,000. The United States granted AeroVironment a contract to produce 2,358 Raven systems, and

[345] "UAS Advanced Development: Raven RQ-11A" and "UAS: Raven RQ-11B."

additional units have been purchased by American allies, including Australia, Italy, Denmark, the Netherlands, the UK, and Spain.[346]

Unlike larger UAVs, such as the Predator or Global Hawk, the Raven is carried by and operated by soldiers in the field. The Raven launches when a soldier throws it in to the air, using an over-the-shoulder motion similar to throwing a javelin.[347] Once in the air, it can be directed manually via the ground control station, or fly autonomously according to pre-programmed specifications using its GPS system. The Raven also lands autonomously and does not require a prepared landing strip, making it well-suited for forward-deployed units, especially in harsh terrain.[348] However, some soldiers have complained that the Raven is difficult to launch and crashes often, requiring frequent repairs or replacement.[349]

AeroVironment also makes a smaller "micro air vehicle" known as the Wasp. Less than a foot long, with a wingspan of 28.5 inches, the Wasp weighs only one pound, making it highly portable and easy to throw. It carries two cameras, each approximately the size of a peanut,[350] that can gather information day and night, and, like the Raven, transmits the information it gathers to a ground-based control station. Using an electric motor with rechargeable lithium ion batteries, it can travel at speeds ranging from 20 to 40 mph, reach heights of 1,000 feet above ground level, and fly by remote control or autonomously using GPS and an internal navigation system.[351] Unlike the Raven, the Wasp comes in an "all environment" version capable of full functionality at sea, as well as on land.[352] Each system—plane and control station—costs approximately $50,000.[353]

[346] "RQ-11 Raven Unmanned Aerial Vehicle."
[347] Singer, "Wired for War," p. 37.
[348] "RQ-11 Raven Unmanned Aerial Vehicle."
[349] "Why Soldiers Hate the Raven UAV."
[350] Singer, "Wired for War," p. 37.
[351] "Wasp III."
[352] "UAS: Wasp AE."
[353] "Wasp III."

Small UAVS, like the Raven and the Wasp, provide soldiers with the ability to gather information about their surroundings at their discretion. Instead of requesting assistance from a nearby ISR drone, and having to wait for a response, they can direct a small UAV to quickly acquire relevant information. With a Raven or Wasp, soldiers can look over hills or onto rooftops, scout ahead to the next city block, around a curve on a mountain path, or a few miles down a road, and observe their immediate vicinity from a better vantage point. This gives them lead time to prepare for approaching circumstances, such as a potential encounter with civilians or enemy fighters, and a layout of the terrain in which it could take place. Perhaps most importantly, aerial observation could give soldier advance notice of an ambush, or at least help them locate the source of incoming fire and determine the easiest way to counter it.

Recently deployed tiny helicopters provide a smaller and more maneuverable alternative to these small planes. Beginning in 2012, British forces in Afghanistan began utilizing a "nano helicopter" drone known as the Black Hornet produced by the Norwegian company Prox Dynamics.[354] Officially called the PD-100 PRS (for "Personal Reconnaissance System"), the Black Hornet is four inches long and weighs only 16 grams (about half an ounce), easily fitting in the palm of an adult's hand. Despite its small size, it is capable of operating in windy conditions, can fly up to 22mph, and remain in the air for a maximum of 25 minutes at a time before its batteries require recharging.[355] It launches from a small base station, which, together with the drone, weighs less than a kilogram and can fit inside a pants pocket. Like the Raven and Wasp, the Black Hornet can be piloted remotely using a hand-held controller, follow a pre-programmed course, or utilize GPS to autonomously survey a designated area.[356]

[354] Hill, "Toy-Size Helicopter Drones Now on Surveillance Duty in Afghanistan."
[355] "PD-100 PRS – Your Personal Reconnaissance System."
[356] Hill, "Toy-Size Helicopter Drones Now on Surveillance Duty in Afghanistan."

Essentially a flying camera that can provide real time video or still photos with a maximum visual range of 1,000 meters, the Black Hornet provides ISR capability to individual soldiers. While large UAVs, like the Global Hawk or Predator, typically serve theaters and are operated from remote command centers, and smaller UAVS, such as the Raven, typically serve a platoon, the Black Hornet can serve soldiers as they operate within a squad. Each nano helicopter launches itself, requires minimal training and no pilot experience to fly, and transmits information back to a small display unit.[357] It is thus possible for multiple soldiers in a small, 8-12 man unit to each operate a Black Hornet, looking in multiple directions at the same time, or maintaining ISR capabilities even if they split into smaller sub-units.

Nano UAVs can therefore help small groups of soldiers overcome asymmetries of information as they advance over open ground, patrol streets, or raid buildings. These actions are among the most dangerous counterinsurgents can undertake, as they expose soldiers operating in the open to fire from hidden locations. However, by flying ahead of soldiers, nano helicopters can help determine the location of enemy positions, and give advance notice whether people are armed fighters or civilians. According to British Sergeant Christopher Petherbridge of the Brigade Reconnaissance Force in Afghanistan, the "Black Hornet is definitely adding value, especially considering the lightweight nature of it. We use it to look for insurgent firing points and check out exposed areas of the ground before crossing, which is a real asset."[358] Additionally, because they are so small, they can operate inside buildings as well as outside, and are sufficiently quiet as to attract minimal attention.[359] In Afghanistan, British soldiers have used them to see around corners and into rooms.[360] The British Ministry of Defense granted a contract to Prox Dynamics for 20 million pounds (approximately $31

[357] "PD-100 PRS – Your Personal Reconnaissance System."
[358] Quoted in "Miniature surveillance helicopters help protect front line troops."
[359] "PD-100 PRS – Your Personal Reconnaissance System."
[360] Hoffman, "British soldiers flying nano helicopters in Afghanistan."

million) to provide 160 Black Hornet systems,[361] and, based on the positive early reviews, other countries will likely follow suit.

Besides aiding soldiers by looking beyond their line of sight, small UAVs can be used for electronic surveillance. In 2011, at the Black Hat and DEFCON security conferences, which feature hackers and computer security professionals, two security consultants and engineers, Mike Tassey and Richard Perkins, presented a homemade drone known as a Wireless Aerial Surveillance Platform (or WASP—no relation to the small ISR drone by AeroVironment known as a Wasp) that can spy on both wireless computer networks and cell phones.[362] This UAV is 76 inches long, with a wingspan of 67 inches, and can remain in the air for 30-45 minutes with a maximum altitude of 22,000 feet.[363] The WASP can hack password encrypted Wi-Fi computer networks, and also act as a GSM antenna (Global System for Mobile), which allows it to intercept cell phone calls and text messages.[364] Any cell phone that is closer to the WASP than a cell tower will connect with the drone first, allowing it to gather any information sent to or from nearby mobile devices.

Tassey and Perkins, who have experience working for the US intelligence and defense communities, built the drone to prompt new developments in electronic security by demonstrating the potential risks to electronic communications, but it offers apparent intelligence-gathering capabilities as well. A WASP could intercept insurgent communications and gather information off of militants' computers without their knowledge. This would allow intelligence analysts to monitor communications insurgents believe to be secret, in which they might discuss strategy, identify members, or plan attacks. Even if a terrorist network discovered the WASP's capabilities, the result

[361] “Miniature surveillance helicopters help protect front line troops.”
[362] Greenberg, “Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones.”
[363] “About Us,” *the Rabbit-Hole*.
[364] Humphries, “WASP: The Linux-powered flying spy drone that cracks Wi-Fi & GSM networks.”

would be avoidance of wireless networking or cell-phones, which would greatly hinder their ability to communicate.

Not all small information-gathering robots are airborne. The Scout XT, from Recon Robotics, is a “throwbot,” a small ground-based robot that soldiers can throw over walls or into buildings. It looks like a rolling dumbbell with antennae: a cylindrical tube with a wheel on each end in place of the weights. The Recon Scout weighs 1.2lbs and can be thrown up to 120 feet. Upon landing, its camera and microphone switch on and transmit data back to a hand-held control unit, which a soldier uses to direct the robot. The Scout includes infrared, as well as ambient light cameras, enabling operation in both dark and light conditions.[365] In demonstration videos, the Scout proved its durability by falling 30 feet onto a concrete surface, bouncing, and then rolling along as normal.[366] Together, the robot and its control unit weigh three pounds, making it easily transportable by individual soldiers. In early 2012, the US Army awarded a $13.9 million contract to Recon Robotics for 1,100 Scouts, the largest order in the company's history.[367]

The tactical advantages of the Scout are similar to those of the Black Hornet, with a few noticeable differences. The Recon Scout is quiet, operating at just 22 decibels.[368] To put that in perspective, a typical refrigerator hums at 40 decibels, and a human whisper is around 30 decibels.[369] Therefore, like a nano helicopter, the Scout can stealthily look around corners and enter rooms ahead of soldiers, sending back information that can alert them to potential dangers. Comparatively, the main disadvantage of a Scout is that it rolls rather than flies, which means it cannot climb stairs or view a scene from above. However, it is far more cost effective. Based on recent orders, each Scout costs less than $13,000, while each Black Hornet costs just under $200,000.

[365] “The Throwbot XT with Audio Capabilities.”
[366] “The Military's New Weapon: Mini Spy Robots You Throw Like Grenades.”
[367] “Army Orders 1,100 Recon Scout XT Robots from ReconRobotics.”
[368] “The Throwbot XT with Audio Capabilities.”
[369] “Decibel Levels of Everyday Sounds.”

To illustrate how new technologies can overcome asymmetries of information, consider the microcosm of combat between a squad and a sniper. With more people and more guns—plus, perhaps, mortars, RPGs, and the ability to request assistance from tanks and aircraft—the squad of soldiers enjoys a considerable resource advantage over an individual sniper, or two-man sniper team. However, the sniper can threaten the squad because of his advantage regarding an asymmetry of information. The sniper is hidden, his location unknown to the squad. By contrast, the soldiers are on patrol or advancing in the open. As such, the sniper can capitalize on surprise, shoot at the squad, and continue shooting with relative security until the soldiers discover his location. In settings with considerable cover, such as cities or jungles, the sniper can shoot and quickly move to a new spot. A squad of soldiers from a powerful military could easily defeat a sniper team, if they knew its location. However, as long as the snipers remain hidden, their informational advantage neutralizes the squad's resource advantage.

To overcome this informational disadvantage, the squad could use recently developed gunfire detection systems. These anti-sniper systems utilize sound detection to determine the location of a gunshot. For example, the Boomerang Mobile Acoustic Shooter Detection System (MASDS) from BBN Technologies, a subsidiary of Raytheon, identifies the location of a shooter to plus-or-minus 15 degrees accuracy within one second of the shot. According to BBN, the MASDS can detect fire from AK-47s and other small arms at ranges of 50 to 150 meters, and can operate on a vehicle moving up to 60 miles per hour.[370]

An alternative that does not require a separate system is the Robot Enhanced Detection Outpost with Lasers (REDOWL) addition to the commonly used PackBot from iRobot.[371] In conjunction with the Photonics Center at Boston University, iRobot has developed a system that combines optic and

[370] Crane, “Anti-Sniper/Sniper Detection/Gunfire Detection Systems at a Glance.”
[371] Sofge, “5 Robots We Should Deploy Right Now,” p. 4.

acoustic sensors to pinpoint the origin of gunfire. It utilizes an algorithm based on human hearing to process acoustic information, as well as daylight and low-light cameras, thermal imaging, a laser range finder, and GPS positioning to locate the shooter day or night and shine a laser pointer at the shot's point of origin. In firing range field tests for the Army's Rapid Equipping Force, the REDOWL system demonstrated a 94% success rate locating the origin of shots from M-16 and AK-47 rifles at more than 100 meters.[372]

While these and other gunfire detection systems have proven their capabilities in controlled demonstrations, they have yet to be deployed to combat zones. The systems are not able to distinguish friendly weapons and calibers from hostile fire, and the robot becomes useless, or potentially a little dangerous, in a firefight. As shots ring out from all sides, the robot's head goes “into a laser-aiming seizure,”[373] swinging around wildly. This negates its capability and creates the risk that it will hit, or shine its laser pointer into the eyes of, a friendly soldier.

Despite these technical issues, development of gunfire detection systems will continue, because the potential advantages are considerable. The ability to locate the origin of gunfire would neutralize the informational advantage that allows a sniper to threaten a squad of soldiers, and would allow soldiers to respond more effectively to ambushes. If the REDOWL or similar systems can remain focused on the first shot, or can learn to distinguish nearby fire by friendlies from more distant fire by enemies, they will enhance strong actor capabilities by allowing soldiers to assert their resource advantage against hidden foes.

[372] Ibid.
[373] Ibid.

Conclusion

Relatively weak actors engaged in asymmetric warfare exploit non-material asymmetries to combat strong foes, especially regarding information. However, advancements in robotics and computing technology can help strong actors overcome these asymmetries and reassert their resource advantage. This is already apparent from the American-led asymmetric conflicts in Iraq and Afghanistan, where unmanned systems on the ground and in the air have decreased strong actor casualties, improved the efficiency of targeting and reduced collateral damage, and revolutionized information acquisition. As robotics technology continues to advance, unmanned systems will play an increasing role in military strategy.

Chapter 5: Robotics and Non-State Networks

As with any new technological development, it is tempting to overstate the potential advantages robots can provide to the states that produce them and downplay the risks. As the robotics revolution progresses and the technology spreads, actors with fewer resources will find it easier to acquire unmanned weapons and information-gathering systems. These robotic systems appeal to networks for the same reasons they appeal to states: as a method of acquiring information or striking targets without risking personnel. Given the overwhelming resource advantage enjoyed by states relative to non-state networks, terrorist or insurgent groups will almost certainly not develop their own squadrons of aerial or ground-based robots. However, with more and more countries producing and selling military robotics technology, it becomes increasingly likely that networks could purchase some through the black market or receive some from state sponsors, much as they acquire firearms or explosives.

While many of the most notable developments in the field of robotics have been military in nature, the robotics revolution will increasingly feature commercially available automated systems. In the early 21st century, numerous non-military versions of ground-based and aerial robots have become available for use by individuals and businesses, and, as with earlier inventions like personal computers or cell phones, this trend will likely accelerate. From driverless cars to small UAVs that shoot movies or deliver food, a large variety of privately controlled robots will become increasingly commonplace in developed countries. Inadvertently, this will provide relatively weak actors, from individual self-starters to organized non-state networks, with robots they can adapt to enhance their capabilities in asymmetric warfare.

Acquiring Military Robots

Attacks from large unmanned aircraft operated by networks in localized insurgencies or irredentist conflicts are unlikely to pose a strategic risk to powerful militaries. Given their resource advantage, states have little difficulty maintaining air superiority in state-network conflicts. With the airspace above any active theater monitored by radar, and the location of friendly aircraft known, any drone large enough to carry missiles is unlikely to escape notice. If states detect an unfriendly or unidentified Predator or similar UAV flying in airspace they control, they could target it with ground-based air defense systems. Alternatively, interceptor aircraft could engage and destroy the enemy drone, much as an Iraqi MiG shot down an American-operated Predator in 2002. States will likely feel few qualms firing on unidentified or potentially hostile unmanned aircraft, as there is no chance that a pilot will be killed, and thus less risk of accidentally harming an innocent or creating an international incident.

However, if insurgents acquire smaller drones that fly low to the ground and could escape radar detection, such as a Switchblade, they could pose a threat to ground forces with kamikaze attacks. Such robotic non-line-of-sight weapons are far more maneuverable and accurate than the alternative measures of striking targets at a distance employed by weaker actors fighting powerful militaries, such as mortars or crude rockets. Small UAVs fly considerably slower than rockets, which means they would present easy targets for the automated C-RAM systems that protect bases, ships, and convoys; but counter-rocket-and-mortar systems would not protect soldiers that venture outside of bases, in groups smaller than a defended convoy. Smaller units operating in urban environments would be especially vulnerable to kamikaze drones, since insurgents could direct them from covered positions, using the UAV's camera to locate their target. With its flight time of 20-40 minutes and effective range of 10km, a Switchblade could provide urban guerrillas with an effective method of attacking exposed soldiers or unarmored vehicles without revealing their location.

While fortified military areas may be able to counter the UAV capabilities that non-state networks could acquire, small drones in the hands of terrorist or insurgent groups could prove especially threatening to non-combatants, including in developed countries. An individual operative could crash a Switchblade or a similar UAV into populated areas, such as a market, causing damage on the scale of a small bomb planted on the ground. Once an attack is in progress it would be difficult to stop, since aircraft tracking and anti-air defense systems are designed to monitor and potentially shoot down larger aircraft flying higher above the ground, and C-RAM systems would be impractical in densely populated areas due to the possibility of falling debris and the massive cost of protecting everywhere at once.

As with other military technology, governments can restrict the sale of small and large UAVs to friendly states. For example, the United States only permits General Atomics and other defense contractors to sell unmanned aircraft to allied governments, primarily members of NATO. European companies such as AeroVironment, the maker of small UAVs including the Raven and the Switchblade, face similar restrictions, as do drone makers in Israel and other non-European US allies. It is unlikely, however, that other countries with emerging UAV manufacturers, such as China, Russia, and Iran, will only allow sales to governments friendly with the United States, or that any purchasers or manufacturers will refrain from reselling or granting drones to non-state actors.

In February 2013, General Atomics reached an agreement to sell an undisclosed number of unarmed Predators to the United Arab Emirates for $197 million, which, pending authorization from Congress, would be the first time an American company sold large drones to a non-NATO ally.[374] Even though this potential sale only includes RQ models designed for reconnaissance, rather than the

[374] Hennigan, W.J., “United Arab Emirates set to buy U.S. Predator drones.”

MQ models outfitted with weapons, it has drawn some scrutiny because of the possibility that the UAE will use the Predators for domestic spying and repression of political dissidents. Additionally, some critics have raised the possibility that terrorist groups could steal or purchase a Predator from the UAE, though they have not presented any evidence in support of this speculation.

While this potential sale provides further evidence that the number of countries acquiring UAVs continues to expand, it also demonstrates the political barriers and prohibitive monetary cost that make it unlikely that non-state networks will acquire Predators or other large UAVs, whether legally or illegally. Governments have strong incentives to prevent theft of any weapons they control, and there is no known instance of a terrorist group stealing manned military aircraft, which indicates that Predator theft is probably not a serious risk. Sales to foreign entities by UAV-manufacturing defense contractors that do their primary business with the United States and American allies require governmental authorization, and any country suspected of transferring the technology to others would likely forfeit the ability to acquire more drones or the parts necessary for maintenance. While UAV manufacturers based in unallied or adversarial countries may sell to different clients, they are also likely to punish unauthorized transfers by cutting off future sales of aircraft and parts. The incentives for states to control military-grade drone technology reduce the risk that large UAVs will be stolen or sold illegally.

Even if a state decides to sell large drones it has manufactured or purchased to a non-state network, or rogue members of a military try to sell some on the black market, the cost is likely too high to be practical for non-state actors. At its high point in the late 1990s/early 2000s, al Qaeda's annual operating budget was approximately $30 million according to the CIA.[375] Since September 11, 2001, efforts to track and freeze the funds of al Qaeda's financiers and various charitable or business fronts by the United States Treasury Department, other governments including the UK and Saudi Arabia, and

[375] Vardi, Nathan, “Is al Qaeda Bankrupt?”

international bodies such as the Financial Action Task Force,[376] have reduced this considerably. With each RQ-1 Predator costing approximately $4 million and each MQ-1 Reaper costing $30 million when legally purchased in bulk by the United States, large UAVs are too expensive for non-state networks, even before accounting for black market premiums.

Spending that much on a large drone would go against the cost-effectiveness at the core of weak actor strategy. For comparison, the largest attacks by al Qaeda or its affiliates cost considerably less than a single unarmed Predator drone. CIA estimates place the cost of the September 11th operation at approximately $500,000, while the 2004 Madrid train bombings cost $70,000, and the 2005 attacks on London's transit system cost only $10,000. According to Stuart A. Levey, the Under Secretary for Terrorism and Financial Intelligence in the US Treasury from 2004 to 2011, the majority of al Qaeda's funds go towards training, operatives' salaries, travel and the purchase of travel documents, payments to families of suicide bombers, and bribes for public officials.[377] Therefore, it would make little strategic sense for al Qaeda or any other non-state network to spend so much money to acquire a Predator drone, especially given that one could be easily spotted by strong actors' radar and shot down.

Small UAVs, however, are considerably less expensive, and may prove attractive to terrorist or insurgent groups. Under contracts signed in 2011, each Switchblade cost approximately $100,000—which includes training and other services—while each observational Wasp drone cost $50,000. Though still expensive, these or similar drones would not break the bank for a well-funded network. More likely, since small UAVs are easier to produce than the large alternatives, cost less, and can be operated by individuals with little training, states may be willing to give them to networks that they sponsor.

[376] “What is the FATF?”
[377] Vardi, Nathan, “Is al Qaeda Bankrupt?”

On October 6, 2012, Israel shot down a small drone in the northern Negev, near its border with the West Bank, for which Hezbollah claimed responsibility. According to Hassan Nasrallah, the Lebanon-based group's leader, the drone was manufactured in Iran, assembled in Lebanon, and used for "reconnaissance flights inside occupied Palestine."[378] This was not the first time that Hezbollah flew Iran-provided UAVs over Israeli territory.

The first flight occurred in late 2004. The unidentified drone model flew around 1,000 feet above the ground, escaping detection by Israeli radar due to its small size and low altitude. It was spotted by an Israeli officer on the ground near the Lebanese border. The UAV spent approximately five minutes in Israeli airspace, before turning west towards the Mediterranean Sea, where it crashed. Israel's military interpreted the incursion as a demonstration of capabilities, and initiated a review to determine how the flight originally escaped notice.[379]

In April 2005, Hezbollah flew an Iranian-made Mersad UAV over northern Israel. The Mersad, also known as a Mohajer (which means "migrant" in Persian), was first developed in the 1980s by Ghods Aviation, an Iranian company, for reconnaissance in the Iran-Iraq war. In the years since, Ghods built four versions of the Mohajer, the most recent of which is approximately three and half meters long and capable of flying as fast as 135 miles per hour for a short while, with an operational range of approximately 100 miles. The Mohajer-4 underwent a successful flight test in February 2002, and, unlike the original version, includes autopilot, superior cameras, and the ability to paint targets with a laser for guided munitions.[380] According to a diplomatic cable from the American embassy in Beirut released by WikiLeaks, Iran provided Hezbollah with three Mersads in 2004 or 2005, one of which was operational at the time of the flight into Israeli airspace. Sources in Syria and southern

[378] Barnett, "Hezbollah takes responsibility for last week's drone over Israel."
[379] Harel, "Air Force: Hezbollah drone flew over Israel for five minutes."
[380] "Mohajer (UAV)."

Lebanon indicated that Syrian intelligence assisted with the Mersad's launch, which flew over Israel to gather information and demonstrate Hezbollah's growing unmanned capabilities.[381]

In the 2006 war between Israel and Hezbollah, there were at least three incidents in which the Israeli Defense Forces shot down Hezbollah-controlled Ababil UAVs over Israel.[382] Also built by Ghods, the Ababil (which means "swallow" in Persian), is slightly under three meters long, but more aerodynamic than the Mohajer, giving it a top speed of approximately 185 mph, and an operational range of 150 miles. Its ISR capabilities operate similarly to a Raven, with images transferred to a ground-based control station. Though decently larger than the Switchblade, the Ababil launches out of a similar pneumatic tube mounted on a truck or via a rocket launch system.[383] It therefore does not require a runway to takeoff.

While the Ababil was primarily designed for ISR missions, it is capable of carrying a single warhead with up to 50 kg of explosives.[384] Of the three Ababils shot down by Israel in the 2006 war, at least one held 30 kg of explosive material.[385] Israeli forces recovered the explosives from an Ababil intercepted by an Israeli F-16, and suspected that one additional drone of the three they shot down was carrying a similar payload, while the remaining Ababil was probably outfitted exclusively for surveillance.[386] In the years since its 2006 conflict with Israel, Hezbollah has reportedly acquired additional Ababils from Iran, some of which carry 45 kg warheads.

These flights demonstrate that advancements in robotics can enhance the capabilities of relatively weak actors in asymmetric conflicts, as well as those of their stronger opponents. With kamikaze drones providing a more accurate method of attacking strong actor soldiers than mortars or rockets, networks could create more casualties and deny their enemies an easy victory, weakening the

[381] "Syrian Intelligence May Have Worked with Hizballah on UAV Launchings."
[382] Ephron, "Hizbullah's Worrisome Weapon."
[383] "Ababil (Swallow) Unmanned Aerial Vehicle."
[384] Bergman, "Hezbollah boosting drone unit."
[385] Harel et. al., "Hezbollah drone brought down over Galilee held 30 kg of explosives."
[386] Bergman, "Hezbollah boosting drone unit."

strong actor's resolve. Similarly, in irredentist conflicts such as that between Israel and Hezbollah, where the fighting takes place in close proximity to the strong actor's territory, UAVs equipped with explosives could threaten nearby civilian populations, enhancing strategies built around the asymmetries of responsibility and expectations. While Hezbollah expects to face significant casualties when resisting militarily superior Israel, and is therefore not considered responsible for protecting all areas of Lebanon at once by its supporters, Israelis expect decisive victory and minimal casualties, especially among civilians inside Israel proper, when facing a weaker opponent. By improving networks' ability to kill strong actor soldiers and civilians, kamikaze drones can help them impose additional costs that convince their stronger opponents to halt offenses, negotiate ceasefires, or withdraw forces.

In addition to the destructive capacity of smaller drones that carry an explosive charge, the information gathering capabilities of small UAVs can enhance weak actor strategies as well. In 2006, Israeli ground forces advancing on Hezbollah-controlled positions in the mountains of southern Lebanon faced fierce resistance. Despite a significant resource advantage, with 30,000 soldiers backed by armored vehicles and aircraft against an estimated 10,000 fighters, Israel was unable to secure southern Lebanon or advance more than a few miles to the Litani River. Before withdrawing, the Israeli Defense Forces lost 116 soldiers,[387] with an additional 628 wounded, while Hezbollah lost an estimated 600 fighters with as many as 1,500 wounded.[388]

Nasrallah claimed that Hezbollah's success was in part attributable to a cell phone network, which enabled his forces to share the location of Israeli troops that they spotted.[389] By sharing this information, Hezbollah forces could move through the tunnel system they prepared in southern

[387] “Middle East Crisis: Facts and Figures.”
[388] Cordesman, “The Lessons of the Israeli-Lebanon War,” p. 16.
[389] “Nasrallah hits out at government.”

Lebanon to mass at the point of the Israeli attack or raid weaker sections of the Israeli columns.[390] Following guerrilla strategy, Hezbollah used the element of surprise to ambush Israeli forces, and retreated when overwhelmed, combining the techniques of hit-and-run and defense-in-depth. If Hezbollah could have used small ISR drones to gather information about the advancing Israeli forces, they would have been in an even better position to anticipate Israeli troop movements, and prepare their defenses accordingly.

Small ISR drones would thus increase Hezbollah's advantage regarding the asymmetry of information. As an invading force entering mountainous territory with which their opponent was intimately familiar, Israeli troops were at an informational disadvantage. Hezbollah scouts could observe the movements of Israeli columns climbing the foothills or moving through passes, while most of their forces remained hidden in tunnels. When Hezbollah fighters launched rockets into Israel from fixed batteries or the backs of trucks, they would reveal their location to Israeli radar and aerial surveillance, after which Israel would attempt to destroy the rocket batteries with targeted missiles. However, Israel's cameras mounted on satellites, manned, and unmanned aircraft could not see the underground movement of Hezbollah guerrillas or differentiate between civilian vehicles and trucks carrying covered rockets. Hezbollah utilized this informational asymmetry to shoot almost 4,000 rockets into Israel over the five weeks of conflict,[391] killing 43 civilians and causing “serious” or “moderate” wounds to an additional 76.[392]

If Israeli forces had been able to secure southern Lebanon, they would have greatly reduced Hezbollah's ability to fire rockets into populated areas of Israel. The maximum range of a Katyusha rocket, which made up the vast majority of Hezbollah's arsenal in 2006, is approximately 25km. When fired from across the Lebanese border, this limited range makes Katyushas only capable of threatening

[390] Cordesman, “The Lessons of the Israeli-Lebanon War.”
[391] Cordesman, “The Lessons of the Israeli-Lebanon War,” p. 3.
[392] “Middle East Crisis: Facts and Figures.”

northern Israel.[393] Major population centers are farther from the Israel-Lebanon border, with Tel Aviv about 100km away. Israeli airstrikes and ground incursions were able to destroy numerous rocket launchers, but unable to prevent daily rocket fire throughout the conflict. This inability to prevent an ongoing threat to its civilians likely contributed to Israel's willingness to accept the UN-brokered ceasefire.

In the years since the 2006 conflict, Hezbollah has reportedly rearmed, acquiring missiles with greater range. This has allowed them to set up defended missile batteries further from the Israel-Lebanon border in anticipation of another Israeli ground invasion.[394] In November 2012, at an event marking the Day of Ashura, Hezbollah displayed a Fajr-5 missile it acquired from Iran.[395] The Fajr-5 has a maximum range of 75km, which, if fired from the Lebanese border, could easily hit Haifa and potentially reach the suburbs of Tel Aviv. It is larger and flies faster than Katyusha rockets, making it more difficult for C-RAM systems, such as Israel's Iron Dome, to shoot down. Even with a robust Iron Dome presence on the Lebanese border, some missiles would likely get through. This increases the importance for Israel of securing territory further into Lebanon to push Hezbollah out of range of its largest population centers and disable the batteries stationed farther from the border.

However, with unmanned aircraft observing Israeli movements while Hezbollah's forces remain hidden until firing, Hezbollah would enjoy a larger informational advantage if Israel attempted to invade southern Lebanon again in the future. Mersad or Ababil drones could spot Israeli ground forces at a distance, granting Hezbollah greater lead time to mass forces or move rocket launchers. With Hezbollah forces moving through tunnels or other prepared cover, they would be difficult for Israeli UAVs to spot from the air. Therefore, in the event of another Israel-Hezbollah war, unmanned aircraft

[393] “Hezbollah's rocket force.”
[394] Schneider, “Hezbollah rearms away from border.”
[395] “Hezbollah Displays Iranian Fajr-5 Missile.”

have the potential to increase Hezbollah's advantage regarding the asymmetry of information, improving their ability to deny Israel victory.

In addition to guerrillas resisting military advances into rough terrain, urban insurgents could enhance their informational capabilities utilizing small unmanned aircraft. A fixed or rotary wing UAV with a camera that transmits video to a ground station would allow insurgents to monitor the movements of strong actor soldiers. This could help them determine the patterns of patrols, which would improve their ability to set up roadside bombs and plan ambushes. By watching the streets near any meeting locations, safe houses, bomb-making factories, or weapons caches they could anticipate raids from strong actor soldiers. This would provide insurgents with some advance notice, granting them a window of opportunity to disperse, and for them to hide or destroy incriminating material. Small ISR drones could therefore enhance the informational capabilities of localized insurgencies, such as those fought in Iraq or Afghanistan against American and allied forces.

Adapting Commercially Available Robots

Unlike Hezbollah, many networks do not enjoy significant state sponsorship, and therefore may not be able to acquire military UAVs like the Mohajer or Ababil. However, that might not be necessary, since unmanned technology is becoming increasingly available for commercial use. Even if they are unable to acquire small UAVs on the black market or from state sponsors, networks or individuals could adapt aerial and ground-based non-military drones into weapons or information-gathering systems. Any remotely-controlled vehicle with a camera that can transmit real-time video could function as a basic ISR platform. Add some explosive material and any small robot could act as the crude equivalent of a Switchblade and perform a kamikaze attack.

Commercially Available Aerial Robots

The commercial drone industry in the United States is in its infancy, and expected to grow dramatically in the coming years. Beginning the process of opening the skies to legal use, a new federal law passed in February 2012 (H.R. 658, the FAA Air Transportation Modernization and Safety Improvement Act) instructed the Federal Aviation Administration to allow various types of privately-controlled unmanned aircraft by 2015. As of 2013, hobbyists can legally fly small "recreational" UAVs short distances at low heights (under 400 feet, always within the operator's line-of-sight), just as they have long been allowed to fly model airplanes, but commercial interests cannot. At the time of the bill's passage, the overall UAV market was valued at $5.9 billion, and expected to at least double over the next ten years.[396] By 2020, according to FAA estimates, as many as 30,000 private and government drones could be legally flying over the United States.[397]

Small UAVs, ranging in cost from less than one hundred to almost one million dollars, have proliferated in the early 21st century. Like the comparatively complex and expensive military UAVs, many of these commercial drones gather information. Some are as simple as a camera attached to a model airplane, or a video camera held aloft by multiple rotaries, or "multicopter," gathering aerial photographs of properties for real estate agents, taking pictures or videos of celebrities for paparazzi, or monitoring the location of livestock while feeding live images to farmers through a wireless connection. Larger and more expensive commercial drones combine video cameras with infrared sensors, and are used by a variety of organizations, from law enforcement agencies gathering surveillance for SWAT teams or searching wooded areas for missing persons, to oil companies tracking

[396] Wingfield and Sengupta, "Drones Set Sites on U.S. Skies."
[397] Sasso, "Hollywood wants drones for filmmaking."

spills. Additional, non-informational uses include crop dusting, managing road traffic after accidents, and dropping water on wildfires.[398]

Perhaps the biggest proponent of legalizing commercial drone use is the film industry. The industry's primary lobbying group, the Motion Picture Association of America (MPAA), first disclosed in October 2012 that it has been pushing the FAA to authorize filmmakers' use of unmanned aircraft in US airspace.[399] The industry plans to make use of small fixed-wing and rotary UAVs to shoot film from the air, in place of current methods that are more expensive, more restrictive, and potentially more dangerous. According to MPAA spokesman Howard Gantman, cameras on small unmanned aircraft would enable directors to utilize innovative camera angels, and “could be used much more safely than going up a tree and much more cheaply than renting a helicopter.”[400] For comparison, studios looking to capture footage from the air typically rent helicopters for $1,700 per hour, plus an additional $1,900 per day for a pilot, while a drone that could accomplish the same task could retail for less than $1,000.[401] This economic incentive and the associated lobbying efforts from one of America's largest industries will likely lead the FAA to adapt rules allowing considerable private drone use.

Other countries have already allowed movie studios to utilize unmanned aircraft. The Belgian company Flying-Cam leases an unmanned aerial system called the Special Aerial Response Automatic Helicopter, or SARAH. The SARAH is an automated helicopter weighing 55lbs that can take off and land vertically, and remain in the air for 30 minutes. Designed for commercial filming, it includes a stabilized “Gyro Head” that carries a high resolution digital camera, and is capable of both recording and broadcasting live.[402] Eon Productions, a UK-based film production company, utilized a SARAH to shoot some footage in Istanbul in 2012 for the James Bond film *Skyfall.* The drone followed alongside

[398] Wingfield and Sengupta, “Drones Set Sites on U.S. Skies.”
[399] Sasso, “Hollywood wants drones for filmmaking.”
[400] Teinowitz, “Hollywood to the FAA: Let Us Use Drones!”
[401] Ibid.
[402] “The Totally New SARAH Unmanned Aerial System.”

007 as he chased after a train on a motorcycle, all while maintaining a steady horizon and adjusting speed when necessary.[403]

There is little effective difference between unmanned systems designed to help movie directors capture an aerial shot and information-gathering UAVs built for military purposes. Besides size, and a higher resolution camera, the SARAH is functionally equivalent to the Black Hornet miniature unmanned helicopters used by soldiers in Afghanistan. That means a non-state network could acquire a drone designed for commercial filming and use it to film strong actor soldiers or scout locations for attacks. The broadcast feature would enable real-time monitoring of a given area in a manner similar to military ISR drones, while the recording feature would allow a network to film a potential target and study its security to discover ways to increase the chances an attack will succeed.

While aerial shots for movies may be an apparent use for unmanned aircraft, there are other, less obvious potential commercial uses, such as food delivery. In late 2012, researchers at Darwin Aerospace in San Francisco designed the Burrito Bomber, a small unmanned plane capable of dropping an item—in this case, Mexican food—via parachute to a pre-programmed target.[404] The engineers at Darwin Aerospace got the idea from the conceptual Taco Copter, a Mexican-food delivery multicopter that attracted attention on the internet in early 2012, but was never actually built. John Boiles, one of the designers, explained that they focused on burrito delivery because “Mexican food is really popular” and “burritos are kind of bomb-shaped.”[405]

The Burrito Bomber may sound ridiculous, but it provides further evidence that robotics technology will continue to spread and become increasingly available for civilian use. In the course of a few decades, unmanned aircraft will have transitioned from the military, to other government agencies and large corporations like movie studios, to individuals and smaller businesses, such as

[403] “Flying-Cam and Bond 007 'Skyfall.'”
[404] Janik and Armentrout, “Industry looks to use drones for commercial purposes.”
[405] Koebler, “Burrito Bomber Attacks Hunger with Drone-Delivered Mexican Food.”

restaurants that deliver. Like other technologies, as robots become more ubiquitous, they will become cheaper and easier to acquire. That means that, much like information technology, smaller, commercially available aerial drones will end up enhancing the capabilities of non-state networks.

Networks could acquire any of these commercially available UAVs, through legal or illegal means, and put them to use against relatively stronger actors. Insurgent organizations could use information-gathering drones to monitor counterinsurgent troop movements, helping them set up ambushes or avoid raids. Terrorists and saboteurs could scout the security of potential targets to determine the ideal time and location to strike. Or they could simply load a drone with explosives and fly it into a target. This would fulfill a similar function as a car or truck bomb, but would be able to fly over barriers, and would not require sacrificing a driver. Unfortunately, it would not be surprising if, in the next decade or two, a terrorist loaded a commercial drone with explosive material and tried to crash it into a building, bridge, or crowded area in the United States or another economically developed country.

The FBI has already thwarted one such attack in the planning stage. In July 2012, Rezwan Ferdaus, an American citizen who was born in Massachusetts and received a degree in physics from Northeastern University, pleaded guilty to charges of attempting to destroy or damage a federal building and providing material support to terrorists.[406] Ferdaus was arrested in September 2011 after outlining his plan to FBI agents posing as al Qaeda operatives—in which he intended to crash drones loaded with explosives into US landmarks including the Pentagon and the Capital building—and accepting delivery of hand grenades, AK-47s, and C-4 plastic explosives. Ferdaus had already designed and built cell phone-triggered detonators, obtained a remote-controlled replica of an F-86 Sabre using a false name, and scouted locations in Washington DC from which to launch the planes.[407]

[406] Bidgood, “Massachusetts Man Gets 17 Years in Terrorist Plot.”
[407] Johnson, “Man accused of plotting drone attacks on Pentagon, Capital.”

Modeled after the 1950s-era fighter jet, the F-86 replica is almost three feet long, requires extensive assembly, and retails for under $200.[408] Though authorities stopped this planned attack before it advanced to the execution stage, it presages the possibility of similar attempts in the future.

The type of remote-control model airplanes Ferdaus planned to use have been available for decades, though there is no publicly known case of someone else attempting to employ one in a terrorist attack. This suggests that he got the idea from the prevalence of military drone attacks in news reports of American activity in Afghanistan, Pakistan, and Yemen. According to the federal affidavit, Ferdaus was obsessed with using unmanned planes for an attack inside the United States, and saw himself as a devoted member of the global jihadist movement.[409] He had been under FBI surveillance since at least 2010, when he attempted to supply Iraqi insurgents with homemade cell-phone detonators for IED attacks against American soldiers.[410] Like many other self-starters, Ferdaus frequented jihadist websites, and claimed that discussions on those forums helped him realize that America is “evil” and that violent attacks against Federal targets in Washington DC could be his contribution to the “solution.”[411] He may have seen a kamikaze drone attack as quid pro quo for the American UAV campaign, or perhaps just thought that it would be the most effective method of delivering explosives.

After it became public, Ferdaus' plan was mocked on the DIY Drones internet forum, which calls itself “the leading community for personal UAVs.” One member pointed out that the model F-86 that Ferdaus planned to use requires “a substantial dedicated runway, and plenty of flying practice,” which means there was a decent chance that he would have crashed while trying to take off.[412] Others expressed relief that Ferdaus selected older model airplanes, rather than more modern personal-use

[408] “E-Flite F-86 Sabre 15 Ducted Fan Jet ARF.”
[409] Cacace, “Affidavit of Special Agent Gary S. Cacace: 11-mj-4270-tsh.”
[410] Johnson, “Man accused of plotting drone attacks on Pentagon, Capital.”
[411] Cacace, “Affidavit of Special Agent Gary S. Cacace: 11-mj-4270-tsh,” pp. 39-40.
[412] “Man, 26, charged in model airplane plot to bomb the Pentagon,” p. 2.

drones that can carry larger payloads and be easily adapted to autonomous flight, for fear that the government would crack down on their hobby.[413]

The existence of this do-it-yourself drone community indicates the extensive information on UAV construction and modification available online. The DIY Drones website offers instructions on how to build an "amateur UAV" from parts that retail for a few hundred dollars. Whether plane, helicopter, or multicopter, DIY Drones defines a UAV as "an aircraft capable of autonomous flight, without a pilot in control."[414]

To expand access to this capability, the DIY Drones community created ArduPilot, a small, dedicated computer chip that enables autonomous flight for UAVs. Billed as "the world's first universal autopilot,"[415] ArduPilot is based on the Arduino open source electronics platform, a single-board microcontroller that was first released in 2005 and retails for under $25.[416] As an open source platform, the Arduino software can be downloaded for free, and runs on Windows, Mac OS X, and Linux.[417] DIY Drones directs members to the website of 3D Robotics, which sells the latest version of the Arduino chip pre-programmed with the autopilot software, ArduPilot Mega 2.5, for $179. It is outfitted with gyros for controlling balance, pressure sensors, and a GPS system to assist with navigation. The mission planner software is free, and allows common desktops or laptops to program predetermined flight paths and analyze mission logs afterward.[418]

This means that anyone with a modicum of technical savvy and the ability to perform a simple internet search can find their way to the DIY Drones website and learn how to construct a small UAV capable of autonomous flight. The parts and software are fairly inexpensive and available for purchase on a variety of websites, "recreational" flights by individuals are legal, and the DIY Drones social

[413] "Man, 26, charged in model airplane plot to bomb the Pentagon," p. 1.
[414] Anderson, "A newbie's guide to UAVs."
[415] Anderson, "A newbie's guide to UAVs."
[416] "ArduPilot."
[417] "Download the Arduino Software."
[418] Anderson, "A newbie's guide to UAVs."

network is open to all. While the website operators and active participants all appear to be well-intentioned techno-hobbyists and students, there is nothing that would prevent a terrorist from utilizing the information. Official DIY Drones policy bans any discussion of “military or weaponized applications” or “illegal or harmful use of UAVs;” and the community has “encouraged all relevant regulators, defense agencies and law enforcement agencies to become members” to help them “understand what's possible with amateur UAVs, so they can make better-informed policies and laws.”[419] However, it would be easy for someone to use DIY Drones to assist with UAV construction and operation without informing the community of illegal or harmful intentions. Acknowledging the possibility that some participants may fail to follow the community's policies, the DIY Drones mission statement declares that “we follow the current interpretation of the FAA guidelines” on recreational UAV use, but, if anyone does not, “we're going to assume you've got the proper FAA clearance or we don't want to know about it.”[420]

A popular type of UAV on DIY Drones that is more commonly used by individuals than by militaries is the multicopter. These small, light aerial drones feature multiple small rotors (usually 3, 4, or 6) attached to a central base. Like helicopters, they can take off vertically, hover, and smoothly move along both vertical and horizontal axes. Multicopters maneuver by changing the pitch or rotation rate of one or more blade, and are cheaper and easier to construct than single or dual rotor helicopters. This makes them popular with drone hobbyists and photographers. In addition to a large section on the DIY Drones website, there are numerous online resources devoted to multicopters, such as MulticopterWorld.com, which focuses on their use in aerial photography. Many currently available

[419] Anderson, “The DIY Drones Mission (aka The Five Rules),” site policies.
[420] Anderson, “The DIY Drones Mission (aka The Five Rules),” rule #3.

models use a remote control, but multicopters can be adapted for autonomous flight using the ArduCopter autopilot from DIY Drones.[421]

Multicopters with four rotaries, known as quadcopters, are the most popular type, and range in price from small plastic toys under $100 to more advanced models for about $700. A well-reviewed high-end commercially available model is the Phantom, from DJI Innovations. This sleek quadcopter weighs less than one kilogram, with a length and width of 35cm and a height of 19cm. It can fly horizontally up to 22 miles per hour with a maximum accent/decent speed of approximately 13 mph, and remain in the air for 10-15 minutes depending on activity level. Though it is primarily controlled by a remote, the Phantom includes a GPS sensor and a basic autopilot capable of returning the drone to its base and automatically landing if it loses contact with the controller. Notably, the Phantom features a mount designed to carry a camera, and DJI advertises it as well suited for video photography, though not on the professional level of a SARAH.[422] Many cheaper, alternative quadcopters can carry cameras as well.

Given the size and payload capacity, the Phantom and similar multicopters would not be able to carry enough explosive material to pose much threat as a weapon. However, they could prove useful as information gathering platforms. A quadcopter with a camera could help a terrorist case a target, recording information about the structure or the presence of security. For example, New York City bans photography near the entrances of tunnels and on or close to bridges to prevent anyone from taking pictures they could use to search for structural flaws or any other information that could be exploited in an attack.[423] Many cities in the US, UK, and other developed countries have similar restrictions for infrastructure and government buildings. If someone takes a photo or records video in

[421] “ArduCopter User Group.”
[422] “Phantom.”
[423] “Camera Restrictions in New York.”

these restricted areas, the police may confiscate their equipment.[424] However, a multicopter recording video or still images of potential targets would be more difficult to notice or confiscate. Even if a police officer observes one in a restricted area, and it is not out of reach or able to fly away, the operator could remain unknown, because the officer would not have a face-to-face encounter with the photographer. This would be even more likely in the case of multicopters adapted for autonomous flight.

In addition to photographing potential terrorist targets inside nuclear states, multicopters equipped with cameras could help localized insurgents in less powerful countries gather information on locations they plan to attack. By photographing or recording video of police stations, government offices, and military installations, insurgents could determine the ideal time to strike with a raid or a car bomb, using the information they acquire to discover when security patterns offer windows of opportunity. This would provide them with an alternative to scouting targets in person, reducing the risk of getting noticed by police, guards, or security cameras.

Stopping insurgents from using relatively inexpensive multicopters to gather information would be more difficult than preventing similar efforts by people on the ground. Visible signs forbidding photography, along with the presence of police or soldiers authorized to confiscate cameras, represent a deterrent for network operatives. However, while these humans may fear getting caught and then possibly interrogated, the same could not be said of UAVs. In urban environments, it would be difficult for officers to follow aerial drones that can fly over buildings and move horizontally at over 20 miles per hour. Unless the UAVs could be tracked with radar or other sensors, security officers would need to shoot them down, which would be not be easy given their size and speed, and could be dangerous in populated areas. In the event security services were able to shoot down a small, makeshift surveillance drone, they still would have difficulty determining who was operating it.

[424] Geoghegan, Tom, “Innocent photographer or terrorist?”

However, to remotely control an average recreational UAV, like a quadcopter or the replica planes Rezwan Ferdaus planned to use in his attack, the operator must send a signal which can be traced using the sort of electronic sensors included on the latest Global Hawks and other advanced military surveillance drones. While advanced militaries usually control UAVs from considerable distance by relaying a signal via satellites, or program the aircraft to autonomously carry out a predetermined mission, less sophisticated drone operators typically send radio waves from a nearby remote control. Using the same technology that identifies the location of radar stations, states could determine the location of anyone flying a drone by remote control. This would enable a response, from a police car to a missile strike. However, such a technique is rendered moot by the various versions of ArduPilot and other commercially available autopilots that enable pre-programmed flights.

To stop terrorists or insurgents from using a UAV as a kamikaze weapon, or from gathering information that could be used to aid an attack, a state would first need to identify a drone as suspicious. This would be comparatively less difficult against a localized insurgency in an active theater of war, in which all authorized aircraft are operated by the counter-insurgents and allied forces. It becomes much more problematic in an environment with legal commercial drone flights, in which every UAV is potentially a smart bomb.

For organizations that utilize suicide bombers, smaller ground-based or flying robots present an alternative method of guiding explosives to a target that would not expend human operatives. A robot in a populated area would stand out more than a person, limiting its ability to surprise or to move to a location where an explosion would cause the greatest damage. However, this limitation will decrease as drones become increasingly normal sights, especially in cities. If food delivery drones and others undertaking daily tasks become widespread, then the presence of small unmanned aircraft will be fairly commonplace and won't raise any alarms. Furthermore, delivery UAVs, or any drone modified with an ArduPilot, would follow automated flight plans, like the K-MAX helicopters used for supply delivery in Afghanistan, which eliminates the possibility that police or military could locate the drone operator by tracing the radio signal used for remote-control aircraft. These, in turn, increase the probability that a terrorist will acquire a commercially available drone, or construct one from parts by following online directions, and transform it into a weapon.

Commercially Available Ground-based Robots

In addition to unmanned aerial systems, ground-based robots will likely proliferate for non-military and private use. Ground robots utilized by the military already come in versions designed for non-military tasks. For example, iRobot advertises the PackBot to HazMat technicians and first responders, who could use its ability to enter dangerous areas and manipulate objects with its arm to scout ahead of humans, remove hazardous material without risking human contact, and enter disaster zones that would be difficult for people, such as the rubble of a collapsed structure.[425] After an earthquake and tsunami in March 2011 damaged the Fukushima nuclear plant in Japan, two PackBots entered the plant equipped with sensors that measure radioactivity, oxygen levels, temperature, and hazardous chemicals. Once they had surveyed the affected area, operators used the PackBots to move 30 pounds of debris determined to be unsafe for human contact.[426]

Terrorists are more typically associated with spreading hazardous material than cleaning it up, but, as the PackBot demonstrates, ground-based robots could provide a method of guiding explosives, or a radiological, biological, or chemical weapon to a target. A PackBot may be too expensive and difficult to acquire to be practical for a terrorist group, but smaller, commercially available robots are cheap and widely available. Simple, do-it-yourself methods of upgrading a toy remote-control car to

[425] "Ground Robots – 510 PackBot."
[426] Koren, "3 Robots That Braved Fukushima."

drive autonomously are widely available on the internet.[427] For less than $200 worth of items available at RadioShack, anyone can convert a remote-control car into a basic robot capable of turning corners, sensing surrounding objects, and avoiding obstacles on its own.[428] With a GPS device, the cheapest of which cost less than $100, the car could travel to a pre-programmed location. While it lacks the sophistication of a PackBot and would be incapable of climbing up steps or over curbs, this simple robot could allow a terrorist group or self-starter to move a bomb to crowded area at less risk to themselves.

Similar to iRobot and the PackBot, Recon Robotics markets the Scout Throwbot to police forces and first responders in addition to the armed forces. A small, rolling robot that can transmit video and audio is useful to SWAT teams for the same reason it is useful to soldiers: as a stealthy method of scouting potentially dangerous areas ahead of humans. Recon specifically recommends the Scout to police forces for “barricaded subjects, hostage situations, and room-clearing operations.”[429] Additionally, given its small size, the Scout can move through areas too narrow or dangerous for human first responders to locate disaster victims in need of rescue.

Because it is cheaper and sold in greater number than the PackBot, there is a greater chance that non-state networks would be able to acquire a Scout on the black market. While terrorists, insurgents, and guerrillas do not often find themselves staging hostage rescues against strong actor forces, the information gathering capabilities of these small robots could grant them some additional lead time to react to the actions of strong actor soldiers. Alternatively, the Scout could observe locations ahead of an attack or during a raid, whether on a police station, government building, or weapons depot.

In addition to potentially acquiring ground-based robots intended for security services and first responders, weak actors could adapt some of the robots designed for civilian use that are likely to

[427] Bowman, “Learn how to turn an R/C car in to an autonomous robot.”
[428] “RC Car to Robot.”
[429] “Recon Scout Throwbot LE.”

proliferate in the coming years. Perhaps the most notable forthcoming ground-based robot that will be available for private use is the driverless automobile. In September 2012, California became the third state, after Nevada and Florida, to legalize driverless cars. There was no law written on autonomous automobiles, and therefore their presence on roads was not illegal, but proponents at Google lobbied California to officially legalize them to pave the way for their spread in the near future.[430]

These robots autonomously navigate roads populated by traditional cars with human drivers, using a variety of cameras and sensors to maintain a safe distance from surrounding vehicles. The cameras read road signs and an internal computer processes the information to ensure that the vehicle adheres to speed limits, stop lights, and other rules of the road. Using GPS and online map programs, the cars' navigation system can take passengers to their preselected destination without additional input. They can autonomously select a space and parallel park, and perform any other task undertaken by human drivers.[431]

In March 2004, DARPA held its first Grand Challenge competition for robotic cars. The research agency offered a $1 million prize to the first autonomous car to complete a 150-mile off-road course in the Mojave Desert. None of the entrants were able to finish, and DARPA raised the prize to $2 million for the next year's contest, designing a new course to ensure that the cars were navigating an unknown environment. In October 2005, five vehicles successfully completed the course, with the winner, a modified Volkswagen Touareg built by a team from Stanford University led by Sebastian Thrun, finishing in under seven hours.

For the 2007 challenge, the robotic automobiles had to complete an urban course, in which the cars had to recognize street signs and lights, obey various regulations, and merge into traffic. This time, the Tartan Racing team from Carnegie Mellon University, led by Chris Urmson, claimed the $2

[430] Miller, “With a Push from Google, California Legalizes Driverless Cars.”
[431] Lassa, “The Beginning of the End of Driving.”

million prize, with an automated version of a Chevy Tahoe. Tartan, which placed second in the 2005 Grand Challenge, defeated that contest's victor, the Stanford Racing team, who placed second in the Urban Challenge with a modified Volkswagen Passat, receiving $1 million.[432] Urmson and Thrun both now work for Google[x], Google's ambitious research lab focused on futuristic technologies, developing a commercial version of the driverless car.[433]

Driverless cars are likely to become widespread due to their ability to enhance safety. Using cameras, radar, and an emergency breaking system, autonomous cars can react more quickly than human drivers, and stop before colliding with other cars or pedestrians.[434] Unlike humans, the program controlling the driving will never exceed the speed limit, run a red light, get road rage, or aggressively cut off other cars. Insurance companies already offer discounts to drivers with cars equipped with an automated emergency brake system because of its strong record of reducing the risk of and damage from accidents. Some Google employees already use the company's autonomous cars to commute to work, and the company's co-founder, Sergey Brin, expects Google's driverless system to be ready for the mass market before 2020.[435] In August 2012, Chris Urmson announced that prototype self-driving cars had driven over 300,000 miles under a “wide range of traffic conditions, and there hasn't been a single accident under computer control.”[436]

While they could greatly improve road safety, autonomous automobiles also create the possibility of car or truck bombs without drivers inside. For organizations with limited budgets and considerable manpower, a driverless car bomb would be less cost effective than using a suicide bomber to drive a cheap used car. But individuals, or any organization for which operatives are more valuable than the cost of a driverless automobile, could fill an autonomous car with explosive material—such as

[432] Belfiore, “Carnegie Takes First in DARPA's Urban Challenge.”
[433] “Look, no hands.”
[434] Lassa, “The Beginning of the End of Driving.”
[435] “Look, no hands.”
[436] Urmson, “The self-driving car logs more miles on new wheels.”

the ammonium nitrate fertilizer, nitromethane, and diesel fuel mix that Timothy McVeigh used in the Oklahoma City bombing in 1995 to kill 168—and instruct it to drive to a target. McVeigh left an explosive-laden Ryder truck in a drop off zone, lit a timed fuse, and fled the scene. Using a driverless car with a cell phone-triggered bomb would allow a terrorist to direct a car bomb to a target without visiting the scene shortly before the explosion, and potentially being caught on camera or witnessed by a bystander. If a network can steal a driverless automobile, or buy one using a false identity, it would be more difficult for authorities to track down the perpetrator.

Much like commercial UAVs, as driverless cars become more common, they will seem less out of place, and therefore it will become more difficult to prevent one from being used in an attack. In every country with cars and roads there are many locations with legal parking spaces nearby from which a car bomb could cause considerable damage. Even if someone notices an autonomous car approaching or parked near a government building or another potential target, there is no driver for the police to instruct to move. As the technology becomes more widespread, governments will have to create laws that address the differences between human-operated and driverless cars, and the associated security concerns.

Hacking Unmanned Systems

In addition to controlling their own UAVs, an adversarial state or network could hack into opponents' drones. In December 2009, the United States admitted that Iraqi insurgents had intercepted the video feeds of Predator drones operating in the area. Insurgents used software such as SkyGrabber—an “offline satellite internet downloader” designed to gather free-to-air movies, music, and pictures from satellite internet providers[437]—to view the footage as it was transmitting from a

[437] “SkyGrabber.”

satellite back to the plane's base. The software can be purchased legally for as little as $26, or less than $100 when accompanied by a tuner card that receives satellite transmissions. American forces confirmed that they found “days and days and hours and hours” of video taken by Predators on captured insurgent laptops, and that the insurgents had distributed the footage to multiple organizations.[438]

Intercepting a Predator's video feed falls far short of electronically taking control of an MQ drone and firing Hellfire missiles. The insurgent hackers were not able to direct the UAVs flight path or the position of its cameras. However, accessing the video transmission provided insurgents with valuable information. Not only were they able to see everything captured by the cameras, they also learned which targets the United States was keeping under surveillance. With this knowledge, they would be able to move activity that they wanted to keep secret to a different location, act more carefully at places they knew were on camera, or deliberately feed the United States false information.

The Predator video feed was unencrypted, which left it vulnerable to simple software like SkyGrabber. Therefore, this particular problem can be addressed with a fairly simple fix. However, it reveals a vulnerability in remotely operated UAVs. To navigate and communicate with operators, they rely on signals that travel thousands of miles and bounce off satellites. Encryption can protect against most efforts at corruption or interception, but rendering these signals completely secure one hundred percent of the time is difficult, if not impossible.

In 2012, a research team from the Radionavigation Lab at the University of Texas used a technique called “spoofing” to misdirect an unmanned aircraft. Demonstrating the technique for the Department of Homeland Security on a university-owned drone, the researchers sent a false GPS signal, which caused the drone to fly to a different location than its operators ordered.[439] UAVs, both

[438] Gorman et. al., “Insurgents Hack U.S. Drones.”
[439] “Researchers use spoofing to 'hack' a drone.”

commercial and military, rely on the Global Positioning System network of satellites to determine their current location and the location of their targets. By sending a “spoofed” GPS signal, the University of Texas team convinced the drone that it was in a different location than it actually was. As a result, it altered its flight path to travel from the fake current location to the originally programmed destination. This caused the drone to veer off course and fly to a different destination, even while its navigating computer believed it was arriving at the pre-programmed target.

Iran may have used a similar spoofing technique to bring down an American RQ-170 Sentinel that was on a covert reconnaissance mission over its territory in late 2011. Iran claimed that it jammed the signal between the drone and its operators, which caused the plane to switch to autopilot. Then, using fake GPS signals, the Iranians were able to land the drone undamaged.[440] The United States has not confirmed this account, but did admit that American operators lost control of the drone while it was flying a mission over western Afghanistan near the Iranian border.[441] Shortly thereafter, the Iranians proudly displayed what appeared to be an undamaged RQ-170 Sentinel, which is more consistent with a controlled landing than a crash.

The University of Texas researchers redirected their drone using signals produced by commercially available equipment that cost approximately $1,000,[442] thereby demonstrating that non-state actors, as well as states, could acquire the means to launch electronic attacks on UAVs. Spoofing circumvented the more difficult—and yet to be demonstrated—technique of hacking into the signal issuing directions to the drone, which would enable the hackers to issue new orders, from new destinations to missile attacks. This highlights two potential risks, as military and commercial drone use expands. The possibility exists that resourceful hackers could create a new technique that completely takes over a drone and uses it to launch attacks. Or, even if signal encryption continues to

[440] Mackenzie and Duell, “We hacked U.S. drone.”
[441] “Drone shot down over Iran 'lost' over Afghanistan last week.”
[442] “Researchers use spoofing to 'hack' a drone.”

protect against an adversary gaining control of a military drone, computer-savvy individuals could use spoofing or a similar technique to trick a military or commercial UAV to veer off course. This would allow a network to disrupt drone missions, capture UAVs for sale or study, or, potentially, crash one into a target.

Conclusion: Robots and the Precedent of Computers

These examples of drone hacking highlight the back-and-forth nature characteristic of most technological developments. As with radar and stealth technology, computer viruses and anti-virus software, or improvised explosive devises and explosive ordinance disposal robots, one side gains an advantage from an innovation, leading the other side to seek ways to counter the advantage by exploiting loopholes or developing a corresponding innovation. Given strong actors' resource advantages, the robotics revolution has the potential to aid states in their efforts to counter the threats posed by non-state networks. However, as with widespread technological advancements like information technology, the spread of robots, and militaries' increasing reliance on unmanned systems, will create exploitable opportunities for networks in both predictable and unforeseen ways.

Information technology was, at first, monopolized by governments. Before personal computers became available commercially, computing and networking technology helped state militaries store, process, and share information. The United States Department of Defense created the world's first computer network that employed packet-switching[443] and TCP/IP communications protocol,[444] the data transmission techniques now utilized by the internet. Known as ARPANET—after the Advanced Research Projects Agency, the precursor to DARPA—the network launched in 1969, connecting two

[443] “Packet Switching.”

[444] “TCP/IP.”

University of California campuses with the University of Utah and the Stanford Research Institute. By 1983, it included more than 300 nodes and split off the military-specific MILNET.[445]

However, information technology spread and became increasingly available for civilian use. In the 1970s, private universities and corporate research facilities utilized computers and built their own internal networks utilizing TCP/IP. In 1977, Apple, RadioShack, and Commodore began selling computers to individuals for home use, and in 1981 IBM introduced the personal computer (PC) with floppy disks and the DOS operating system from Microsoft.[446] Throughout the 1980s and early 90s, ARPANET expanded rapidly, connecting various public and private networks into an integrated network of networks, or "internet." Meanwhile, in 1991, CERN, the European Organization for Nuclear Research, launched the World Wide Web, enabling various research institutions to create easy-to-read pages that could be accessed with browser software over the internet.[447] In 1995, commercial service providers took control of the network's major backbones, bringing the internet into private homes.[448] Accompanying this network expansion, the World Wide Web grew exponentially, from 10,000 pages in 1995 to over 30 million by 2000, and more than 1 trillion unique web addresses as of 2010.[449]

Now, in the second decade of the 21st century, almost everyone in economically developed countries, and many in the developing world, have access to computers, the internet, and cell phones. With smart phones, average citizens carry portable computers that are more powerful and have access to far more information than military computers from the 1970s or commercially available desktops from the 1980s. It is reasonable to assume that robotics technology will follow a similar pattern, with access progressively spreading from governments to large corporations to individuals.

[445] "ARPAnet."
[446] "Personal Computer."
[447] "World Wide Web."
[448] "ARPAnet."
[449] "World Wide Web."

Whereas information technology originally enhanced the capabilities of state militaries and research facilities, as increasingly powerful computers became commercially available and gained access to the internet, terrorist and insurgent groups found ways to utilize the technology to their advantage. By 2005, every organization on the U.S. State Department's list of identified terrorist groups had a presence on the web, with at least 4,300 separate sites dedicated to the groups or their supporters.[450] This dramatically enhances their ability to recruit, fund raise, spread propaganda, strategize, and share information, from expressions of solidarity to bomb making techniques. Computers and cell phones played a significant role in various post-Cold War asymmetric conflicts and terrorist attacks, including Hezbollah sharing intelligence about enemy troop movements in their 2006 war with Israel. Smart phones were essential to Lashkar e Taiba's attack on Mumbai in 2008, as the attackers used their phones' GPS to reach Mumbai by boat, studied online maps to plan their coordinated attacks, and actively monitored news websites during the attack to gather intelligence on each other's activities and the response of Indian security services.

Perhaps most notably, the internet magnifies the self-starter problem, enabling disaffected individuals from many countries to see themselves as part of a global movement. Al Qaeda sympathizers—from the British-born doctor of Iraqi decent who attacked the Glasgow airport, to the Nigerian son of a prominent banker who attempted to destroy an aircraft with explosives hidden in his underwear, to the Chechen-born brothers who set off a bomb at the Boston Marathon, one of whom was a US citizen—all saw themselves as activists fighting for the same cause; thinking globally but acting locally. It is difficult to imagine this loosely connected transnational network of individuals with shared sympathies existing without the internet. And, since most self-starters either learned how to build explosives from information acquired on the web, or made contact with terrorist groups online

[450] Weimann, "Terror on the Internet," p. 15.

who later supplied them with explosive material, the ubiquity of information technology enhanced their ability to cause damage.

The spread of robotics technology will probably repeat this pattern, at least along the basic outlines: first enhancing the military capabilities of the wealthiest governments, then assisting with military and non-military tasks of smaller and sub-national governments along with the commercial efforts of larger corporations, eventually achieving widespread use by individuals. Much as governments and corporations control the world's most powerful supercomputers, these large organizations will likely control the world's largest and most advanced robots. However, the spread of robotics technology will enable networks and individuals to acquire the cheaper, commercially available versions, and put them to use.

It is therefore likely that, within a few decades, robotics will occupy a similar position as information technology regarding asymmetric warfare. Aerial and ground-based unmanned systems will enhance the capabilities of strong actors, but their monopoly on the technology will continue to fade as weak actors make use of robots as well. Small unmanned aerial vehicles designed for military use have already proven useful as information gathering platforms for state sponsored networks, and adapted commercially available versions are likely to follow suit. Additionally, as privately controlled robots, from driverless cars to UAV photographers and even food delivery drones, become increasingly commonplace, the chances increase that one will be utilized in a terrorist attack.

While it is difficult to predict who will attempt this sort of attack, it is easier to identify risks and create countermeasures in advance. In anticipation, states should develop a method of taking control of any robot within a given area in an emergency. Much as the FAA can order commercial aircraft to remain on the ground or human pilots to change course, governments should be able to order unmanned aircraft to land or alter their flight plan as needed. Additionally, as commercial drones proliferate, infrastructure, government buildings, and other potential targets could be outfitted with measures that force any UAV that gets too close to turn around, perhaps by triggering the return-to-base feature common to drones that use ArduPilot. These defenses would serve a similar function as physical barriers designed to defend against car bombs by preventing vehicles from getting too close to potential targets. By anticipating the ways terrorists could utilize commercial robotics technology and developing countermeasures in advance, states can mitigate the risk of an attack. However, it is impossible to predict every way that networks will adapt to the robotics revolution.

Chapter 6: Robots and Strong Actor Strategy against Localized Insurgencies: Pursuing Information Dominance

In *Wired for War,* Brookings scholar P.W. Singer argues that the United States lacks a robotic warfare doctrine, an overarching strategy designed to achieve military goals utilizing the new capabilities robots provide.[451] Analogously, tanks and airplanes appeared in World War I, but only in support of existing attrition and trench-warfare strategies, scouting ahead or supporting infantry and artillery. It wasn't until World War II that Germany built a strategy around these new technologies, utilizing their strength and speed to target the political and industrial support base of national war efforts. Even though France had more tanks than Germany in WWII—3,245 to 2,574—the French doctrine dispersed a few to each infantry unit, while the German blitzkrieg coordinated tanks with air and artillery "to create a concentrated force that could punch through enemy lines and spread shock and chaos."[452] German forces went around, over, or through French defenses, rapidly taking Paris and conquering all of France in less than two months. Citing soldiers, generals, and roboticists, Singer warns that "developing the right doctrine for using unmanned systems is thus essential to the future" of American security, so that the US does not develop "the Maginot Line of the 21st century."[453]

Currently, the US military utilizes robots to enhance pre-robot strategies. Existing units get small unmanned aerial vehicles or links to larger robotic airplanes for scouting; ground-based bots to carry equipment or scout ahead with cameras; and specialized robots designed to meet current needs, such as searching for and disposing of IEDs ahead of advancing convoys. Meanwhile, aerial drones

[451] Singer, *Wired for War*, pp. 208-212.
[452] Singer, p. 209.
[453] Singer, p. 210.

have taken over many of the missions previously conducted by piloted aircraft, from long-range reconnaissance to airstrikes. The military thus uses robots to enhance previously developed capabilities and reduce the risk to personnel, but "doesn't yet have an overall doctrine on how to use them or how they fit together."[454]

In part, that is because they are thinking about how humans would use robots to fight, not how computers would fight a war. The main advantages granted by robotics are reduced risk to human personnel, and increased information gathering and processing. Unmanned systems do not significantly improve destructive capability. Any weapon attached to a land, sea, or air-based robot could be carried by a human soldier or manned vehicle. Bullets, bombs, and missiles, along with potential futuristic weapons like lasers, could be used by humans and robots alike to kill and destroy when necessary. There are no countermeasures that can sufficiently protect against these destructive capabilities—many targets are unarmored, and larger or more directed explosives, such as bunker-busters or shaped charges, can destroy those with physical protection—which means that destructive capacity would not distinguish computerized warfare from the pre-robot doctrine of the early 21st century. Since the invention of precision-guided munitions (AKA "smart bombs"), advanced militaries have been able to quickly destroy a known target at will. The problem is knowing what to target.

Therefore, the gathering and processing of information should be the basis of a comprehensive doctrine of robotic warfare. Like human commanders, a computer fighting a war would want as much information as possible, avoiding action without sufficient information when it can, and filling in information gaps with assumptions and educated guesses when it must. However, unlike humans, a computer can simultaneously utilize as many streams of information as software and processing power

[454] Singer, p. 210.

allow. Taking this idea to its theoretical limit, a network of robots integrated with a powerful computer system could fight with perfect information.

The ideal of fighting with complete information is not new—arguably it has been a goal of militaries since the first organized fighting forces sent out scouts—but technology is finally approaching the point at which something close becomes plausible. Of course, perfect information is impossible. To take an extreme example, mind reading would greatly enhance military tactics by revealing an opponents' intentions, but acquiring this information is far beyond the scope of any existing or forthcoming technology. However, with Wide Area Airborne Surveillance Systems high in the air and hundreds or even thousands of information-gathering robots on or near the ground, each carrying a variety cameras and sensors, all linked to a powerful information processing computer, a fully roboticized military could achieve real-time awareness of people and objects within a given area. This would allow more informed decision-making, on a larger scale, than any military in the history of the world.

Network-Centric Warfare

The United States has made information sharing and widespread battlefield awareness a priority since the 1990s under the rubric of "Network-Centric Warfare" (NCW), which was coined by Arthur Cebrowski and John Garstka, and developed by the Office of Force Transformation under Cebrowski's direction.[455] Drawing upon internet-era theories of business, economics, and sociology, NCW emphasizes using modern information technology to share information and coordinate actions among various units and platforms in real time, so that the whole of a military force is greater than the sum of

[455] Cebrowski, Arthur K., and John J. Garstka, "Network-Centric Warfare: Its Origin and Future."

its parts. Ideally, transforming the military to a seamlessly networked force would eliminate the fog of war (Clausewitz' term for the uncertainties inherent in combat) by removing the friction between separate military units and their commanders. According to Cebrowski, NCW represents no less than “transforming from the Industrial Age to the Information Age,” in which “power is increasingly derived from information sharing, information access, and speed, all of which are facilitated by networked forces.”[456] By linking and coordinating the military's various parts, Cebrowski and Garstka theorized that a smaller and more mobile fighting force could command the destructive power of larger armies, but with greater speed and precision, granting the United States armed forces a qualitative military advantage.

The core strategic goal of NCW is “information dominance” or “information superiority.” According to the US military's “Joint Doctrine for Information Operations” (also known as Joint Pub 3-13), this refers to “the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same.”[457] Essentially, the more that soldiers, sailors, marines, airmen, and their commanders know about a given battlespace, the more efficiently they can pursue their objectives. Increasing knowledge reduces the risk of mistakes, such as friendly-fire, by informing engaged units of their allies' locations, and allows forces to act with greater speed and precision by reducing ambiguity. Perfect information is a limit, a goal that can be approached but never reached, and information dominance works to serve and enhance traditional war-fighting concepts, rather than replace them. As NCW advocates David Alberts, John Garstka, and Frederick Stein point out, “even in the case where information is far less than perfect, it could

[456] “The Implementation of Network-Centric Warfare,” p. 1-2.
[457] “Joint Doctrine for Information Operations.”

reasonably be argued that being able to have a shared understanding of what is known and what is not known would be preferable to a situation in which units operated in isolated ignorance."[458]

Network-Centric Warfare received its first major tests in Iraq, garnering numerous critics. For example, P.W. Singer declares networking-based strategies a "failure" and dismisses the "networks of email and Internet fiber optics that now bind military units together" as merely quicker versions of "radios, phones, or faxes."[459] The "network crowd," he argues, "was wrong that the fog of war would be lifted,"[460] citing instances in which American forces lost track of Iraqi tanks in the early conventional phase of the invasion, and then had difficulty identifying and tracking insurgents after the defeat of Saddam Hussein and the Iraqi army. Defense analyst Loren Thompson goes further, arguing that NCW was conceived before 9/11 and designed for conventional warfare, and thus should not have surprised anyone when it performed poorly against asymmetric adversaries like the Iraqi insurgency.[461]

Part of the problem was the Bush administration's, especially Secretary of Defense Donald Rumsfeld's, overzealous conviction that NCW was ready in time for the invasion of Iraq. In Operation Iraqi Freedom, the equipment for network-centric strategies ran into problems both technical and logistical. "Rather than a seamless flow of information, soldiers wrestled with everything from Web browsers constantly crashing due to desert sand to heat fouling up equipment designed for use in offices, not battlefields."[462] Additionally, the newly networked fighting forces faced unexpected bottlenecks, from a shortage of batteries to power mobile devices, to an overwhelmed bandwidth spectrum for wireless communications. These problems stem from the fact that NCW had not been

[458] Alberts et al, p. 8.
[459] Singer, *Wired for War*, p. 193-194.
[460] Singer, p. 193.
[461] Thompson, "The Twilight of Network-Centric Warfare."
[462] Singer, p. 190.

tested in actual fighting conditions; and the war in Iraq revealed ways in which the military fell short of Cebrowski's vision. Though this is a legitimate criticism of the confidence with which some officials in and outside of the Defense Department championed military transformation in the early 2000s, it presents technical problems to be overcome rather than a reason to discredit the larger theory.

More problematic were difficulties in identifying and tracking adversaries, especially in the post-invasion insurgency phase of the Iraq War. In *Armed Forces Journal*, Milan Vego argued that NCW “appears not to provide much of an advantage in fighting an insurgency in the post-hostilities phase of a campaign, as the current situations in Afghanistan and Iraq illustrate. In fact, the ongoing insurgency in Iraq is a powerful proof, if any is needed, of how little practical value networking one’s forces has in obtaining accurate, timely and relevant information on the enemy.”[463] Casualty data support this, as the United States defeated the Iraqi army and deposed Saddam Hussein in two months, losing 187 soldiers, but suffered 4,299 military deaths while fighting the subsequent insurgency for 8½ years.

Red Force Tracking

The Iraq War clearly demonstrates that network-centric operations did not overcome the advantages insurgents enjoy from the asymmetry of information, but that is because the information fed into the network was gathered primarily by humans. As Loren Thompson put it, “all those networks the Pentagon was planning are just conduits” and “what matters more for victory is the accuracy and completeness of the information moving through the networks.”[464] Information gathered by human soldiers, and by humans watching video feeds from cameras mounted on soldiers' helmets, satellites, or

[463] Vego, “The NCW Illusion.”
[464] Thompson, “The Twilight of Network-Centric Warfare.”

spy planes, is inherently incomplete and of limited accuracy. When directing combat, senior officers can follow the real-time location of friendly forces on interactive maps (not unlike those of Google Earth) using “blue force trackers,” which employ GPS to transmit the location of personnel and equipment. Blue force tracking allows greater coordination of friendly “blue” forces, but the utility is limited by the absence of data on the location of enemy “red” forces. The lack of “red force tracking” creates problems even when the identity of the enemy is known; it is especially problematic in counter-insurgent warfare when there is difficulty distinguishing enemy fighters from civilians. As long as the identity and location of enemy forces is unknown, perfect networking does not get the US military remotely close to the ideal of information dominance.

Therefore, a system capable of red force tracking should be a primary goal of the robotics revolution. Imagine a swarm of flying sensors: hundreds or thousands of micro UAVs equipped with sensors, cameras and microphones, feeding information into a supercomputer. These intelligent Systematic Warfighter-Assisting Reconnaissance Measures, or “Smart SWARM,” could fly in front of advancing forces and provide detailed, real-time information about what lies ahead. Taking advantage of computers' ability to simultaneously process exponentially more streams of information than humans, portions of the swarm could fly off in all directions, gathering information from all sides. The computer could then account for any people and objects within range and create a fluid three-dimensional display that changes as circumstances evolve. It could present the full 3D image or a two-dimensional bird's-eye view on screens in a command center, and display a simplified version to soldiers in the field in a manner that would not obstruct their vision, such as a hand-held device or a headset display similar to “wearable computers” like Google Glass. Depending on the needs of various users, the system could utilize algorithms to prioritize the likelihood of threats, alerting soldiers or commanders when something requires their attention. For example, with information-gathering robots surrounding soldiers at periodic intervals, this system could alert units to approaching enemies, track fleeing suspects, and discover awaiting ambushes.

Combining a Smart SWARM with a Wide Area Airborne Surveillance System like the ARGUS-IS would provide considerable advantages in the kinetic aspects of counter-insurgent warfare. While the ARGUS can cover a wide area, and a computer system could process its feed to track vehicles or search for threatening behavior such as someone burying an object beside a road, it is only capable of looking down, and therefore cannot see through cover. However, in urban settings, the SWARM could peer around corners, fly over rooftops, search under awnings and look in windows, providing information on the location of snipers or hidden enemies.

Additionally, the Smart SWARM could enter buildings before soldiers, informing them of the locations of any people or weaponry. With many small, mobile robots, the SWARM could provide a real-time map of the inside of any building, and individual micro UAVs could follow people as they move around inside. Using object recognition, the system could determine which individuals are carrying weapons, and locate any guns or other relevant objects stored on the premises. With infrared sensors, it could find anyone waiting to ambush soldiers or hiding to escape capture. Add Fido sniffers and the swarm could identify booby traps and discover stored explosives. This would provide commanders with detailed information about the contents of any house or compound before sending in soldiers, greatly reducing the ability of enemies to surprise or flee and increasing the thoroughness of the search.

Beyond kinetic operations, the SWARM would be hugely beneficial to intelligence gathering. A system of small, flying robotic sensors, cameras and microphones could eavesdrop on various targets, observing meetings or hiding in suspected safe-houses. They could sneak through pipes or between walls, resembling small insects to reduce suspicion. This would provide a method of bugging targets without the risk that a human operative could be caught planting or recovering the recording device. Furthermore, the bug wouldn't be fixed to a single location, and a human operator or computer program could direct it to move as the target moves, or if the audio or video feeds become obstructed. The system could thus monitor terrorist or insurgent leaders targeted for drone strikes, or snatch-and-grab missions, confirming the identity of the target and informing decision-makers of anyone in proximity, thereby reducing mistakes and limiting collateral damage.

It would be naïve to assume that the Smart SWARM can eliminate the fog of war, but it can reduce it considerably and provide relative information superiority. With robots, rather than humans, gathering information, and computers, rather than humans, processing the numerous streams, the United States military could achieve a considerably higher level of battlefield awareness than it achieved in the Iraq War, in both the first phase against the Iraqi military and the second phase against the insurgency. Wide Area Airborne Surveillance Systems, Ravens or other small UAVs, ground-based robots like Throwbot Scouts and PackBots, and a Smart SWARM of micro UAVs carrying various sensors could together gather enough information to provide a detailed portrait of a given area.

Nevertheless, pre-robot intelligence techniques would remain essential to strong actor strategies against insurgent and terrorist organizations. A widespread network of information-gathering robots could monitor the location of people and objects, and a sufficiently intelligent computer program could identify actions such as carrying weapons or planting IEDs. However, robots could not determine intentions or allegiances. Therefore, human intelligence techniques, from infiltrating hostile organizations to establishing relationships with locals, would remain essential to counterinsurgent strategy. Information gathered in traditional ways would direct and be informed by information gathered and processed by robotic systems. In this way, the Smart SWARM would both enhance and depend upon existing informational strategies, much as NCW seeks to compliment rather than replace classical war-fighting strategies.

Building the Smart SWARM

Hundreds of miniature flying robots working in conjunction to create a 3D map of all people and objects in a given area that updates in real-time may sound like science fiction, but most of the elements already exist. Micro UAVs designed to gather information are already used in active military theaters, such as the Black Hornet miniature helicopters British soldiers operate in Afghanistan. Prototypes of UAVs that look like and mimic the abilities of various insects have been built, and more are expected soon. Groups of small robots independently working together to accomplish a single task already exist, though they have not been mass produced or put to widespread use. Finally, though it appears that no software capable of constructing a constantly updating 3D map from all of these inputs currently exists, various existing programs suggest that such a thing is possible.

A team from Georgia Tech's Robotics and Intelligent Machines Department has developed a miniature UAV that mimics the flying capabilities of a dragonfly. Developed with a $1 million grant from the US Air Force's Office of Scientific Research, the Dragonfly drone can fly and hover in a manner similar to its namesake.[465] It employs a combination of quadcopter, helicopter, and fixed-wing technology to achieve considerable maneuverability, and, with a length of six inches and a weight of 25

[465] Danigelis, “Tiny Dragonfly UAV Flies and Hovers to Spy.”

grams, is small enough to fit on a human palm.[466] TechJet, a company spun off from the Robotics and Intelligent Machines Department to market the Dragonfly, envisions various versions tailored to different uses, including gaming, photography, home security, and military surveillance.[467] With its small size, ability to both fly and hover, and flexibility regarding components, the Dragonfly, or an alternative UAV with similar capabilities, could form the basis of the Smart SWARM.

TechJet expects the Dragonfly to retail between $250 and $1,500, depending on the level of computing and flying capabilities included.[468] That is more expensive than the $700 quadcopters advertised on DIY Drones, but far less costly than the Black Hornet, which the UK bought for approximately $200,000 per unit. Unlike the Dragonfly, each Black Hornet includes a camera that can capture video or still images one kilometer away, and a hand-held display that can show these images to an operator. Although the Dragonfly does not come with these accessories, its drastically lower price demonstrates that forthcoming UAVs based on insects could provide a cost-effective basis for building the Smart SWARM. Furthermore, since the distance between each drone in the SWARM would be considerably less than one kilometer, they would not require the Black Hornet's powerful camera.

An even smaller alternative is a tiny flying drone that vaguely resembles a crane fly developed by the Wyss Institute for Biologically Inspired Engineering at Harvard. This micro UAV is only 3 centimeters from wingtip to wingtip and weighs only 80 milligrams. Whereas the Dragonfly is a little smaller than a palm, the crane fly drone is barely larger than a penny. Unlike miniature helicopters and other micro UAVs that use rotaries, it is an ornithopter, with flapping wings modeled after the *Eristalis*

[466] Green, “Dragonfly Robotic Insect UAV is Freaking Cool.”
[467] Danigelis, “Tiny Dragonfly UAV Flies and Hovers to Spy.”
[468] Green, “Dragonfly Robotic Insect UAV is Freaking Cool.”

genus of flies.[469] This miniature drone can hover and execute simple flight maneuvers, demonstrating the feasibility of flying robots tiny enough to escape casual notice. Though the Dragonfly or crane fly drones would not be confused with actual insects by anyone paying attention, as UAVs get smaller and closer in appearance to real insects, they will become increasingly capable of stealthy spy missions.

To fulfill the Smart SWARM's goal of information superiority, many of these small robots would need to independently coordinate actions. This is simpler than it might seem at first. To act as a swarm, robots do not require constant instructions from a centralized decision-maker. In a manner similar to the way that bees or ants work together, each robot follows some simple rules in relation to the other units in the swarm, which, when taken together, produce collective action.[470] For example, ants carrying food back to the main colony just follow the ant in front of them along a chemical trail that was left by the ants that originally discovered the food source and reinforced by every ant that walks along the path. Similarly, each robot in a swarm of information-gathering micro UAVs could be programed with the simple rule never to get too close or too far from another member of the SWARM. This would keep them close enough to cover a selected area with no blind spots, but spaced out enough to avoid crashes or unnecessary redundancy.

There has been considerable research into robot swarms, much of it published in robotics journals, some of which are specifically devoted to swarming technology. In particular, the Future and Emerging Technologies program of the European Commission sponsored a venture called “Swarm-bots,” and a successor called “Swarmanoid,” to advance coordinated robot behavior. The Swarm-bots project focused on homogenous groups of robots that autonomously assembled themselves into a single

[469] “Robodiptera.”

[470] Sahin and Franks, “Measurement of Space: From Ants to Robots.”

structure.[471] Swarmanoid built upon this by creating a heterogeneous swarm consisting of approximately 60 robots of three different types that moved as a group through human environments while working together to negotiate obstacles.[472] The Swarmanoid system won an award from the Conference on Artificial Intelligence in 2011, and its success indicates the feasibility of an autonomous swarm that features different types of information-gathering micro UAVs working together with ground-based and aerial ISR robots.

Drawing lessons from the behavior of insect societies, programmers have developed groups of robots that can make decisions from a collective process of individual actions. For example, researchers working on the Swarm-bots project noted how group decisions emerge from the interactions of individual ants seeking the most efficient path to a food source. No single ant knows the best way to reach the food, but, through trial-and-error and the ability of individuals to chemically communicate success or failure, the group of ants finds and then adheres to an effective route. With this in mind, researchers programmed a group of ground-based robots with simple rules that enabled the group to avoid falling into holes. As each robot moved in a general direction across terrain featuring holes from which they could not escape, some inevitably would fall in. However, any that fell into a hole would send a simple signal to the other robots to keep their distance, which resulted in most of the group avoiding the holes and reaching their destination. The group's decision to steer clear of holes emerged from simplistic actions of, and signals from, individual members.[473] In another example of emergent group decision-making, a heterogeneous swarm improved group efficiency by

[471] "Swarm-bots."
[472] "Swarmanoid."
[473] Trianni and Dorigo, "Emergent Collective Decisions in a Swarm of Robots."

increasing the role of machines that proved the best at performing various tasks, autonomously creating a division of labor.[474]

The ability to learn from circumstances and reassign roles based on performance would make a robotic SWARM capable of reacting to combat conditions. Some early ideas for swarms depended on aerial drones that would fly above the other robots to provide information about the surrounding environment and issue directions. However, in the event of accident or malfunction to these central robots, the functionality of the entire swarm would suffer. More recent robot swarms based on emergent group decision-making are more robust, which makes them better suited for military operations. The entire swarm is valuable, but each individual unit is incidental. If a few became damaged, whether through accident or hostile action, the group could adjust and continue with its mission.

Moving a swarm through an outdoor area is relatively easy compared to navigating indoor environments. However, a paper presented at the 2012 International Conference on Robotics and Automation detailed an “entirely decentralized approach” of moving around inside that “relies solely on local sensing without requiring absolute positioning, environment maps, powerful computation or long range communication.”[475] The authors reported successfully testing this method using quadcopters. In the experiment, the robots in the swarm did not possess any prior knowledge of the halls they moved through, but were able to navigate the indoor space based on basic information each robot gathered about its environment and simple rules governing relations between the units of the swarm. Using an advanced version of this application, a Smart SWARM would be able to enter a

[474] Labella et. al., “Division of Labor in a Group of Robots Inspired by Ants' Foraging Behavior.”
[475] Stirling et. al., “Indoor Navigation with a Swarm of Flying Robots.”

building and move throughout it, searching for people and objects while providing a layout to human operators.

With robotic swarms capable of independently navigating both outdoor and indoor environments, the next step towards a militarily useful Smart SWARM is software that could synthesize the various streams of information to create a user-friendly display. Many of the components for this exist as well. Three dimensional mapping software is commonly used by architects, land developers, city planners, miners, and other professions that make use of geographic and spatial data. The maps created by this software are static models of topographical features, city blocks, or buildings, rather than the constantly updating displays necessary for the Smart SWARM to monitor the locations of moving objects.[476] However, existing software can build detailed 3D maps that users can navigate virtually, and a more advanced version could use this template while adding the ability to account for real-time tracking of moving objects.

Commercially available 3D mapping software is primarily a tool for human users to build virtual models, but computers have demonstrated the ability to autonomously create 3D displays of indoor spaces using limited information. In a May 2013 paper published by the National Academy of Sciences, a team presented an algorithm that "reconstructs the full 3D geometry" of a room "from a single sound emission." By using acoustic echoes in a manner similar to the way that bats "see," the software records sounds bouncing back off of walls and uses the information to build a three dimensional map of a room.[477] With all the noise present in a combat environment, this technique might not be the best fit for war-fighting. However, the software shows how a computer system can quickly create a model of a room from information acquired by automated processes, and the Smart

[476] See, for example, "AutoCAD Map 3D."

[477] Dokmanic et. al., "Acoustic echoes reveal room shape."

SWARM would be able to use information from various sensors and cameras, instead of just a few microphones monitoring the echoes from a single sound.

To create software that builds three dimensional images based on the information collected by each robot in the Smart SWARM, programmers should consider the example set by a method of studying hurricanes. In 2013, a team from the University of Florida announced that it is working on a project to predict the strength and path of powerful storms using a swarm of robots. Combining micro UAVs about 6 inches long that fly into the storm with small submersible robots that swim in the ocean below, the hurricane-hunting swarm uses sensors carried by each robot to collect data on air pressure, temperature, humidity, wind speed, and wind direction. As with other robotic swarms, each unit is relatively cheap: only $250 per miniature plane. If any are lost—which is to be expected when flying in extreme weather, even though the UAVs are designed to fly with, rather than fight, the powerful winds—the group adjusts autonomously. The swarm sends the data it collects in real-time to computers out of the storm's range, which then create sophisticated weather models that predict the hurricane's trajectory and intensity.[478]

This system has not been completed yet, but the existing method of studying hurricanes demonstrates how a computer can build a model of complex phenomena using data collected by many small units. To gather data on powerful storms, a large manned airplane flies into the eye and ejects hundreds of lightweight cylinders known as “dropsondes.” The dropsondes fall through the storm attached to parachutes, going wherever the winds blow them, and gather data that they send back to

[478] “Tiny airplanes and subs from University of Florida laboratory could be next hurricane hunters.”

base via radio signals.[479] This offers a potential model for how the Smart SWARM's central computer could utilize real-time data coming in from multiple sources to create a detailed model of a given area.

These developments in computing and robotic systems demonstrate that the Smart SWARM is technologically plausible. Many types of small UAVs that gather information, swarms of robots that coordinate the actions of different types of autonomous machines without central direction, computer software that creates three dimensional maps of indoor and outdoor spaces, and algorithms that create models from information gathered from numerous sources all exist. These components could therefore be combined and further developed to produce a robotic swarm and dedicated computer system designed to provide soldiers and commanders with a detailed picture of a selected area. Combined with object recognition and facial identification software, such a system could help the United States military achieve information dominance in both symmetric and asymmetric conflicts.

Countering Weak Actor Robots

A swarm of flying sensors, cameras and microphones monitored by supercomputers would greatly enhance information gathering and processing capabilities, but the core strategy of network-centric operations focuses on "information superiority," which also includes denying information to enemies. In asymmetric warfare, this entails minimizing or eliminating weak actors' advantage in the asymmetry of information, or even creating informational asymmetries that favor the stronger actor. To realize these goals, strong actors not only need to maximize their information acquisition and processing capabilities, but also minimize the ability of weak actors to do the same.

As discussed in the previous chapter, information-gathering robots, especially small UAVs, will likely prove increasingly useful to non-state networks in their fights against states. Whether acquiring

[479] Bittel, "Studying Hurricanes with Swarms of Smart Drones."

unmanned technology designed for military use from state sponsors or on the black market, or adapting commercially available robots, insurgents and guerrillas could use small UAVs with cameras and other information-gathering unmanned systems to anticipate enemy movements, plan ambushes, and avoid raids. Therefore, a strong actor strategy based on information superiority would need to counter the information-gathering abilities of small drones and other robots that relatively weak actors may acquire.

One possible technique is signal jamming. By overwhelming radio transmissions with static, or “noise,” jammers could prevent communication between drones and their operators. This technique would be especially useful against remote control aircraft and less so against drones that fly autonomously, although it would prevent both types of unmanned aircraft from transmitting images back to ground stations. By preventing operators from receiving video feeds in real-time, jammers would eliminate the ability of robots to provide networks with actionable battlefield intelligence.

Both the American and Israeli militaries have utilized jamming to prevent remote detonation of improvised explosive devices, which provides a precedent for using similar technology against robots. The United States credits the tens of thousands of jammers it deployed to Iraq and Afghanistan with saving numerous lives.[480] However, to ensure successful interference with cell phones and other devices used to remotely trigger IEDs, jammers saturate an area with electromagnetic energy, broadcasting over many frequencies at once.[481] IED jammers are typically mounted on vehicles, which protects the vehicles from remotely detonated explosives in their vicinity, but to disrupt the communications of an enemy UAV high in the air, a jammer would need to be considerably more

[480] Shachtman, “The Secret History of Iraq's Invisible War.”
[481] “IED Jammer.”

powerful than one protecting a vehicle from IEDs. Therefore, any jammer powerful enough to disrupt enemy robotics would also interfere with friendly unmanned systems in the area.

A similar problem applies to an electromagnetic pulse (EMP). This burst of electromagnetic energy damages or disrupts the function of electronic devices, and would therefore be a useful weapon against robots. An EMP is produced by a nuclear explosion, but a non-nuclear EMP can be created by an explosively pumped flux compression generator, which is a device designed for this purpose, as well as some microwave generators.[482] However, while an EMP would disable enemy robots, it would have the same effect on friendly robots or electronic equipment within the blast range, diminishing its utility.

Since both jammers and EMPs have considerable drawbacks, the best method of countering robots may be simply to spot, track, and shoot them. However, as Israel found out when the first Hezbollah UAVs entered Israeli airspace, the sort of unmanned aircraft likely to be used by networks are often too small, or fly too low to the ground to be noticed by traditional aircraft tracking methods. Therefore, improved radar, both on the ground and in the air to avoid interference from mountains and other obstacles, could spot smaller objects flying lower than typical planes. Sensors that track electronic signals, such as those featured on Global Hawks and other large ISR drones, could intercept communications between a small UAV and its ground station. Additionally, strong actors should consider developing drones dedicated to autonomously identifying and tracking unmanned aircraft. Once the location of an enemy drone is known, it could be shot down by anti-aircraft weaponry, including C-RAM systems, surface-to-air, and air-to-air missiles. These missiles are frequently more expensive than the UAV they would be shooting down, but this should not be considered a problem

[482] Kopp, “The Electromagnetic Bomb – a Weapon of Electrical Mass Destruction.”

because it would be taking advantage of material superiority, the one clear advantage strong actors have in asymmetric conflict.

The Smart SWARM, Robots, and Military Strategy (Keeping Humans in the Loop)

At this point, we should probably talk about Skynet. In the *Terminator* movies, the United States military creates Skynet, a powerful artificial intelligence system, to reduce reaction time and eliminate human error, and gives it control of all computerized military hardware, including stealth aircraft and nuclear weapons. The system becomes self-aware and turns on its human masters, using America's arsenal to kill billions and take over the planet. This is one of many science fiction stories in which computers and robots end up threatening human survival—*2001: A Space Odyssey* and *The Matrix* are among the most famous—contributing to a widespread wariness of military robotics, especially autonomous systems. When thinking about how a computer would fight a war and what sort of technological developments would help achieve information superiority, it is worth considering the ethical questions relating to autonomous robots.

While pop-culture driven fears of current or forthcoming unmanned systems choosing to rebel against humanity are unfounded, military strategists and roboticists have raised reasonable concerns about the autonomy of killer machines. Since the earliest targeting computers on bombers, machines have assisted humans with life-or-death decisions, and automated systems capable of killing on their own have been in use for at least three decades. In the 1980s, the United States Navy began using the Phalanx close-in weapons system, a precursor of 21st century land-based C-RAMs, to protect ships. The Phalanx, Patriot missile batteries, and other anti-air and missile defense systems at sea or on land are capable of autonomously detecting enemy aircraft or incoming projectiles and firing without human input. Given the speed of missiles, the quickness of automated reactions has saved lives and equipment. However, on rare occasions, the systems have mistakenly identified targets and destroyed civilian or friendly aircraft. This precedent creates concern that human beings remain "in the loop" and retain control of most decisions to fire weaponry as unmanned systems become increasingly capable of autonomous decision-making in the 21st century.[483]

There are, however, numerous advantages to robots that can make decisions on their own, making increased autonomy inevitable. Besides the combat advantages associated with rapid decision-making, autonomous machines act as a force multiplier. It is difficult for humans to actively operate more than one robot at a time, but autonomy enables multiple robots in the field per human operator. Additionally, if robots can carry out their primary functions without directions from a remote control, they cannot be thwarted by signal jamming or unintentional interference. While many people remain hesitant to grant robots the ability to select targets or choose when to fire without direct human input, if unmanned systems can demonstrate a near-perfect rate of success, most will come to accept it, much as virtually no one fears the use of autopilot in passenger jets or denounces automated anti-air defenses.

Even as individual robotic systems become more autonomous, they will not be taking over military strategy in the foreseeable future. It is dangerous to say technology will never be able to accomplish something—forever is an awfully long time—but strategy is so complex, and must take into account so many variables, as to be far beyond the capabilities of early 21st century computers. At the highest level, military strategy is linked to political objectives, which are definitionally dependent upon human preferences. However, even with human-determined objectives as inputs, the world's most powerful computers still could not handle strategy.

[483] Singer, *Wired for War*, chapter 6, especially pp. 124 - 125.

Computers originally mastered tic-tac-toe and checkers, because there are a limited number of possible moves and situations. There are considerably more in checkers, but in both games there exists a perfect strategy that will either win or draw against every possible opponent.[484] Similarly, chess has a finite number of situations, albeit exponentially more than checkers. The upper bound of the number of possible arrangements of chess pieces has been mathematically proven to be, at most, 10^46.25, and is probably lower by a few orders of magnitude.[485] When playing chess, computers play out millions of potential games from a given point and then select the move that leads to the highest probability of victory. Though no computer program has found an unbeatable strategy for chess like those for tic-tac-toe and checkers, given the finite number of possible positions a sufficiently powerful computer could theoretically play every possible game and develop a formula for perfect chess.

Since IBM's Deep Blue first defeated grandmaster Gary Kasparov in a series of games in 1997, chess programs have had a strong record against human champions; but computers still cannot master poker. Programs have proven quite adept at simple versions of the game, with just two players and narrow betting limits, but have greater difficulty determining optimal strategy in no-limit games where bettors may risk any or all of their chips at any point. Furthermore, each additional player exponentially increases the factors a computer must take into account, and no machine has proven successful in multi-player no-limit games.[486]

Unlike chess, poker includes both randomness (the cards each player is dealt) and considerable unknowns. What cards do opponents have? If they bet, does it reflect the strength of their hand or are they bluffing? What type of strategy do they prefer, and have they changed strategies since the

[484] Nelson, “Checkers computer becomes invincible.”

[485] Chinchalkar, “An Upper Bound for the Number of Reachable Positions.”

[486] Wilson, “Jeopardy, Schmeopardy.”

previous hand? How has their recent performance affected their mood? And how would they answer all of these questions about me? These factors create many more possible situations than chess, more than any current computer program can handle. War includes considerably more pieces than chess, and far more unknowns than poker, and if computers cannot win poker tournaments, they will not be taking over military strategy any time soon.

With this in mind, the goal of the Smart SWARM is to reduce the unknowns in warfare to improve the decision-making capabilities of the participants. By providing soldiers and commanders with the outline of outdoor and indoor areas and the location of people and relevant objects, the SWARM could reduce strong actors' disadvantage in the asymmetry of information. However, this system would not be capable of determining political objectives, guessing opponents' strategies or enemy fighters' intentions, determining civilians' allegiances, or handling any of the other complex human considerations incorporated into strategy.

Though the concept of the Smart SWARM draws upon ideas of how a computer would theoretically fight a war, it is a tool to assist human decision-makers rather than a replacement for them. By focusing on gathering and processing information, the SWARM leverages the capabilities of robots and computers to provide soldiers and commanders with information dominance. The robots act autonomously to ensure coverage of a targeted area, while the central computer autonomously organizes the streams of information and identifies potential objects or persons of interest. However, since the SWARM would only be gathering and processing information, rather than destroying property or killing people, it raises fewer concerns about whether humans are sufficiently in the loop than weaponized robots.

It is likely that advanced militaries will increasingly rely on robots that decide on their own what and when to attack, but the Smart SWARM's function would be the same whether humans or robots are the ones firing upon targets. The system therefore could provide an avenue for the development of military robotics that raises fewer concerns about human control. The SWARM enhances informational, rather than destructive, capabilities and therefore not only avoids ethical questions regarding whether machines or humans should be responsible for decisions to fire weapons, but also improves the ability of human soldiers and commanders to remain in the loop, by keeping them informed, in real-time, of the activities of both friendly and enemy humans and robots during combat.

Conclusion

Information-gathering robots networked to powerful computers could provide information superiority and bring the ideal of Network-Centric Warfare closer to reality. As a doctrine for the United States military, NCW did not succeed in Iraq or Afghanistan because the information feeding into the network was of insufficient quantity and quality. In particular, asymmetric warfare against insurgencies appeared poorly suited for a doctrine based on networking forces. However, with a Smart SWARM of robots gathering considerably more information, and a dedicated computer system processing more information more quickly, networked forces could acquire the inputs they need to gain informational advantages as counterinsurgents.

Therefore, robotic technology could provide the means for a strong actor strategy designed to overcome weak actors' advantage regarding the asymmetry of information. Weak actor strategy relies on superior local knowledge, the ability to surprise, and exploitation of strong actors' responsibility to protect everything at once. If utilized in a comprehensive informational strategy, robots have the potential to neutralize many of these weak actor advantages, allowing strong actors to assert their resource superiority to defeat terrorists, insurgents and guerrillas.

Chapter 7: Robotics and Strong Actor Strategy in Irredentist Conflicts: Defending Israeli Civilians

Both a Smart SWARM and counter-robot technology would be useful to strong actors in irredentist conflicts, because, like localized insurgencies, they feature asymmetries of information. However, in irredentist conflicts, unlike localized insurgencies, the strong actor's main territory is in close proximity to the weak actor. While weak actor strategy in localized insurgencies focuses on prolonging the conflict and imposing costs upon the strong actor's military to convince the strong actor to withdraw forces, weak actors in irredentist conflicts can also threaten strong actors' civilians, and they use this ability to try to win concessions from their stronger opponents. However, robotic systems could help protect strong actors' civilians, undermining this element of weak actor strategy.

While the localized insurgents in Iraq or Afghanistan would have to travel thousands of miles to threaten civilians in the United States, Israel faces ongoing asymmetric threats from two non-state actors positioned on its borders: Hezbollah in southern Lebanon and Hamas in the Gaza Strip. When these conflicts escalate, both groups have fired various types of rockets against civilian targets in Israel. These rockets, especially the homemade Qassams fired by Hamas, are fairly inaccurate, and do not cause many casualties. However, when fired in larger numbers, the rockets have killed and injured Israeli civilians, and forced hundreds of thousands of Israelis to flee their homes or take shelter instead of going to school or work. By disrupting normal life in Israel and imposing costs on Israeli civilians, Hezbollah and Hamas have compelled Israel to accept ceasefire agreements that leave Israel's stated goals in the conflicts unaccomplished.

However, if Israel can protect its civilians from rocket fire, it would reduce these networks' ability to exploit the asymmetries of responsibility and resolve. To this end, the Israeli company Rafael Advanced Defense Systems has developed Iron Dome, which is probably the world's most famous counter-rocket system. Unlike the C-RAM systems that protect military bases and convoys, Iron Dome is designed to protect population centers from more distant fire. Like other C-RAMs, Iron Dome utilizes a series of radar, sensors and cameras to determine the flight path of incoming projectiles. However, Iron Dome's central computer only chooses to shoot at the rockets and mortars it determines are heading towards populated areas, and ignores the others. It also aims to destroy incoming projectiles outside of the defended area, ensuring that debris does not fall where it could cause damage.[487]

Iron Dome has already demonstrated an ability to shoot down incoming rockets, and, if it can be expanded to cover all Israeli population centers, this robotic system could facilitate a shift in Israel's strategy against the adversaries on its borders. By reducing the threat from rockets, Israel would have less need to launch attacks aimed at destroying rocket arsenals. These offensive operations put Israeli soldiers at risk, incite retaliatory attacks against Israel, and regularly prompt international condemnations that harm Israel's relations with neighboring states and the international community.   Iron Dome could thus facilitate a more defensive strategy, in which Israel shoots down incoming rockets while refraining from retaliation, thereby protecting its population and nurturing international sympathy. Additionally, in the event of a successful attack against Israel that Iron Dome cannot prevent, such as a cross-border raid, Israel would have greater latitude to retaliate knowing that its population faces less risk from rocket fire.

[487] "Iron Dome."

Hezbollah

As detailed in chapter five, Hezbollah's constant rocket fire into Israel during the 2006 conflict was an essential part of its strategy. In fighting that lasted from July 12 to August 14, 2006, Hezbollah shot almost 4,000 rockets into Israel, primarily inaccurate Katyushas with a maximum range of 30km.[488] These salvos killed 43 civilians and caused “serious” or “moderate” wounds to 76 and “light” wounds to an additional 614, while the threat of rocket attacks displaced about 500,000 Israeli civilians.[489] Rejecting international calls for an early ceasefire, Israeli officials stated their intention to cripple Hezbollah and force the Lebanese government to assert control over Hezbollah's stronghold in southern Lebanon.[490] As Israel's ambassador to the United States Daniel Ayalon put it, “we will go to the end now. We will not go part way and be held hostage again. We'll have to go for the kill – Hezbollah neutralization.”[491]

However, on August 13, Israel accepted a UN-brokered ceasefire despite failing to achieve this goal. Not only did Israel's airstrikes and ground forces fail to neutralize Hezbollah, they were not even able to prevent daily rocket fire against Israeli civilians. Hezbollah fired no fewer than 100 rockets into Israel every day of the conflict, and shot almost 250 on the final day.[492] The Winograd Committee, an independent commission appointed by the Israeli government to investigate and draw lessons from the 2006 war, cited the rocket barrage, and the Israeli Defense Forces' inability to prevent it, as a primary reason that Israel did not achieve its goals.[493]

[488] Cordesman, “The Lessons of the Israeli-Lebanon War,” p. 3.
[489] “Middle East Crisis: Facts and Figures.”
[490] Cordesman, “The Lessons of the Israeli-Lebanon War,” p. 6.
[491] Wright, “Strikes Are Called Part of Broader Strategy.”
[492] Cordesman, “The Lessons of the Israeli-Lebanon War,” p. 3.
[493] “Winograd Committee Submits Final Report,” number 6.

In the years since the 2006 conflict, Hezbollah has rebuilt its arsenal, and now possesses more than 40,000 rockets.[494] These include some missiles that are more sophisticated than the inaccurate Katyushas, such as the Fajr-5, which Hezbollah acquired from Iran. With a maximum range of 75km, a Fajr-5 fired from southern Lebanon could easily hit Haifa and potentially reach the suburbs of Israel's largest city, Tel Aviv.[495] Besides a longer range, the Fajr-5 is larger and flies faster than Katyusha rockets, which makes it harder for Iron Dome to intercept.

To address this threat, Rafael Systems is developing a more advanced anti-missile system with Raytheon known as David's Sling. Unlike Iron Dome, which is designed for shorter range projectiles, David's Sling aims to intercept ballistic missiles and medium range rockets. The system uses a similar combination of radar and electro-optical sensors to track the target projectile and guide an interceptor to collide with it. However, the Stunner interceptor missiles used by David's Sling are faster and more maneuverable than the Iron Dome's Tamir interceptors, similar to a next-generation version of the Patriot anti-ballistic missile used by the United States. In a November 2012 test, David's Sling scored a direct hit on a vehicle simulating a medium-range rocket. Israeli officials expect the system to begin operating in 2014.[496]

The emphasis Hezbollah has placed on acquiring rockets reveals the importance projectiles play in its strategy against Israel. In the event of another conflict, Hezbollah would likely employ an upgraded version of its 2006 strategy, firing more rockets daily, with some of them reaching further into Israel. Meanwhile, this threat somewhat deters Israel from moving more aggressively against Hezbollah or its state sponsor Iran.

[494] Windrem, “Why Hezbollah is sitting on 40,000 rockets and missiles and sitting out the Gaza conflict.”
[495] “Hezbollah Displays Iranian Fajr-5 Missile.”
[496] Eshel, “David's Sling Makes Direct Hit in Interceptor Test.”

Even with a robust Iron Dome presence on the Lebanese border, complimented by David's Sling to defend against Fajr-5s and other more advanced rockets, some missiles would likely get through. Nevertheless, intercepting a significant percentage of rockets would reduce Israeli civilian casualties, which would provide the Israeli military with greater latitude to sustain operations in the event of another conflict with Hezbollah. Israel and Hezbollah are thus engaged in an arms race, with Hezbollah seeking to maintain the capabilities to repeat its successful 2006 strategy and Israel aiming to neutralize a key component of that strategy.

Hamas and other Palestinian Organizations

A similar dynamic has played out on a smaller scale in Israel's ongoing conflict with Hamas, which took control of the Gaza Strip in mid-2007, and other Palestinian resistance groups. Since withdrawing its settlements from Gaza in August 2005, Israel has faced ongoing, sporadic rocket, missile and mortar fire from Hamas' military wing, known as the Izz ad Din al Qassam Brigades, as well as Palestinian Islamic Jihad and other Gaza-based militant groups. Supporters argue that these attacks are a justified response to Israel's ongoing occupation of Palestinian territory, while Israel has demanded that they cease, and launched multiple military operations aimed at preventing further fire. As the following table demonstrates, the number of launches has varied, but the frequency has been sufficient to keep southwestern Israel under constant threat of attack by rockets and mortars:

Rockets, Missiles and Mortars Fired against Israel by Palestinian Organizations 2005-2012			
Year	Rockets[497]	Mortars[498]	Total
2005	401	854	1255
2006	1722	55	1777
2007	1276	1531	2807
2008	2048	1668	3716
2009	569	289	858
2010	150	215	365
2011	419	258	677
2012	2200	196	2396

Rocket attacks are the best tool Hamas and other Palestinian organizations have for imposing costs on Israel. Israel's borders with Gaza and the West Bank are tightly secured, greatly reducing the ability of operatives from Hamas, Palestinian Islamic Jihad, Al Aqsa Martyrs’ Brigades or other groups to enter Israel to attempt suicide bombings. According to Shin Bet, Israel's domestic security service, suicide bombings by Palestinian organizations declined from a high of 53 in 2002, to 26 in 2003, 12 in 2004, and 8 in 2005. Following Israel's withdrawal from Gaza, suicide attacks further declined to 6 in 2006, 1 in 2007, 1 in 2008 and none in either 2009 or 2010.[499] These figures include attacks against Israeli settlers in the West Bank and Gaza (up until the withdrawal in August 2005), civilian targets in Jerusalem and Israel proper, and military checkpoints throughout. The decline in suicide attacks coincides with an increase in rocket and mortar fire from Gaza, indicating both Israel's improved ability to stop the

[497] 2005 through 2010 from “2010 Annual Summary: Data and Trends in Terrorism,” p. 7; 2011 and 2012 from adding up monthly summaries from Israel's Shin Bet Security Agency.

[498] 2005 through 2010 from “2010 Annual Summary: Data and Trends in Terrorism,” p. 8; 2011 and 2012 from adding up monthly summaries from Israel's Shin Bet Security Agency.

[499] “2010 Annual Summary: Data and Trends in Terrorism,” p. 6

former and continued inability to stop the latter, as well as a shift in Hamas' preference in favor of projectiles.

Rockets and mortars fired from Gaza can strike populated areas in Israel, allowing Hamas and other Gaza-based organizations to threaten Israeli civilians. Their primary arsenal includes various mortars, the largest of which carries five pounds of explosives and, with a range of six miles, can reach the southwestern Israeli town of Sderot, as well as Qassam rockets, which are made in Gaza. The first Qassam launch against Israel was in February 2002, with rockets landing between four and five miles from their launch site,[500] but the latest versions, which carry a 20lb warhead, can fly up to 11 miles, putting the seaport city of Ashkelon in range.[501] In addition to these homemade projectiles, Hamas has fired Katyusha and Grad rockets, which were originally produced by the Soviet Union and most likely acquired from Iran, that each carry 35 pounds of explosives and can reach a maximum range of 20 miles. These crude rockets are fairly inaccurate and incapable of reaching Israel's largest population centers.

However, beginning in December 2008, Hamas utilized some more sophisticated, longer range rockets, placing more of Israel under threat. Upgraded Grad rockets, which can travel 30 miles and carry up to 100lb warheads, have hit the city of Beersheba.[502] The WS-1E Weishi rocket, built by the Chinese company Sichuan Aerospace, can fly approximately 30 miles and has also hit Beersheba. The WS-1E includes fin and spin stabilization mechanisms to improve accuracy, and is capable of carrying warheads that include thousands of steel balls, which shoot out up to 100 meters from the point of impact.[503] Most harrowing for Israelis, Hamas has acquired Fajr missiles from Iran's Revolutionary Guard. These 333mm military-grade rockets

[500] “Palestinians launch rockets at Israel.”

[501] “Hamas' Weapons Arsenal Continues to Grow.”

[502] “Two Grad rockets hit Be'er Sheva; IAF strikes Gaza launching squad.”

[503] Shachtman, “Hamas Fires Long-Range Chinese Rockets at Israel.”

can fly more than 46 miles, carry almost 400 pounds of explosives, and travel over 2,280 miles per hour, considerably faster than anything else in Hamas' arsenal. Iran's Fars news agency, which is affiliated with the Revolutionary Guard, published an article in 2012 asserting that introducing the Fajr-5 would change the military balance in the conflict between the Israelis and Palestinians.[504]

Even though most of the rockets Hamas and other Gaza-based groups fire are inaccurate and infrequently hit a person or building, the ongoing threat is sufficient for many Israeli civilians to pressure their government respond. As the following table demonstrates, rockets and mortars fired by Palestinian organizations into Israel have killed 45 Israeli civilians and injured an additional 1,994 in the period from 2006 through 2012. On average, less than one fifth of the projectiles cause any civilian casualties. However, additional costs include property damage, civilians who go to hospitals to be treated for shock, economic losses from business closings, and disruption of normalcy such as internal displacement and school closings.

Israeli Civilian Casualties from Projectiles Fired by Palestinian Groups 2006-2012					
Year	Rockets and Mortars Fired into Israel	Israeli Civilian Casualties[505]		Civilian Casualty Rate Per Projectile	
		Deaths	Injuries	Deaths	Injuries
2006	1777	9	371	0.51%	20.88%
2007	2807	10	578	0.37%	20.59%
2008	3716	15	611	0.40%	16.44%
2009	858	2	11	0.23%	1.28%
2010	365	5	35	1.37%	9.59%
2011	677	3	81	0.44%	11.96%
2012	2396	1	307	0.04%	12.81%

[504] Dehghan, “Iran supplied Hamas with Fajr-5 missile technology.”

[505] 2006 through 2011 from “Hamas' Weapons Arsenal Continues to Grow;” 2012 from adding up monthly summaries from Israel's Shin Bet Security Agency.

In response to rocket fire, Israel has launched airstrikes, artillery shells, and ground raids, imposed an embargo of Gaza in an attempt to prevent weapons and rocket-making materials from entering the territory, and initiated two military operations designed to cease rocket and mortar attacks from Gaza into Israel: Operation Cast Lead from December 27, 2008 to January 18, 2009, and Operation Pillar of Defense from November 14 to 21, 2012. Both conflicts ended in ceasefires; and, as with Israel's war with Hezbollah in 2006, both operations ended without the elimination of Hamas' ability to fire rockets into Israel. However, these conflicts can be considered relatively more successful for Israel than the 2006 war against Hezbollah, because the rate of fire after each conflict declined significantly compared to the rate prior to the operations' beginning.

The Lead-Up to Operation Cast Lead

Operation Cast Lead began after an Egypt-brokered truce between Israel and Hamas from June 2008 collapsed in November 2008, and cross-border rocket and mortar fire resumed. From January through June 18, 2008, Palestinian militants fired 1,199 Qassam rockets and 1,072 mortars into Israel, resulting in 10 fatalities. Over the same period, Israeli shelling, airstrikes, and raids killed 388 Palestinians in Gaza. The ongoing violence prompted Israel and Hamas to enter into an agreement mediated by Egypt's Minister of Intelligence Omar Suleiman. Hamas agreed to halt rocket and mortar attacks and ensure that other Gaza-based groups did as well, and also to negotiate with Israel over the release of their prisoner, Israeli Corporal Gilad Shalit. Egypt and Israel agreed to ease the blockade, and reopen crossings into Gaza, while Egypt would increase its efforts to prevent weapons smuggling and Israel would cease ground raids.[506]

[506] "Israel reopens third Gaza crossing."

The truce held for almost five months. Hamas refrained from firing rockets or mortars into Israel and largely prevented other Palestinian groups from doing so. From June 18th through early November, Israel faced a total of 19 rockets and 18 mortars, suffering only three deaths in an incident in July and none after. Israeli forces killed one Palestinian in Gaza in July and none in the months that followed. Meanwhile, Israel partially eased the blockade, opening the Sufa border crossing and permitting construction materials and an increase of fuel supplies into Gaza.[507]

Despite this relative calm, both sides accused each other of bad faith and the truce collapsed in November. Throughout the five-month truce, Gaza remained under partial blockade, with border crossings and the flow of goods restricted, and Corporal Shalit remained captive. Additionally, Israel accused Hamas of continuing to build tunnels and smuggle weapons into Gaza. To destroy a tunnel that Israel claimed was designed for a raid to kidnap Israeli soldiers in a repeat of the operation that captured Shalit, Israeli forces crossed into Gaza on November 4, 2008, killing one Hamas fighter in the incursion. In response, Palestinians fired mortars at Israeli forces, Israel responded with airstrikes that killed five more Hamas militants, after which Hamas retaliated by firing 35 rockets into Israel, one of which reached the city of Ashkelon but caused no fatalities. As per usual, both sides accused the other of violating the ceasefire, with Israel identifying the tunnel as an immediate threat and Hamas citing the Israeli incursion as the first shots fired.[508] After this incident, attacks escalated back to pre-truce levels. From November 4 to December 27, Palestinian groups fired 486 rockets and 309 mortars into Israel, killing two, while Israeli airstrikes and ground raids killed 17 Palestinians in Gaza.

[507] "Guide: Gaza under blockade."

[508] McCarthy, "Gaza truce broken as Israeli raid kills six Hamas gunmen."

Tensions continued rising as December 19, 2008, the official expiration date of the truce agreement, approached. A high-level Hamas delegation told Egyptian Minister of Intelligence Omar Suleiman on December 14 that they would be willing to stop rocket fire into Israel in exchange for opening all Gaza border crossings with both Israel and Egypt to commercial traffic and a pledge not to launch any attacks in Gaza. A spokesman for Hamas leader Khaled Meshaal expressed skepticism that Israel would honor a ceasefire agreement, but confirmed that Hamas would halt attacks if Israel agreed to "lift the siege of Gaza" immediately after the cessation of hostilities.[509] However, this was accompanied by a promise to continue violent resistance with rocket fire if Israel did not agree to lift the blockade. According to Osama al Muzaini, an official Hamas spokesman, the ceasefire would "not be renewed as long as there is no real Israeli commitment to all of its conditions" because "there is nothing that encourages us to continue with a deal that did not achieve the results we hoped for," namely an end to the blockade.[510]

Similarly, Israeli officials indicated that they would be willing to renew the ceasefire, but expressed doubt that Hamas would honor Israel's demands. Primarily, Israel sought a complete cessation of rocket and mortar fire into Israel and credible verification of an end to weapons smuggling into Gaza, along with progress in negotiations to free Gilad Shalit. Amos Gilad, a representative of Israel's Defense Ministry, expressed these demands in a mid-December meeting with Egypt's Omar Suleiman.[511] However, like Hamas, Israel accompanied this expressed willingness with a threat. "If Hamas doesn't come to its senses and calm the situation," an Israeli defense official warned, "there will be no choice other than an Israeli military response."[512]

[509] Porter, "MIDEAST: Israel Rejected Hamas Ceasefire Offer in December."
[510] "Gaza-Israel truce in jeopardy."
[511] Sofer, "Israel in favor of extending Gaza lull."
[512] Quoted in Ravid et. al., "Hamas declares end to cease-fire, Israeli gov't sources fear violence in unavoidable."

The two sides were unable to reach an agreement and Hamas officially declared the truce over on December 18, one day before it was scheduled to expire.[513] It is unsurprising that Israel and Hamas could not find common ground and chose not to renew the truce, because their goals were incompatible. Hamas demanded a complete end to Israel's blockade of Gaza, which Israel would not agree to since it would permit the importation of weaponry. Israel demanded that Hamas stop importing weapons, especially rockets and rocket-making materials, which Hamas would not agree to, because it would remove its main source of leverage in the ongoing conflict over the Israeli occupation without making tangible progress towards an independent Palestinian state.

Both sides seemed to believe they could get closer to achieving their goals by engaging in an escalated confrontation before returning to negotiations. As with Hezbollah in 2006, Israeli decision-makers hoped that a limited war would enable Israel to destroy some of Hamas' weaponry and send a message that future attacks would be met with military escalation, which would hopefully deter Hamas from firing rockets. Hamas, meanwhile, hoped to deny Israel a military victory while demonstrating its ability to launch enough rockets to harm and frighten the Israeli population despite Israel's efforts to prevent it, which would ideally deter Israel from attacking Gaza or tightening the embargo in the future. This means that both sides wanted an eventual resumption of the ceasefire, but only after what they hoped would be a successful conflict that improved their negotiating position. As Yuval Diskin, the head of Israel's domestic security agency Shin Bet, told an Israeli cabinet meeting, Hamas “is interested in continuing the truce, but wants to improve its terms.”[514]

[513] “TIMELINE – Israeli-Hamas violence since the truce ended.”
[514] “Israeli leaders 'to topple Hamas.'”

Domestic politics likely played a role as well in both sides willingness to escalate. Hamas, which controls Gaza, is engaged in an ongoing competition with Fatah, which controls the West Bank, for domination of Palestinian politics. In addition to Hamas' ability to provide domestic services, a significant portion of its popularity comes from its status as a resistance organization, willing and capable of standing up to Israel, in contrast to Fatah, whose security services coordinate with Israel's. Therefore, if choosing between the two main factions, Palestinians who prefer a nonviolent approach based on negotiation and cooperation with Israel are more likely to side with Fatah, while Hamas' base is made up of Palestinians who advocate confrontation and violent resistance. Hamas entered into a truce agreement with Israel that was supposed to include an end to the blockade of Gaza. Instead, they got a slight relaxation of the embargo, which Israel often re-tightened in response to limited rocket fire from Islamic Jihad or other non-Hamas organizations. Therefore, Hamas had an incentive to reestablish its resistance bona fides by engaging in violent confrontation with Israel, even if it could not achieve a more favorable bargain than the original ceasefire.

Meanwhile, an Israeli general election was scheduled for February 10, 2009, and politicians were trying to establish their security credentials. The two main competitors for Prime Minister, Benjamin Netanyahu of the Likud party, and the Foreign Minister at the time, Tzipi Livni of the Kadima party, both blamed Hamas for the end of the truce and vowed to use force to stop the rockets flying from Gaza. Livni announced that “a government under me will make it a strategic objective to topple the Hamas regime in Gaza,” and that “Israel must react with force when it is fired upon, must re-establish its force of dissuasion and stop the rockets.” Meanwhile, Netanyahu blamed Livni for being too “passive” and claimed that Israelis living near the Gaza border were “paying a heavy price for the mistakes made by Livni and her ministers.” He accused the Israeli government of excessive passivity, and advocated an “active policy of attack.”[515] This campaign rhetoric demonstrates that the two front runners for Prime Minister both believed that a hawkish stance towards Hamas and other Gaza-based organizations would appeal to many Israeli voters.

The Gaza War (December 27, 2008 – January 18, 2009)

On December 27, 2008, Israel launched Operation Cast Lead. The campaign began with airstrikes against targets relating to Hamas' control of Gaza, including government buildings, police stations, and the group's headquarters. As this demonstrates, the Gaza War was between the Israeli state and a state-network hybrid. Hamas is effectively the governing body in the Gaza Strip, though it does not control Gaza's borders and is not recognized by much of the international community, and therefore would not qualify as a small state under the definition presented in chapter two. However, its state-like status presented Israel with targets to attack with precision-guided weaponry at the beginning of Cast Lead, allowing Israel to take advantage of its resource superiority. As with big state – small state conflicts, Israel did not face an informational disadvantage; Israel knew where to strike and Hamas only learned that Israel was launching an air campaign when the first strikes fell. The opening barrage destroyed numerous buildings used by Hamas, and primarily killed Hamas members. Of the 225 killed, only 15 were confirmed civilians.[516]

However, after the first airstrikes, Hamas abandoned official posts, blended into the population, and called on other Palestinian militant groups to work together to resist Israel, giving the conflict a state-network framework. In the air campaign from December 28, 2008 through

[515] “Israeli leaders 'to topple Hamas.'”
[516] “Death toll passes 225 in Israeli offensive on Gaza.”

January 3, 2009, Israel continued to attack targets associated with Hamas, including leaders' homes and mosques believed to be used for weapons storage, and dropped powerful bombs on suspected locations of smuggling tunnels under the border with Egypt. However, the rate of civilian casualties rose from less than 10% to as much as 25%,[517] demonstrating the relative difficulty in hitting military targets after destroying Hamas' official state-like buildings in the original surprise barrage.

The second phase of Operation Cast Lead, a ground invasion, began on January 3, 2009 and lasted until January 17, when Israel declared a unilateral ceasefire. Israel ceased military operations and announced that, if Palestinian groups stopped firing rockets, it would withdraw its forces from Gaza, but would reenter if rocket attacks resumed. One day later, Hamas announced a ceasefire to allow Israeli troops to withdraw, effectively ending the war.[518] Casualty estimates varied, with the Palestinian Ministry of Health claiming 1,314 dead, at least 522 of whom were civilians, and 5,300 additional wounded, split evenly between civilians and militants;[519] while the Israeli Defense Forces reported 1,166 Palestinian deaths, including 709 fighters, 295 civilians, and the remaining 162 unknown.[520] Using these figures, the percentage of Palestinian civilians among the dead was between 25% and 40%.

Israel achieved a number of its tactical goals, and Israeli political leaders declared victory. The IDF killed many Gaza-based militants, including numerous members of the Qassam Brigades,[521] destroyed rocket batteries and other weaponry, and damaged or destroyed up to 80% of the smuggling tunnels,[522] with only nine Israeli soldier deaths and 336 injuries.[523] Israel drew

[517] “Israel steps up offensive in Gaza.”
[518] “Hamas announces ceasefire in Gaza.”
[519] “Field Update on Gaza from the Humanitarian Coordinator.”
[520] Lappin, “IDF releases Cast Lead casualty numbers.”
[521] Harel, “Senior Shin Bet official: Hamas completely lost Gaza war.”
[522] Ramadan and Ferziger, “Gaza Tunnel Owners Renew Smuggling Under Egypt Border.”

international attention to the issue of weapons smuggling into Gaza, and secured an agreement with the United States to increase security and intelligence cooperation and “work with regional and NATO partners to address the problem of the supply of arms and related materiel and weapons transfers and shipments to Hamas and other terrorist organizations in Gaza.”[524] Notably, whether due to destruction or depletion of arsenals, or deterrence created by the military assault, rocket and mortar fire from Gaza slowed considerably, with around 300 total in the nine months after the end of Cast Lead, compared to approximately 600 in the month before alone.[525]

Though Israel achieved these short term military goals, the long term strategic outcome was more mixed. Rocket and mortar attacks slowed considerably, but never stopped entirely. Tunnel operators based in Rafah reported that many tunnels were damaged but remained intact, and after clearing rubble and making some repairs they were able to resume smuggling.[526] While the tunnel operators who spoke to the press discussed smuggling commercial goods, not weapons or weapon-making materials, their comments indicate that Israel did not destroy Hamas' ability to smuggle arms. Overall, Operation Cast Lead did little to advance Israel's goals in the larger Israeli-Palestinian conflict. As Israeli analyst Aluf Benn pointed out, Hamas “won international legitimacy and sympathy, and its forces still control the Gaza Strip.”[527]

Using Robotics to Enhance Israel's Military Capabilities in Asymmetric Combat

Hamas' strategy vis a vis Israel leading up to and during the Gaza war fits the model of a weak actor in an irredentist conflict. Hamas denied Israel victory while imposing costs on Israeli

[523] “Field Update on Gaza from the Humanitarian Coordinator.”
[524] “Text of U.S.--Israel Agreement to end Gaza arms smuggling.”
[525] Kershner, “Along Gaza, a Quiet (but Still Tense) Life.”
[526] Ramadan and Ferziger, “Gaza Tunnel Owners Renew Smuggling Under Egypt Border.”
[527] Benn, “Israel declares victory in Gaza, but at what cost?”

soldiers and civilians to pressure Israel into accepting a deal more favorable to Hamas than the status quo. Given its resource disadvantage, Hamas would not be able to defeat the Israeli Defense Forces in open combat. Additionally, unlike localized insurgencies against foreign powers, Hamas could not convince Israel to withdraw completely. Therefore, to move towards its short term goals of cessation of all Israeli military activity in Gaza and a lifting of the blockade, Hamas utilized a strategy based on exploiting non-material asymmetries.

Hamas exploited the asymmetries of resolve and expectations by denying Israel an easy victory while harming and continuing to threaten Israeli citizens. Once Cast Lead began, Hamas' fighters and other Palestinian militants in Gaza mostly avoided taking positions in the open, where they would be vulnerable to Israeli airstrikes, and prepared for urban guerrilla warfare. Perhaps learning from Hezbollah's tactics in the 2006 war with Israel, they dug an extensive network of tunnels, booby-trapped houses and other structures, and planted IEDs, especially in Gaza City, the largest urban area.[528] This, along with the fact that Palestinian fighters dressed the same as Palestinian civilians, created an asymmetry of information. Not knowing the location of explosives or enemy fighters slowed Israeli operations, while surprise attacks from IEDs or guerrillas emerging from tunnels accounted for a significant percentage of the injuries to Israeli soldiers. An Israeli paratroop brigade commander that briefed reporters estimated that one third of the houses in Gaza City, Khan Yunis, and Rafah were booby-trapped, and that Hamas set up mannequins to distract soldiers, or draw them in for a closer look, whereupon Palestinian fighters would detonate explosives or pop up from a hole in the floor that had been covered with a rug.[529]

A networked swarm of ISR drones integrated with a dedicated computer server would help Israel neutralize this informational disadvantage. Infrared sensors could easily distinguish

[528] Butcher, “Israeli soldiers shocked by tunnel network.”
[529] Bronner, “Israel Lets Reporters See Devastated Gaza Site and Image of a Confident Military.”

between mannequins and people, and identify individuals hiding below rugs or other thin surfaces. Aerial or ground-based robots equipped with Fido sniffers could identify explosives before troops enter houses, which explosive ordinance disposal robots could then remove. Notably, a Smart SWARM would help Israel locate rocket launching batteries before they fire, find weapons caches, and help distinguish between civilians and fighters by identifying who is carrying weapons. Once the SWARM located any of these targets, the system could alert commanders, who could use the information to determine whether to order an airstrike, ground raid, alternative attack, or take no action.

While an integrated Smart SWARM would have a greater effect, Israeli forces did utilize unmanned systems in Cast Lead to counter Hamas' informational advantage. High above Gaza, Israeli UAVs—primarily the Hermes 450, from Elbit Systems, and the Heron, made by Israel Aerospace Industries—carried out ISR missions using infrared and visible light cameras, and sensors capable of intercepting electronic communications.[530] Both unmanned systems, which were developed and built by Israeli companies, are similar in size and function to the RQ-1 Predator, transmitting information gathered from various sources in real-time to a ground station. Like the Predator, both the Hermes and Heron can be modified to carry guided missiles. Additionally, Israel employed at least one unmanned blimp, which remained tethered over the northern border between Gaza and Israel, monitoring the Erez crossing and relaying information from ISR drones to ground stations based inside Israel.[531]

In addition to this higher altitude aerial surveillance, Israeli ground forces utilized small ground-based drones as they moved through Gaza. The Versatile, Intelligent, Portable Robot, or VIPeR, by Elbit Systems, saw combat for the first time in Cast Lead. Similar to a smaller Talon

[530] Esposito, “The Israeli Arsenal Deployed against Gaza during Cast Lead,” p. 182.
[531] Ibid., p. 183.

or more weaponized PackBot, the VIPeR is stout and moves around on adaptable treads that enable the robot to traverse uneven surfaces and climb stairs. It weighs approximately 25 kg, depending on accessories, such as infrared and visible light cameras, an explosives sniffer, an electronic jammer to disrupt remote-detonated IEDs, a four foot arm with a gripper for moving objects, and a weapons mount capable of carrying a 9mm mini-Uzi or grenade launcher. However, unlike the PackBot or Talon, the VIPeR is operated by a harness and helmet-mounted display, which projects what the robot sees to the operator.[532] In Cast Lead, the IDF primarily used VIPeRs to enter buildings ahead of soldiers to gather information and, if necessary, dispose of explosive ordinance.

Israeli soldiers also utilized, for the first time, a ball-shaped camera known as Bull Island. Approximately the size of a tennis ball, this robot can be thrown, dropped, or rolled into a building by soldiers, whereupon it rolls around providing 360-degree imagery of its surroundings.[533] The functionality and limitations are similar to the Throwbot Scout, albeit with a greater ability to provide 360-degree video due to the ball-like instead of dumbbell-like shape.

Taken together, these systems provided what could be considered a preliminary test case of the utility of a Smart SWARM. Gaza is a limited area—the entire Strip is 139 square miles, approximately twice the size of Washington DC—which means the entire territory could be monitored by ISR drones. Unlike Hezbollah's base in southern Lebanon, there are no mountains in Gaza, and Israel directly controls its borders, with the exception of a small section in the south bordering Egypt. The information gathered by aerial and ground-based robots helped Israel limit soldier casualties to 9 deaths and 336 wounded;[534] an impressive rate for 20,000 soldiers engaged

[532] "Elbit Systems Unveils VIPeR a Portable Combat Robot."
[533] Page, "Hurlable 360 cam-grenades used by IDF in Gaza."
[534] "Field Update on Gaza from the Humanitarian Coordinator."

in urban asymmetric warfare. Nevertheless, IDF soldiers were still surprised by booby traps and ambushes. Integrating the large UAVs conducting aerial surveillance and the ground-based robots entering buildings with smaller UAVs and a swarm of insect-sized drones, and processing all of this information through a dedicated computer system, could have reduced Israeli military casualties, sped up the ground operation, and improved the targeting of airstrikes.

Countering Hamas' Rocket Strategy

However, Hamas' strategy did not depend on defeating Israeli ground forces in combat. Given its extreme resource disadvantage, Hamas expected to suffer considerable losses, and could not have hoped to maintain military control of Gaza in the face of an Israeli assault. To achieve its goals, Hamas needed to survive the Israeli attack while exploiting the expectation that the stronger actor in asymmetric conflict has greater responsibility to avoid civilian casualties, shining a spotlight on the suffering of civilians in Gaza to garner domestic and international sympathy. Perhaps most importantly, Hamas needed to demonstrate that it could maintain the ability to threaten Israeli citizens. For that, it needed rockets.

During the Gaza War, Hamas and other Palestinian groups fired 571 rockets and 205 mortars into Israel, maintaining their ability to fire on Israeli citizens throughout the conflict despite Israel's efforts. These attacks resulted in four civilian deaths, 15 “severely” or “moderately” wounded, and an additional 167 lightly wounded. In addition to these casualties, 584 received treatment for shock or anxiety due to proximity to explosions.[535] This places the ratio of civilians killed or wounded per projectile fired from Gaza during the conflict at 24%.

[535] “Operation Cast Lead: Israel strikes back against Hamas terror in Gaza.”

While many rockets did not kill or injure anyone, the barrage from Gaza successfully disrupted normalcy for Israeli civilians. Using longer range rockets, Hamas was able to hit the Israeli cities of Ashdod, Beersheba, and Gedera for the first time. Many fled their homes or hid in bomb shelters, with an estimated 40% of Ashkelon's 110,000 citizens abandoning the city once the rockets began to fall.[536] The projectiles damaged homes and other property, and rockets directly hit at least two schools, leading to closures throughout southern Israel.[537] Numerous businesses closed, and those that remained open faced absenteeism. With an estimated 50% of workers at businesses within range of rockets from Gaza choosing not to go to work, the Manufacturers Association of Israel estimated direct losses to Israeli businesses of 88 million shekels (about $25 million) and tens of millions more in indirect losses, such as delayed shipments or reduced patronage due to customers' fear of rocket attacks.[538] Despite Israeli airstrikes against rocket batteries shortly after they fired, and efforts on the ground to secure rocket-launching positions, Palestinian groups managed to fire rockets into Israel every day of the conflict.

This disruption of life in Israel demonstrates how Hamas uses rockets to exploit asymmetries of expectations and resolve. Given Israel's resource advantage, Israelis expect their government to protect them from rocket attacks. By contrast, Palestinians in Gaza do not expect Hamas will be able to fully protect them from Israeli strikes, and Hamas can therefore utilize Israeli attacks on Gaza to gain additional popular support as Gazans rally around the organization best capable of resistance and retaliation. In hotter conflicts, like the Gaza War launched by Cast Lead, ongoing rocket fire from Gaza led some Israeli civilians to pressure their government to

[536] "Israel-OPT: Ashkelon empties, trauma teams struggle."
[537] Curiel, "Rockets Reach Beersheba, Cause Damage."
[538] Filut and Magen, "Manufacturers claim Cast Lead cost industry nearly NIS 90m."

accept a cease fire. The Israeli government debated a third phase of the war, which would seek to deal Hamas “a knockout blow,” but chose not to because intelligence assessments predicted that this would require prolonged operations that would likely cause heavy casualties on both sides, eroding domestic support for the war and prompting considerable international criticism.[539]

This implies that the Gaza War ended with a mixed outcome due to the asymmetry of resolve. Despite Israel's tactical successes, and large advantage in casualties—1,166 to 1,134 Palestinian deaths, depending on the estimate, compared to 13 Israeli deaths—Israel chose to unilaterally cease fire after achieving some of its immediate goals instead of pursuing a more complete victory. Hamas, by contrast, vowed to fight on, and declared a ceasefire only after Israel ceased operations, which allowed it to consolidate power domestically and rearm.[540] It is unclear whether the possibility of soldier casualties, Israeli civilian casualties, or international criticism played the largest role in Israel's decision not to pursue a more complete victory. Perhaps Israel lacked a plan for what to do in the event it was able to dislodge Hamas from power, and chose not to pursue the conflict further because it did not want to find itself militarily occupying Gaza indefinitely. Whatever the reason, Israel's decision to unilaterally cease fire left its larger conflict with Hamas, and the associated threat of rockets from Gaza, unresolved.

Nevertheless, Operation Cast Lead succeeded in significantly reducing rocket fire from Gaza. After the ceasefires in January, only 162 rockets and 152 mortars flew into Israel from Gaza throughout the rest of 2009. Similarly, in 2010, Israel faced only 150 rocket and 215 mortar attacks.[541] These figures represent a significant decline from the 2,048 rockets and 1,668 mortars fired on Israel in 2008. Furthermore, Hamas did not claim responsibility for any of the launches,

[539] Esposito, “The Israeli Arsenal Deployed against Gaza during Operation Cast Lead,” p. 176.
[540] Al Mughrabi, “Israel plans ceasefire, Hamas vows to fight on.”
[541] “2010 Annual Summary: Data and Trends in Terrorism,” p. 7.

and announced, in November 2009, that it had secured an agreement with other Gaza-based militant groups to refrain from rocket fire, in part to avoid retaliation from Israel.[542] Throughout 2009 and 2010, it appeared that Israel's efforts to deter rocket attacks had mostly succeeded.

However, with the larger Israeli-Palestinian conflict unresolved and the partial blockade of Gaza still in place, the calm did not last. Islamic Jihad fired a mortar in early January 2011 that injured two agricultural workers near the Gaza border.[543] The group launched sporadic rockets and mortars into Israel from Gaza, demonstrating that Hamas was unable, or perhaps unwilling, to ensure that all militant groups refrained from firing.

In March 2011, Israel intercepted a shipment of sophisticated C-704 anti-ship missiles from Iran bound for Gaza aboard the Victoria, a cargo ship owned by a German company and flying a Liberian flag.[544] The shipment was carefully camouflaged, but discovered by an Israeli intelligence operation, and confirmed when Israeli commandos boarded the ship and found the missiles.[545] According to Israeli assessments, the concealed arms shipment was likely placed aboard the Victoria when it docked in the Port of Latakia in Syria, and was probably headed for the Port of El Arish in Egypt, whereupon smugglers would bring the missiles into Gaza through tunnels under the Egyptian border.[546]

This shipment demonstrates that Hamas used the relative quiet with Israel to rearm for future confrontations. Such efforts make sense strategically, as Hamas' main goals remained unrealized and rockets proved its most useful weapon against Israel in recent years. In 2011, Israel still maintained a partial blockade of Gaza, had not entirely ceased occasional military

[542] "Hamas: All Gaza militant groups agree to halt rocket attacks."
[543] "Gaza mortar shell wounds two men at Israeli farm."
[544] Eshel, "Israel Navy Intercepts Missile Loaded Cargo Vessel Bound for Gaza."
[545] Fishman, "Uncovering the missiles."
[546] Eshel, "Israel Navy Intercepts Missile Loaded Cargo Vessel Bound for Gaza."

activity in the territory, and, more broadly, still prevented the creation of an independent Palestinian state. As in 2008 before the Gaza War, Hamas needed rockets if it wished to retaliate against Israeli action or escalate the conflict in pursuit of a more favorable status quo. Even though Israeli intelligence discovered the missiles aboard the Victoria, the incident suggests that there were other shipments that made it to Gaza. The blockade of Gaza may have delayed Hamas' acquisition of weaponry, but it could not provide a lasting solution for Israel to the threat of rocket fire.

By contrast, the Iron Dome counter-rocket system has the potential to protect Israelis rather than simply slow the growth of Hamas' arsenal. From its first deployment, Iron Dome has demonstrated an impressive success rate against limited fire. The first battery was deployed in March 2011 near the southern Israeli city of Beersheba, which had been a target of rockets fired from Gaza.[547] In early April of the same year, Israel deployed a second battery near Ashkelon, which had recently faced a one-day barrage of 15 rockets that wounded two civilians.[548] That battery recorded the first successful interception on April 7, 2011, when it shot down a Grad rocket fired from Gaza towards Ashkelon.[549] Based on this early success, Israel deployed a third battery near Ashdod in August 2011, in anticipation of the start of the school year.[550] After successfully intercepting 75% of targeted rockets in 2011, Iron Dome raised its success rate to 90% in the first three months of 2012.[551]

Each attempted interception costs about $100,000, as Iron Dome typically fires two $50,000 Tamir interceptor missiles at a target to increase the chances of contact.[552] Shooting

[547] “Israel deploys 'Iron Dome' rocket shield.”
[548] Ronen, “Second Iron Dome Battery Deployed – to Protect Ashkelon.”
[549] Pfeffer and Yagna, “Iron Dome successfully intercepts Gaza rocket for first time.”
[550] Katz, “IAF deploys third Iron Dome battery outside Ashdod.”
[551] Katz and Lappin, “Iron Dome ups its interception rate to over 90%.”
[552] Katz, “IAF deploys third Iron Dome battery outside Ashdod.”

down an incoming projectile is thus far more expensive for Israel than the projectile is for the militant groups that fire them; the mortar shells and Qassam rockets manufactured in Gaza cost less than $1,000 each,[553] while the more sophisticated Katyusha, Grad, and Fajr missiles, or the parts necessary to make them, are given to Hamas by foreign sponsors. However, Israel receives money from the United States dedicated to missile defense—$211 million for Iron Dome and an additional $149.68 million for David's Sling in Fiscal Year 2013 alone, with a similar amount expected in FY2014—offsetting much of the cost.[554] More importantly, as a "senior Israeli official" quoted in Time magazine points out, if "rockets actually hit a neighborhood, in terms of the human costs, the wounded, the destruction of infrastructure would be much greater."[555] Furthermore, Iron Dome's ability to anticipate the path of projectiles allows it to refrain from firing at rockets or mortars heading for unpopulated or undeveloped areas, thereby saving Tamirs for interceptions that could save lives, streamlining the system's costs. Factor in the cost of military operations designed to prevent rocket fire, and the indirect economic losses from Israelis fleeing or taking shelter in response to rocket barrages, and Iron Dome is a cost effective solution.

Operation Pillar of Defense

Iron Dome's first real tests came in 2012, with the largest outbreak of violence between Israel and Gaza-based organizations since the Gaza War in December 2008/January 2009. In March 2012, Israel launched a series of airstrikes that killed Zohair al Qaisi, the secretary general of the Popular Resistance Committees, because, Israel claimed, he was planning an attack. The strikes killed at least 15 Palestinians, and Gaza-based militant groups responded with a two-day

[553] Thompson, "Iron Dome: A Missile Shield That Works."
[554] Sharp, "U.S. Foreign Aid to Israel," summary.
[555] Thompson, "Iron Dome: A Missile Shield That Works."

barrage of 95 rockets. Iron Dome intercepted 25 of these, and only one Israeli was injured, while none were killed.[556]

After a string of relatively quiet months—a total of 76 rockets and mortars flew from Gaza in July, August, and September combined—October and November saw an increasing cycle of tit-for-tat escalation, with 171 rocket and mortar launches in October 2012 alone.[557] The Israeli military fired tank shells at a suspected launch site near Rafah, injuring four children and damaging a mosque minaret. A spokesman from the Qassam Brigades announced that "in response to the injury of civilians in the most recent strike on Rafah, the Qassam Brigades and the al-Quds Brigades fired a number of rockets at enemy military positions."[558] This was one of the few times Hamas claimed responsibility for rocket or mortar fire into Israel since the conclusion of the Gaza War in January 2009.

Border clashes continued throughout November, culminating in an attack on Gaza that Israel called Operation Pillar of Defense. On November 5, 2012, Israeli soldiers shot and killed a Palestinian man approaching the Gaza border fence, who medics later said was unarmed and mentally ill.[559] After an IED exploded near an Israeli border patrol, wounding some soldiers, Israeli forces crossed the border in search of bombs, leading to a gunfight with members of the Popular Resistance Committees on November 8. A 12 year old Palestinian boy was killed in the crossfire.[560] In what they stated was a response to the child's death, Hamas operatives blew up a tunnel near the Gaza border fence, which may have originally been constructed to stage a raid into Israel, wounding an Israeli soldier.[561] Two days later, Palestinians fired an anti-tank missile

[556] "At least 15 killed in Israeli air strikes on Gaza."
[557] Murphy, "How many rockets were fired from Gaza at Israel this year?"
[558] "Israel Strikes Gaza after Hamas retaliation."
[559] "Soldiers shoot dead 20-year-old man near Gaza border."
[560] "Israeli gunfire kills Palestinian boy in Gaza clash: medics."
[561] "Gaza: Palestinians killed and Israeli soldiers injured."

at an Israeli jeep patrolling the border, injuring four soldiers, and Israel responded with an airstrike that killed four civilian teenagers but no militants. Gaza-based groups responded by launching 25 rockets, none of which caused any damage. 24 landed in undeveloped areas, while Iron Dome shot down the one rocket headed towards a population center.[562]

These border clashes leading up to Pillar of Defense demonstrate the ongoing instability of the situation between Israel and Gaza, as well as Israel's inability to prevent attacks against its soldiers along the border. Iron Dome cannot shoot down a ground-to-ground anti-tank missile fired at close range, and no defensive measure exists to prevent exploding tunnels. However, these are threats to Israeli soldiers, not civilians, and measures like the tunnel attack require far more elaborate preparation than firing rockets. Iron Dome was able to prevent any Israeli civilian casualties from these rocket attacks, and, if this can restrict Hamas and other Gaza-based groups to attacks against soldiers along the border when they wish to retaliate or escalate, it will weaken their ability to exploit the asymmetry of expectations. Israeli civilians expect their government, as the stronger actor, to protect them from attacks, but accept that soldiers patrolling a volatile border face an ongoing threat. They are therefore more likely to pressure their government to cease fire or make concessions in response to attacks that cause civilian casualties than after attacks that harm soldiers, and more willing to support a sustained military operation if civilians are not dying.

However, further escalation demonstrated that a larger rocket barrage could still harm Israeli civilians. Hamas and other Gaza-based groups fired over 100 rockets in two days, directly hitting a house, a car, and landing near a school, injuring seven. Schools and many businesses

[562] Barzak, “After attack on jeep, Israeli army kills 4 in Gaza.”

were closed, and some power lines were hit, causing outages.[563] While Iron Dome did shoot down numerous projectiles, including a Grad rocket headed towards Beersheba, the system was unable to entirely prevent civilian casualties or disruption of normalcy in Israel when faced with many rockets fired at once.

Claiming that they needed to escalate further to counter these rocket attacks, Israel launched an operation it labeled Pillar of Defense. It began with a surgical strike that killed Ahmed Jabari, the head of Hamas' military wing in Gaza, and lasted from November 14 to 21. The IDF launched airstrikes at over 1,500 targets associated with Hamas and Islamic Jihad, including commanders, rocket launchers and manufacturing sites, and tunnels.[564] The attacks killed 139 Palestinians, at least 70 of whom were civilians, and injured more than 900.[565] However, unlike Cast Lead, Israel opted against following this air campaign with a ground invasion. Israeli officials asserted that the airstrikes had accomplished the goal of stopping rocket attacks, while Hamas leaders claimed that their resistance to Israel's ground invasion in early 2009 had established a deterrent.[566]

Following the assassination of Ahmed Jabari, the Qassam Brigades, Islamic Jihad, and other militant groups launched an operation they called Stones of Baked Clay. According to UN statistics, Gaza-based organizations fired 1,598 rockets over the course of the week, 142 of which landed in Gaza. Of the 1,456 fired into Israel, Iron Dome successfully shot down 409. The barrage included 10 Fajr-5 missiles fired at the suburbs of Tel Aviv and ships stationed offshore, five of which were intercepted by Iron Dome, and three long ranged missiles that hit the outskirts of Jerusalem. The rocket fire killed four Israeli civilians and one soldier, and injured an

[563] “Rockets hit homes in south as fire continues for second day.”
[564] “Operation Pillar of Defense: Summary of Events.”
[565] Ban, “Secretary-General's remarks to the Security Council.”
[566] Barzak and Laub, “Hamas claims victory as ceasefire starts.”

additional 219 civilians and 16 soldiers.[567] This demonstrates the increasing range of Hamas' arsenal, as well as its ability to get some rockets past Israel's defenses when firing many at once.

The conflict ended with a ceasefire brokered by Egypt and the United States with demands and terms similar to previous agreements between Hamas and Israel. Israel agreed to halt all military activity in the Gaza Strip including the targeting of individuals, while Hamas agreed that “all Palestinian factions shall stop all hostilities from the Gaza Strip against Israel including rocket attacks and all attacks along the border.”[568] Additionally, Israel agreed to reopen the border crossings it had shut completely during the conflict, though it has maintained the partial blockade of Gaza and continues inspecting cargo to prevent weapons from entering the Strip.

For Israel, it appears that the operation was mostly successful. In the six months after Pillar of Defense, only 41 rockets and mortars have been launched from Gaza and Sinai towards Israel, compared to 219 in the six months after Cast Lead.[569] However, Hamas remains in control of Gaza, and its grievances, from the blockade of Gaza to the larger Israeli-Palestinian conflict, remain unresolved. Furthermore, the ability of Gaza-based groups to fire almost 1,600 rockets in a week, including some missiles that were more sophisticated than any used during the Gaza War, indicate that Israel's efforts to prevent weaponry from entering the Gaza Strip were at least partially unsuccessful. Given the frequency of cross-border attacks since Hamas took control of Gaza, it would not be surprising if another round of violence brakes out within the next few years.

[567] Ban, “Secretary-General's remarks to the Security Council.”
[568] “TEXT: Cease-fire agreement between Israel and Hamas,” 1A and 1B.
[569] Barnett, “Pillar of Defense versus Cast Lead, 6 months after.”

However, should hostilities escalate in the future, Israel's C-RAM defenses will be more robust. While Iron Dome did not neutralize the threat of rockets from Gaza during Pillar of Defense, the system did demonstrate its ability to reduce the damage they cause. As the following table shows, Hamas and other Palestinian groups fired more rockets during the week-long Pillar of Defense than during the 23 days of Cast Lead, but were not able to kill more Israeli civilians. Facing almost twice as many projectiles, at a rate of over six times as many per day, Israel suffered a lower rate of civilian casualties—approximately 15.3% deaths or injuries per projectile compared to 24% during the Gaza War. And this does not account for the greater prevalence of rockets relative to mortars during Pillar of Defense, or the fact that the rockets used in 2012 were, on average, faster, more accurate, and carried larger payloads than those fired in the 2008/2009 conflict.

Israeli Civilian Casualties: Cast Lead v. Pillar of Defense			
Conflict		Operation Cast Lead	Operation Pillar of Defense
Duration		23 days	7 days
Projectiles fired into Israel		776	1456
Projectiles per day		33.74	208
Civilian Casualties	Deaths	4	4
	Injuries	182	219
Rate of Civilian Casualties per Projectile	Deaths	0.51%	0.27%
	Injuries	23.45%	15.04%

Even though some rockets were able to harm Israeli civilians, the November 2012 conflict demonstrated the potential of the Iron Dome system. Israel has deployed only five Iron Dome batteries, which means much of the country remains unprotected.[570] Even with this limited coverage, the system was able to reduce the casualty rate from rockets; if Pillar of Defense saw a similar rate as Cast Lead, Israeli civilians would have suffered four additional deaths and over 100 additional injuries. Further expanding Iron Dome could cover more of the country, negating the advantage of rockets with longer ranges. Additionally, placing multiple batteries around each city could create some redundancy and increase the number of rockets the system could simultaneously shoot down. The individual batteries have increased their success rate, from hitting 75% of intended targets to over 90%, indicating that engineers have utilized data on Iron Dome's early performance to improve the system. As Israel deploys additional batteries and improves the effectiveness of each interceptor, it will increasingly be able to protect its civilians from the threat of rockets fired across its borders.

Conclusion: Using Iron Dome to Emphasize Defense

Israel's strategy against Hamas has not achieved its goals. To prevent rocket fire, Israel has relied on the use of force: firing airstrikes against rocket launching sites to destroy launchers and kill militants, blockading Gaza to prevent or at least slow rearmament, and engaging in tit-for-tat responses in an attempt to deter future rocket attacks. Twice this strategy led to major escalations in Operation Cast Lead and Operation Pillar of Defense. These measures have had some success at temporarily reducing rocket fire, but the overall strategy has not eliminated the threat.

Israel's attacks on Gaza have not prevented Hamas and other militant organizations from firing rockets and have not created a lasting deterrent. Escalation has achieved short term aims,

[570] Lappin, “Fifth Iron Dome battery deployed in Gush Dan.”

as Egypt-brokered ceasefires in June 2008 and November 2012 created periods of relative quiet that lasted months. Rocket and mortar attacks declined significantly after both Cast Lead and Pillar of Defense, with Hamas holding its fire and working to prevent other Gaza-based groups from launching into Israel. However, all of the lulls in violence still featured some rocket and mortar attacks, rather than zero; and none of the ceasefires have lasted, so it would be naive to assume that the agreement that ended Pillar of Defense will lead to enduring peace. Therefore, Israel's strategy resembles the crude metaphor “cutting the grass,” in which Hamas' arsenal will grow, and Israel will, from time to time, initiate military operations to shrink it back down to a more manageable size.[571] This is a recipe for indefinite conflict; one that becomes more dangerous for Israel as Hamas acquires increasingly sophisticated missiles.

That the grass repeatedly grew to the point where it needed mowing demonstrates that the blockade of Gaza has failed. While there have been individual successes, such as the interception of C-704 anti-ship missiles in March 2011, considerable weaponry has made it past the blockade. Despite Israel's efforts to restrict imports, destroy smuggling tunnels, and deplete stockpiles of rockets and launchers with airstrikes and ground incursions, Hamas and other organizations have managed to fire thousands of projectiles into Israel, including almost 1,600 rockets in one week in November 2012. Clearly, the blockade has not prevented Palestinian resistance groups from acquiring rockets. At best, it has slowed the grass' growth rate and extended the time between cuttings.

Though Israel asserts that preventing weapons from entering Gaza is the exclusive aim of the blockade, it is also possible that an unspoken additional purpose is collective punishment of Palestinian civilians in Gaza. By restricting the supply of consumer goods into the territory,

[571] Bronner, “As Battlefield Changes, Israel Takes Tougher Approach.”

Israel makes life harder for the people living there. Theoretically, residents of Gaza might blame Hamas for this state of affairs, and seek to replace the dominant party with more moderate leaders. However, June 2013 marks six years since Hamas took control of Gaza, and they seem to be in no danger of losing power. More likely, Palestinians in Gaza blame Israel for imposing the blockade and support Hamas for seeking its end, rather than faulting Hamas for pursuing weaponry to resist Israel. Even if Israel sees the suffering of civilians in Gaza exclusively as an unfortunate but unavoidable side effect of its effort to prevent weapons from entering the territory, the result is anger towards Israel and increased support for Hamas.

Furthermore, the tunnel smuggling system has provided Hamas with considerable revenue and a stranglehold on Gaza's economy. Hamas charges a one-time fee to set up each tunnel, and then taxes everything that comes through them. This has generated as much as $750 million per year for Hamas' coffers.[572] If Israel's strategy is to use the blockade to remove Hamas from power, it has been counterproductive.

In addition to increasing Hamas' popularity among Palestinians, the blockade of Gaza has created situations that have galvanized international criticism of Israel. Some may dismiss the international criticism as expression of long-standing anti-Israeli sentiment, but there has been direct harm to Israel's relations with other countries. Notably, relations with Turkey deteriorated after Israeli commandos raided a six-ship flotilla bound for Gaza.

In May 2010, a group of activists organized by the Free Gaza Movement and a Turkish NGO called the Foundation for Human Rights and Freedoms and Humanitarian Relief sailed from Cyprus towards Gaza aiming to break the blockade. To enforce the blockade, the Israeli navy intercepted the ships and directed them to the port of Ashdod for cargo inspection. On one

[572] Verini, “The Tunnels of Gaza.”

of the six ships, a fight broke out between Israeli forces and a group of activists that left nine activists dead, eight of whom were Turkish nationals. Greta Berlin, a leader of the Free Gaza Movement claimed that the flotilla was exclusively carrying humanitarian supplies and that Israeli soldiers "opened fire on sleeping civilians at four in the morning,"[573] while Israel claimed that the soldiers acted in self-defense. According to an Israeli government spokesman, "roughly 40 people on board were jihadis who came for violence. They were preparing to attack, to kill and to be killed" and they attacked the commandos with knives and metal rods immediately upon boarding.[574]

For Israel's larger strategy towards Gaza, what actually happened aboard the ship is less relevant than the aftermath. In response, Turkey recalled its ambassador from Israel and canceled joint military exercises.[575] Israel's relationship with Turkey was arguably closer than with any other state in the region or Muslim-majority country in the world, and deterioration of that relationship and the associated military and economic cooperation harms Israel's position in the Middle East. In March 2013, the United States brokered an agreement that restored relations between Israel and Turkey in which Israel "apologized to the Turkish people for any errors that could have led to the loss of life" and compensated the victims' families.[576] Even if Israel's account of the flotilla raid is entirely accurate, and even though relations with Turkey were eventually restored, this incident illustrates the potential diplomatic costs of maintaining the blockade.

Israel's blockade of Gaza is costly and has not achieved Israel's goal of denying Hamas the weapons to threaten Israeli citizens, but Iron Dome and David's Sling could provide the basis

[573] Kershner, "Deadly Israeli Raid Draws Condemnation."
[574] Sherwood, "Flotilla raid: Turkish jihadis bent on violence attacked troops, Israel claims."
[575] Kershner, "Deadly Israeli Raid Draws Condemnation."
[576] Deitch, "Israel apologizes to Turkey over flotilla deaths."

of an alternative strategy. Weak actors in irredentist conflicts seek to impose costs on their stronger opponents to win concessions and shift circumstances in their favor. To do this, Hamas and other Gaza-based groups depend on rockets, which have proven to be their best means of harming Israeli civilians and disrupting normalcy in Israel. However, if Israel's C-RAM protections can expand and improve to the point where they can shoot down any rockets headed for populated areas, Israel will be able to undermine Hamas' strategy without incurring the costs associated with the blockade or attacks on Gaza.

Iron Dome and David's Sling can facilitate a more defensive strategy, but would not entirely eliminate the threat posed by Hamas or Hezbollah, since a massive rocket barrage may be able to overwhelm Israel's missile defenses. For example, Hezbollah shot almost 4,000 rockets into Israel in the 2006 conflict, and has reportedly rearmed with tens of thousands. Similarly, Hamas and other Gaza-based groups fired almost 1,600 rockets during Operation Pillar of Defense, and may be able to acquire enough to score some hits in a future confrontation, especially if Israel eases the blockade. However, by establishing a strong defense against projectiles, Israel would require its non-state opponents to expend far more rockets to cause any damage. This would neutralize the threat of sporadic rocket fire, reduce Israeli casualties in the event of conflict, and discourage Hamas and Hezbollah from escalating and inviting retaliation if they cannot rely on their rocket arsenals to achieve their goals.

Conclusion

Chapters one and two presented theoretical arguments and empirical support for the claim that the world's most powerful states face a greater security challenge from non-state networks than from small states. This effect increases in the wake of international transitions, as some networks rapidly adapt new strategies to take advantage of changing circumstances. In particular, various networks have enhanced their capabilities by utilizing recent developments in information technology. However, states can marshal their resources to develop new strategies and drive technological innovation in response. As detailed in chapter four, the world’s most advanced states have produced a variety of ground-based and aerial robots that can help compensate for networks’ non-material advantages.

State-network conflicts can be broken down into three categories—localized insurgency, irredentist, and global insurgency—and chapters six and seven propose ways that the most advanced states can use robotics technology to develop informational and defensive strategies to counter localized insurgent and irredentist networks. However, global insurgency is arguably the biggest threat to the world’s most powerful states, and the one for which they are least prepared. Much as weak actor strategists of global insurgency combine lessons from the more localized types of asymmetric conflicts and invent the rest, strong actor strategies in localized insurgencies and irredentist conflicts provide lessons for countering the international jihadist movement.

The threat from this global insurgency is twofold: organized groups, such as al Qaeda in the Arabian Peninsula, who are capable of mounting larger scale attacks; and self-starters, who are less capable of large scale attacks, but harder to identify. The challenge therefore requires a multi-pronged approach: monitoring and shrinking the capacity of any jihadist organization that grows large enough to execute a large terrorist attack or overthrow a friendly government; improving intelligence and hardening targets to thwart attacks by individuals; and reducing the supply of both by winning the war of ideas. As with localized insurgency and irredentist conflicts, robotics can enhance this strong actor strategy.

War of Ideas

Dr. Fadl, one of the first senior members of al Qaeda and the author of “The Essential Guide for Preparation,” began denouncing violent jihad in May 2007. Whereas the “Guide” justifies violence against non-Muslims and called fighting them a religious duty, Fadl's latest writings, which have been published in Egyptian and Kuwaiti newspapers, argue that “we are prohibited from committing aggression, even if the enemies of Islam do that.”[577] Fadl's words always carried special weight based on his widely admired encyclopedic knowledge of Islamic teachings, and al Qaeda accordingly treated his shift from “fight fire with fire” to “two wrongs don't make a right” as a threat. Ayman al Zawahiri released a video publicly dismissing Fadl's new position, indicating al Qaeda's concern.

However, Fadl's change of heart may not make much of a difference in the war of ideas. Though highly respected as a religious scholar, he is 63 years old and the international jihadist movement may have moved on. The relevance of the central al Qaeda organization has decreased, and the movement has shifted towards the loosely connected network of autonomous nodes envisioned by Abu Musab al Suri. Nidal Malik Hassan, a disgruntled Army psychiatrist inspired by Anwar al Awlaki, killed more Americans in the name of jihad on US soil in the Fort Hood shooting than any al Qaeda operative has in the 12 years after the September 11th attacks.

[577] Wright, “The Rebellion Within,” p. 1.

Tamerlan and Dzhokhar Tsarnaev, self-starters sympathetic to the jihadist cause but unaffiliated with any organized group, executed the only successful bomb attack on American soil in the 21st century. Additionally, online jihadist forums have become increasingly relevant, as fixed bases in Afghanistan, Pakistan, Iraq, Somalia, Yemen, and elsewhere have come under pressure. It is possible that the rising generation does not consider Dr. Fadl or Ayman al Zawahiri's opinions to be especially important.

Efforts to win the war of ideas, from economic development programs, to the US-based Arabic language satellite TV channel al Hurra (“the free one”), to eloquent presidential speeches, can reduce the appeal of the international jihadist movement, but will do little to soothe the most radical adherents. On June 4, 2009, President Barack Obama gave a speech at Cairo University, saying “I've come here to Cairo to seek a new beginning between the United States and Muslims around the world, one based on mutual interest and mutual respect, and one based upon the truth that America and Islam are not exclusive and need not be in competition. Instead, they overlap, and share common principles – principles of justice and progress; tolerance and the dignity of all human beings.”[578] This attempt at reconciliation was well received, including by many who had been angry at the United States throughout George W. Bush's presidency. But few, if any of those individuals aim to commit violence or directly support those who do, and the main political grievances motivating jihadists and their supporters remain. The United States has not withdrawn support for Israel or Saudi Arabia and is unlikely to do so in the foreseeable future. Without changing those policies, efforts to win the war of ideas can, at best, achieve improvements at the margins. Similarly, the United States can withdraw troops from Afghanistan as it withdrew from

[578] Obama, “A New Beginning.”

Iraq, and can talk about closing (or actually close) the prison at Guantanamo Bay, but anyone radicalized by American policies in the years after September 11th will not easily forget.

There will be people who want to fight under the banner of al Qaeda, and they will continue to find like-minded individuals and terrorism instructions online, which means the War on Terrorism will continue. Robots and information technology can facilitate a strategy designed to neutralize the transnational jihadist network's advantages regarding non-material asymmetries.

Drone Attacks

As discussed in chapter four, attacks launched from unmanned aerial vehicles can increase certainty and reduce collateral damage by waiting for the opportune moment to strike. Drones provide the United States with a cost-effective measure of targeting known enemies. For example, an attack in Yemen on September 30, 2011 killed Anwar al Awlaki of al Qaeda in the Arabian Peninsula, who had recruited the underwear bomber, and inspired the Fort Hood shooter and would-be Times Square bomber, among others. This method has drawbacks, creating anger in the countries where people are targeted as well as those that host American drone bases. However, it is the least bad solution compared to the others—manned airstrikes and ground raids usually result in higher collateral damage while putting American forces at risk, and doing nothing risks allowing terrorist attacks, whether directed or inspired. For these reasons, targeted UAV strikes are likely to remain central to America's strategy against the global al Qaeda network.

However, demonstrating their strategic adaptability, al Qaeda has a counter-strategy for drones.[579] Fleeing a joint French and African operation to push them out of Timbuktu, Mali, al

[579] "The Al-Qaida Papers – Drones."

Qaeda in the Islamic Maghreb left behind a number of strategic documents. Among them were instructions on how to avoid drone attacks. This provides further evidence that the global jihadist movement acts like a transnational advocacy network, as one node shares information that's useful to the entire group, increasing the effectiveness of each autonomous unit.

After explaining that UAVs provide the United States and United Kingdom with a cost effective method relative to manned aircraft, the document offers both technical and tactical ways fighters can protect themselves from unmanned aircraft. This includes jamming or confusing the drone's signal with high and low-tech methods, using the SkyGrabber system mentioned in chapter five to “infiltrate the drone's waves and frequencies,” and spreading pieces of reflective glass on top of a vehicle or building. Other than the glass, which may or may not work, those methods have a proven track record of success.

Tactical recommendations include: avoid congregating in the open, refraining from using a permanent headquarters, hide under thick trees, stay in places unlit by sun, and enter and exit through multiple entrances. These are all logical methods of avoiding aerial surveillance, all of which could be thwarted by the Smart SWARM proposed in chapter six, since micro UAVs can fly below cover and into buildings. Other techniques, such as “using dolls and statues to be placed outside false ditches to mislead the enemy” underestimate the sensor array on most ISR drones, as both infrared cameras and electro-optical sensors could distinguish the dolls from people.

However, the document does show an understanding of drones' electronic surveillance capabilities, as it instructs everyone to “maintain silence of all wireless contacts” and leaders to avoid all communications equipment “because the enemy usually keeps a voice tag through which they can identify the speaking person.” These techniques would partially thwart efforts to monitor electronic communications. Nevertheless, this reaction demonstrates that the mere threat of drones provides strong actors' with strategic value, as al Qaeda operatives avoid both meeting in person and communicating with each other remotely.

Similarly, the document recommends getting out of and staying away from vehicles, “especially when being chased or during combat,” and fleeing in different directions “because the planes are unable to get after everyone.” Perhaps without realizing it, this responds to the ability of Wide Area Airborne Surveillance Systems and other less sophisticated cameras to follow a vehicle and keep it in frame. More powerful cameras could track individuals, and other objects smaller than vehicles, and the Smart SWARM could assign a couple of tiny UAVs to follow each fleeing suspect. However, if al Qaeda fighters avoid using vehicles when fighting or fleeing, their mobility is already compromised.

Al Qaeda in the Islamic Maghreb's methods to avoid drones show the value of UAVs just from the fear they spread. With more powerful cameras, a complimentary swarm of drones closer to the ground, more sophisticated computers to process more information more quickly, and defensive measures that shield the UAVs from spoofing, most of these counter-drone techniques can be thwarted with technological solutions. This is one example of many possible ways robots can enhance strong actor strategy in what will likely be a prolonged conflict against the jihadist global insurgency.

The Future of Asymmetric Warfare

The end of the Cold War and the information technology revolution created a window of opportunity that various non-state actors were able to exploit. Improved strategies and developments in robotics have helped powerful states respond, improving their capabilities against networks. However, the record of the post-Cold War world still shows non-state networks as an ongoing security challenge for great powers. Given their adaptability, some networks, perhaps a node of the global jihadist movement, will take advantage of increasingly available commercial robotics to gather information or attack targets. The United States and other developed countries would be wise to develop counter-robot capabilities—which would also be useful in symmetric confrontations—instead of waiting until after a network surprises by using one.

As technology develops, the rate of change speeds up. Public internet access is less than two decades old, widespread cell phone use began barely a decade ago, and smart phones and social media have been around for less than ten years. The robotics revolution will bring profound changes, as might advances in other areas, such as biotechnology, creating windows of opportunity for networks to exploit. Therefore, as long as nuclear states can check each other and easily defeat non-nuclear states, networks are likely to remain among the more serious security challenges they face. However, while the level of threat will wax and wane, in part based on how well networks and states react to future transitions, terrorism and insurgency are both unlikely to pose an existential threat or fade to a nuisance in the near future.

Appendix

Nuclear State	Opponent	Conflict Type	Opponent Type	Start Month	Start Year	End Month	End Year	Conflict Duration (months)	Military Fatalities	Civilian Fatalities	Outcome
USA	North Korea/China	Interstate	Small State	6	1949	7	1953	49	36516	0	Mixed
USA	Puerto Rican Nationalist Party	Irredentist	Network	11	1950	11	1950	1	1	0	Success
USA	Cuba	Interstate	Small State	4	1961	4	1961	1	4	0	Failure
USA	North Vietnam/Vietcong	Interstate	Small State	7	1959	5	1973	166	58178	0	Failure
USA	Iranian Revolutionaries	Localized insurgency	Network	11	1979	1	1981	15	8	0	Mixed
USA	Grenada	Interstate	Small State	10	1983	10	1983	1	19	0	Success
USA	Amal, LNM	Localized insurgency	Network	8	1982	3	1984	19	265	17	Failure
USA	Libya	Interstate	Small State	3	1986	3	1986	1	2	0	Success
USA	Panama	Interstate	Small State	12	1989	12	1989	1	23	0	Success
USA	Iraq	Interstate	Small State	1	1991	2	1991	1	235	0	Success
USA	Somali Rebels (Habr Gidr Clan)	Localized insurgency	Network	1	1991	12	1993	36	18	0	Failure
USA	Al Qaeda	Global insurgency	Network	12	1992	7	2013	224	104	3025	Ongoing
USA	Serbia	Interstate	Small State	3	1999	6	1999	3	2	0	Success
USA	Taliban	Interstate	Small State	10	2001	12	2001	2	14	0	Success
USA	Afghan Insurgency	Localized insurgency	Network	12	2001	7	2013	140	2246	0	Ongoing
USA	Iraq	Interstate	Small State	3	2003	5	2003	2	187	0	Success
USA	Iraqi insurgency	Localized insurgency	Network	5	2003	12	2011	103	4299	0	Mixed
Russia/USSR	UPA	Irredentist	Network	1	1944	12	1953	120	5750	456	Success
Russia/USSR	Hungarian revolutionaries	Irredentist	Network	10	1956	11	1956	1	722	0	Success
Russia/USSR	Czechoslovakia	Irredentist	Small State	8	1968	10	1968	2	11	0	Success
Russia/USSR	China	Interstate	Big State	3	1969	12	1969	9	58	0	Mixed
Russia/USSR	Mujahideen	Localized insurgency	Network	5	1978	2	1989	129	13310	0	Failure
Russia/USSR	APF	Irredentist	Network	1	1990	1	1990	1	35	0	Success
Russia/USSR	Republic of Armenia	Irredentist	Network	8	1990	12	1991	16	0	0	Mixed
Russia/USSR	Paramilitary Forces	Irredentist	Network	10	1993	10	1993	1	0	145	Success
Russia/USSR	UTO	Localized insurgency	Network	6	1992	6	1997	42			Mixed
Russia/USSR	Chechen Republic of Ichkeria	Irredentist	Network	12	1994	8	1996	20	4175	0	Failure
Russia/USSR	Chechen Republic of Ichkeria	Irredentist	Network	8	1999	7	2013	167	4611	1361	Ongoing
Russia/USSR	Wahhabi Movement of the Buinaksk district	Irredentist	Network	9	1999	9	1999	1	279	293	Success
Russia/USSR	Forces of the Caucasus Emirate	Irredentist	Network	11	2007	7	2013	69	667	0	Ongoing
Russia/USSR	Georgia	Irredentist	Small State	8	2008	8	2008	1	64	0	Success

Nuclear State	**Opponent**	**Conflict Type**	**Opponent Type**	**Start Month**	**Start Year**	**End Month**	**End Year**	**Conflict Duration (months)**	**Military Fatalities**	**Civilian Fatalities**	**Outcome**
United Kingdom	Malayan People's Anti-British Army	Localized insurgency	Network	6	1948	7	1960	144	509	1	Success
United Kingdom	Mau Mau	Localized insurgency	Network	1	1952	10	1956	46	590	32	Success
United Kingdom	Free Officer's Committee/Egypt	Localized insurgency	Network	1	1952	8	1954	32	59	17	Failure
United Kingdom	EOKA (National Org of Cypriot Fighters)	Localized insurgency	Network	4	1955	3	1959	48	116	26	Failure
United Kingdom	Egypt	Interstate	Small State	10	1956	11	1956	1	22	0	Mixed
United Kingdom	Revolt "led by Ghalib and Talib"	Localized insurgency	Network	7	1957	1	1959	17	7	0	Success
United Kingdom	North Kalimantan National Army	Localized insurgency	Network	12	1962	12	1962	1	7	0	Success
United Kingdom	Indonesia	Interstate	Small State	4	1963	8	1966	40	114	0	Success
United Kingdom	FLOSY, NLF	Localized insurgency	Network	10	1964	11	1967	36	129	19	Failure
United Kingdom	IRA	Irredentist	Network	8	1969	4	1998	332	1114	621	Mixed
United Kingdom	Popular Front for the Liberation of Oman and the Arabian Gulf	Localized insurgency	Network	7	1972	3	1976	44	61	0	Success
United Kingdom	Argentina	Interstate	Small State	4	1982	6	1982	2	257	0	Success
United Kingdom	Iraq	Interstate	Small State	1	1991	2	1991	1	56	0	Success
United Kingdom	RIRA	Irredentist	Network	4	1998	7	2013	182	29	2	Ongoing
United Kingdom	Serbia	Interstate	Small State	3	1999	6	1999	3	0	0	Success
United Kingdom	Revolutionary United Front (RUF)	Localized insurgency	Network	9	2000	9	2000	1	6	0	Success
United Kingdom	Taliban	Interstate	Small State	10	2001	12	2001	2	0	0	Success
United Kingdom	Afghan Insurgency	Localized insurgency	Network	12	2001	7	2013	140	444	0	Ongoing
United Kingdom	Iraq (Saddam Hussein)	Interstate	Small State	3	2003	5	2003	2	33	0	Success
United Kingdom	Iraqi insurgency	Localized insurgency	Network	5	2003	4	2009	71	146	0	Mixed
France	FLN, MNA	Localized insurgency	Network	11	1954	7	1962	92	17456	2788	Failure
France	Tunisia	Interstate	Small State	7	1961	7	1961	1	24	0	Success
France	Gabonese military officers	Localized insurgency	Network	2	1964	2	1964	1	1	0	Success
France	National Liberation Front of Chad	Localized insurgency	Network	8	1969	6	1971	23	35	0	Success
France	Polisario	Localized insurgency	Network	12	1977	12	1977	1	0	0	Success
France	Frolinat	Localized insurgency	Network	4	1978	4	1978	1	2	0	Success
France	Followers of Hissene Habre	Localized insurgency	Network	2	1979	2	1979	1	0	4	Mixed
France	Corsican National Liberation Front	Irredentist	Network	5	1976	7	2013	433	0	103	Ongoing
France	Amal, LNM	Localized insurgency	Network	8	1982	3	1984	19	89	0	Failure

Nuclear State	Opponent	Conflict Type	Opponent Type	Start Month	Start Year	End Month	End Year	Conflict Duration (months)	Military Fatalities	Civilian Fatalities	Outcome
France	Goukouni Oueddei	Localized insurgency	Network	6	1983	1	1987	43	0	0	Success
France	Iraq	Interstate	Small State	1	1991	2	1991	1	9	0	Success
France	Serbia	Interstate	Small State	3	1999	6	1999	3	0	0	Success
France	Taliban	Interstate	Small State	10	2001	12	2001	2	0	0	Success
France	Afghan Insurgency	Localized insurgency	Network	12	2001	11	2012	131	88	0	Mixed
France	Ivory Coast	Interstate	Small State	1	2003	11	2004	23	9	0	Success
China	India	Interstate	Small State	10	1967	10	1967	1	9	0	Failure
China	Myanmar/Burma	Interstate	Small State	1	1969	11	1969	11			Mixed
China	USSR	Interstate	Big State	3	1969	12	1969	9	600	0	Mixed
China	Vietnam	Interstate	Small State	2	1979	3	1979	1	6954	0	Failure
Israel	Egypt, Syria, Jordan, Iraq	Interstate	Small State	6	1967	6	1967	1	831	15	Success
Israel	Egypt	Interstate	Small State	7	1967	3	1969	21	118	0	Mixed
Israel	PLO/Fatah	Irredentist	Network	7	1967	8	1970	38	183	12	Mixed
Israel	Egypt	Interstate	Small State	3	1969	8	1970	17	330	140	Success
Israel	PFLP, PLO	Irredentist	Network	8	1970	12	1987	208	239	239	Mixed
Israel	Egypt, Syria	Interstate	Small State	10	1973	10	1973	1	2674	0	Success
Israel	Syria	Interstate	Small State	3	1974	5	1974	2	83	0	Mixed
Israel	Palestinians (various)	Irredentist	Network	12	1987	9	1993	69	63	100	Mixed
Israel	Fatah, PLO	Irredentist	Network	3	1978	3	1978	1	34	38	Mixed
Israel	Lebanon, Syria, PLO	Irredentist	Network	6	1982	5	1983	11	657	0	Mixed
Israel	Hezbollah and other groups	Irredentist	Network	5	1983	5	2000	84	256	90	Failure
Israel	Iraq	Interstate	Small State	1	1991	2	1991	1	0	2	Success
Israel	Palestinians (various)	Irredentist	Network	9	1993	9	2000	84	86	186	Mixed
Israel	Palestinians (various)	Irredentist	Network	9	2000	2	2005	53	303	654	Mixed
Israel	Hezbollah	Irredentist	Network	7	2006	8	2006	1	116	43	Failure
Israel	Palestinians (various)	Irredentist	Network	2	2005	12	2008	45	216	77	Mixed
Israel	Hamas, Islamic Jihad, and other Gaza-based militant groups	Irredentist	Network	12	2008	1	2009	1	9	4	Mixed
Israel	Palestinians (various)	Irredentist	Network	1	2009	11	2012	46	11	34	Mixed
Israel	Hamas, Islamic Jihad, and other Gaza-based militant groups	Irredentist	Network	11	2012	11	2012	1	1	4	Mixed
Israel	Palestinians (various)	Irredentist	Network	11	2012	7	2013	7	0	1	Ongoing

Bibliography

Academic and Military Articles

Abrahms, Max, “Why Terrorism Does Not Work,” *International Security*, vol. 31, no. 2, Fall 2006, pp.42-78.

Alberts, David S., John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition, February 2000. http://www.dodccrp.org/files/Alberts_NCW.pdf

Arce, Daniel G., and Todd Sandler, “Terrorist Signaling and the Value of Intelligence,” *British Journal of Political Science*, vol. 37, 2007, pp. 576-586.

Atran, Scott “The Moral Logic and Growth of Suicide Terrorism,” *The Washington Quarterly*, vol. 29, no. 2, 2006, pp. 127-147.

Balkin, Jack M. and Levinson, Sanford, "The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State" (2006). *Faculty Scholarship Series.* Paper 231. http://digitalcommons.law.yale.edu/fss_papers/231

Betts, Richard K., “The Soft Underbelly of American Primacy: Tactical Advantages of Terror,” *Political Science Quarterly*, 117, no. 1, 2002.

Bueno de Mesquita, Ethan, and Eric S. Dickson, “The Propaganda of the Deed: Terrorism, Counterterrorism, and Mobilization,” *American Journal of Political Science*, vol. 51, no. 2, April 2007, pp. 364-381.

Bullard, Wilder “All Against All: The Tajik Civil War (1991-1997),” *The Washington Review of Turkish & Eurasian Affairs*, November 2011. http://www.thewashingtonreview.org/articles/all-against-all-the-tajik-civil-war.html

Cebrowski, Arthur K., and John J. Garstka, “Network-Centric Warfare: Its Origin and Future,” *United States Naval Institute Proceedings* 124, no. 1, 1998.

Chinchalkar, Shirish, “An Upper Bound for the Number of Reachable Positions,” *ICCA Journal*, vol. 19, no. 3, 1996, pp. 181-183.

Cordesman, Anthony, “The Lessons of the Israeli-Lebanon War,” *Center for Strategic and International Studies*, March 11, 2008, http://www.csis.org/media/csis/pubs/080311_lessonleb-iswar.pdf

Cronin, Audrey Kurth, “How al-Qaida Ends: The Decline and Demise of Terrorist Groups,” *International Security*, vol. 31, no. 1, Summer 2006, pp.7-48.

Denning, Dorothy E., “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” in Arquilla and Ronfeldt, *Networks and Netwars*, pp. 239-288.

Dokmanic, Ivan and Reza Parhizkar, Andreas Walther, Yue M. Lu, and Martin Vetterli, “Acoustic echoes reveal room shape,” *Proceedings of the National Academy of Sciences of the United States of America*, May 17, 2013. http://www.pnas.org/content/early/2013/06/12/1221464110.full.pdf

Downes, Alexander B., “Restraint or Propellant? Democracy and Civilian Fatalities in Interstate Wars,” *Journal of Conflict Resolution*, Vol. 51, No. 6, December 2007, pp. 872-904.

"Drone Strikes Widely Opposed, Global Opinion of Obama Slips, International Policies Faulted," *Pew Global Attitudes Project*, June 13, 2012. http://www.pewglobal.org/2012/06/13/global-opinion-of-obama-slips-international-policies-faulted/

Duyvesteyn, Isabelle, "How New is the New Terrorism?," *Studies in Conflict and Terrorism*, vol. 27, no. 5, Sept-Oct 2004, pp.439-454.

Eilstrup-Sangiovanni, Mette, and Calvert Jones, "Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think," *International Security*, vol. 33, no. 2, Fall 2008, pp. 7-44.

Esposito, Michele K., "The Israeli Arsenal Deployed against Gaza during Operation Cast Lead," *Journal of Palestine Studies*, vol. 38, no. 3, Spring 2009, pp. 175-191.

Fishel, Kimbra L., "Challenging the Hegemon: Al Qaeda's Elevation of Asymmetric Insurgent Warfare Onto the Global Arena." in Bunker, Robert J. ed., *Networks, Terrorism, and Global Insurgency*, New York, New York: Routledge, pp. 115-128.

Glaser, Charles L., "The Security Dilemma Revisited," *World Politics* 50, 1 1997.

Jervis, Robert, "Cooperation under the Security Dilemma," *World Politics*, vol. 30, no. 2.

Johnston, Patrick B. and Anoop Sarbahi, "The Impact of US Drone Strikes on Terrorism in Pakistan," February 25, 2012. http://patrickjohnston.info/materials/drones.pdf

Juergensmeyer, Mark, "Terror in the Mind of God: The Global Rise of Religious Violence," *Police Practice and Research*, vol. 6, no. 2, May 2005, pp. 201- 208.

Kalb, Marvin, "The Israeli-Hezbollah War of 2006: the Media as a Weapon in Asymmetrical Conflict," February 2007, http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07-012/$File/rwp_07_012_kalb.pdf.

Kalyvas, Stathis, "The Paradox of Terrorism in Civil War," *Journal of Ethics*, vol. 8, pp. 97-138, 2004, http://research.yale.edu/stathis/files/Paradox.pdf

Kissinger, Henry, "The Vietnam Negotiations," *Foreign Affairs*, Vol. 48, No. 2 (January 1969).

Kydd, Andrew, and Barbara Walter, "The Strategies of Terrorism," *International Security*, vol. 31, no. 1, Summer 2006, pp. 49-80

Lake, David A., "Rational Extremism: Understanding Terrorism in the Twenty-First Century," *International Organization*, Spring 2002, pp. 15-29.

Luft, Gal, "Israel's Security Zone in Lebanon – A Tragedy?," *Middle East Quarterly*, September 2000, pp. 13-20. http://www.meforum.org/70/israels-security-zone-in-lebanon-a-tragedy

Lyall, Jason, and Isaiah Wilson III, "Rage against the Machines: Explaining Outcomes in Counterinsurgency Wars," *International Organization*, Vol. 63, Issue 1, 2009, pp. 67-106.

Mack, Andrew, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict," *World Politics*, vol. 27, no. 2, January 1975, pp. 175-200.

Meigs, General Montgomery C., "Unorthodox Thoughts about Asymmetric Warfare," *Parameters*, Summer 2003, pp. 4-18.

Morris, Lieutenant Colonel Michael F., “Al Qaeda as Insurgency,” *U.S. Army War College*, 2005. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA434874

Mueller, John, “Is There Still a Terrorist Threat?: The Myth of the Omnipresent Enemy,” *Foreign Affairs*, September/October 2006. http://www.foreignaffairs.com/articles/61911/john-mueller/is-there-still-a-terrorist-threat-the-myth-of-the-omnipresent-en

Mueller, John, and Mark G. Stewart, “The Terrorism Delusion: America's Overwrought Response to September 11,” *International Security*, Vol. 37, No. 1, Summer 2012, pp. 81-110.

Pomper, Philip, “Russian Revolutionary Terrorism,” chapter three in Crenshaw, Martha ed., *Terrorism in Context*, pp. 63-104.

Powell, Robert, “Guns, Butter, and Anarchy,” *American Political Science Review*, Vol. 87, No. 1, March 1993, pp. 115-132.

Riedel, Bruce, “The 9/11 Attacks' Spiritual Father,” *Brookings*, September 11, 2011. http://www.brookings.edu/research/opinions/2011/09/11-riedel

Siqueira, Kevin, and Todd Sandler, “Terrorist Versus the Government: Strategic Interaction, Support and Sponsorship,” *Journal of Conflict Resolution*, vol. 50. no. 6, 878-898.

Thompson, Loren B., “The Twilight of Network-Centric Warfare,” *Defense Professionals*, August 9, 2010. http://www.defpro.com/news/details/17429/

Tucker, David, “What is New about the New Terrorism and How Dangerous is It?,” *Terrorism and Political Violence*, vol. 13, no. 3, Fall 2001, pp. 1-14.

Valentino, Benjamin and Paul Huth and Dylan Balch-Lindsay, “Draining the Sea: Mass Killing and Guerrilla Warfare,” *International Organization*, vol. 58, no. 2, 2004, pp. 375-407.

Valentino, Benjamin and Paul Huth and Sarah Croco, “Bear Any Burden? How Democracies Minimize the Costs of War,” *The Journal of Politics*, Vol. 72, Issue 02, 2010.

Valentino, Benjamin and Paul Huth and Sarah Croco, “Covenants without the Sword: International Law and the Protection of Civilians in Times of War,” *World Politics*, Vol. 28, No. 3, April 2006, pp. 339-377.

Vego, Milan, “The NCW Illusion,” *Armed Forces Journal*, January 2007.

Books

Allison, Graham, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Henry Holt and Co.: New York, New York, 2004.

Al-Muqrin, 'Abd Al-'Aziz, *A Practical Course for Guerrilla War*, translated by Norman Cigar in *Al-Qa'ida's Doctrine for Insurgency*, Dulles, Virginia: Potomac Books Inc., 2009.

Arquilla, John and David Ronfeldt, *In Athena's Camp*, Arlington Virginia: RAND, 1997.

Arquilla, John and David Ronfeldt, *Networks and Netwars*, Arlington Virginia: RAND, 2001.

Arquilla, John, *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World*, Chicago, Illinois: Rowman and Littlefield Publishing Group, 2011.

Arreguin-Toft, Ivan, *How the Weak Win Wars: A Theory of Asymmetric Conflict*, Cambridge, United Kingdom: Cambridge University Press, 2005.

Beckett, Ian F.W., *Modern Insurgencies and Counterinsurgencies: Guerrillas and their Opponents since 1750*, London, United Kingdom: Routledge, 2001.

Barnett, Thomas P.M., *Blueprint for Action*, New York, New York: G.P. Putnam's Sons, 2005.

Barnett, Thomas P.M., *The Pentagon's New Map*, New York, New York: Berkley Books, 2004.

Bergen, Peter L., *The Longest War*, New York, New York: The Free Press, 2011.

Bergen, Peter L., *The Osama bin Laden I know*, New York, New York: The Free Press, 2006.

Bloom, Mia, *Dying to Kill: The Allure of Suicide Terror*, New York, New York: Columbia University Press, 2005.

Brachman, Jarret M., *Global Jihadism: Theory and Practice*, New York, New York: Routledge, 2009.

Brown, Michael ed. *Offense, Defense and War*, Cambridge, Massachusetts: The MIT Press, 2004.

Carafano, James Jay and Paul Rosenzweig, *Wining the Long War*, Berwyn Heights, MD: Heritage Books, 2005.

Chen, King, *China's War with Vietnam*, Hoover Institution Press, Stanford University, 1979.

Clarke, Richard, *Against All Enemies*, New York, New York: Simon & Schuster, 2004.

Cohen, Avner, *Israel and the Bomb*, New York, New York: Columbia University Press, 1998.

Coll, Steve, *Ghost Wars*, New York, New York: Penguin Books, 2004.

Crenshaw, Martha ed., *Terrorism in Context*, University Park, Pennsylvania: The Pennsylvania State University Press, fourth printing, 2007.

Galula, David, *Counterinsurgency Warfare: Theory and Practice*, London, United Kingdom: Praeger Security International, 1964, 2006.

Galula, David, *Pacification in Algeria*, Arlington, Virginia: Rand, 2006.

Giap, Vo Nguyen, *People's War People's Army*, Honolulu, Hawaii: University Press of the Pacific, 1961.

Giustozzi, Antonio, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan*, New York, New York: Columbia University Press, 2008.

Guevara, Che, *Guerrilla Warfare*, Lincoln, Nebraska: University of Nebraska Press, 1960.

Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror*, New York, New York: Columbia University Press, 2002.

Hammes, Colonel Thomas X., *The Sling and the Stone: On War in the 21st Century*, St. Paul, Minnesota: Zenith Press, 2006.

Hoffman, Bruce, *Inside Terrorism*, New York, New York: Columbia University Press, revised and expanded edition, 2006.

Jervis, Robert, *Perception and Misperception in International Politics,* Princeton, New Jersey: Princeton University Press, 1976.

Joes, Anthony James, *Resisting Rebellion: The History and Politics of Counterinsurgency*, Lexington, Kentucky: University Press of Kentucky, 2004.

Keck, Margaret E., and Kathryn Sikkink, *Activists Beyond Borders*, Ithaca, New York: Cornell University Press, 1998.

Keohane, Robert O., and Joseph S. Nye, *Power and Interdependence*, New York, New York: Longman,1976, 1989, 2001.

Lanchester, F.W., *Aircraft in Warfare*, Ann Arbor, Michigan: University of Michigan, 1916.

Laqueur, Walter, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford, UK: Oxford University Press, 1999.

Laqueur, Walter, *No End to War: Terrorism in the Twenty-First Century*, New York, New York: Continuum International Publishing Group, 2003.

Levitt, Matthew, *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*, New Haven, Connecticut: Yale University Press, 2006.

Lia, Brynjar, *Architect of Global Jihad: The Life of Al-Qaida Strategist Abu Mus'ab al-Suri*," New York, New York: Columbia University Press, 2008.

Mao Zedong, *Selected Military Writings of Mao Tse-Tung*, Beijing, China: Foreign Language Press, 1968.
-"The Struggle in the Chingkang Mountains," 1928;
-"Problems of Strategy in China's Revolutionary War," 1936;
-"Problems of Strategy in Guerrilla War Against Japan," 1938;
-"On Protracted War," 1938.

Maoz, Zeev, *Defending the Holy Land: A Critical Analysis of Israel's National Security and Foreign Policy*, University of Michigan Press, 2006.

Mearsheimer, John, *The Tragedy of Great Power Politics*, New York, New York: W.W. Norton & Company, 2001.

Merom, Gil, *How Democracies Lose Small Wars*, New York, New York: Cambridge University Press, 2003.

Mueller, John, *War, Presidents, and Public Opinion*, Hoboken, New Jersey: John Wiley and Sons Inc., 1973.

Nacos, Brigitte L., *Mass-Mediated Terrorism*, Lanham, Maryland: Rowman & Littlefield Publishers, Inc., 2007.

Nagl, John A., *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam*, Chicago, Illinois: University of Chicago Press, 2002, 2005.

Norton, Augustus Richard, *Hezbollah: A Short History*, Princeton, New Jersey: Princeton University Press, 2007.

Pape, Robert, *Dying to Win: The Strategic Logic of Suicide Terrorism*, New York, New York: Random

House, 2005.

Polk, William R., *Violent Politics: A History of Insurgency, Terrorism & Guerrilla War, from the American Revolution to Iraq*, New York, New York: Harper Collins, 2007.

Quester, George H., *Offense and Defense in the International System*, London: Transaction Publishers, 1977.

Record, Jeffrey, *Beating Goliath: Why Insurgencies Win*, Washington, D.C.: Potomac Books, 2007.

Sageman, Marc, *Understanding Terror Networks*, Philadelphia Pennsylvania, University of Pennsylvania Press, 2004.

Sarin, Oleg and Lev Dvoretsky, *The Afghan Syndrome*, Presidio, 1993.

Schelling, Thomas, *Arms and Influence*, New Haven, Connecticut: Yale University Press, 1966.

Scheuer, Michael, *Imperial Hubris*, Washington, D.C.: Brassey's Inc., 2004.

Scheuer, Michael, *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America*, Washington, D.C.: Potomac Books Inc., 2002, 2006.

Singer, P.W., *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, New York, New York: Penguin Press HC, 2009.

Sonka, Milan, et. al., *Image Processing, Analysis, and Machine Vision*, CL Engineering, 2007.

Stern, Jessica, *Terror in the Name of God*, New York, New York: HarperCollins, 2003.

Summers, Harry G., *On Strategy: A Critical Analysis of the Vietnam War*, New York, New York: Random House, 1982, 1995.

Suskind, Ron, *The One Percent Doctrine*, New York, New York: Simon & Schuster, 2006.

Suskind, Ron, *The Price of Loyalty*, New York, New York: Simon & Schuster, 2004.

Trinquier, Roger, *Modern Warfare: A French View of Counterinsurgency*, London, United Kingdom: Praeger Security International, 1964, 2006.

Valeriano, Napolean D., and Charles T.R. Bohannan, *Counter-Guerrilla Operations: The Philippine Experience*, London, United Kingdom: Praeger Security International, 1962, 2006.

Van Creveld, Martin, *The Changing Face of War: Combat from the Marne to Iraq*, New York, New York: Ballantine Books, 2007.

Wagner, William, *Lightning Bugs and Other Reconnaissance Drones*, Washington, DC: Armed Forces Journal, 1982.

Waltz, Kenneth, *Man, the State, and War*, New York, New York: Columbia University Press, 1954, 1959.

Waltz, Kenneth, *Theory of International Politics*, New York, New York: McGraw Hill, 1979.

Weimann, Gabriel, *Terror on the internet*, United States Institute for Peace: Washington, D.C., 2006.

Wright, Lawrence, *The Looming Tower: Al-Qaeda and the Road to 9/11*, New York New York:

Random House, 2006.

Wyden, Peter, *Bay of Pigs - The Untold Story*. New York, New York: Simon and Schuster, 1979.

Data Collections

"Covert War on Terror," *The Bureau of Investigative Journalism*, http://www.thebureauinvestigates.com/category/projects/drone-data/

Dobrydney, David, "Combined Forces Air Component Command Airpower Statistics," *United States Air Force Central Command*, January 6, 2013. http://www.afcent.af.mil/shared/media/document/AFD-130106-001.pdf

"Fatalities in the first Intifada," *B'Tselem*. http://www.btselem.org/statistics/first_intifada_tables

Jenkins, Brian Michael, "Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001," *The Rand Corporation*, 2010. http://www.rand.org/pubs/occasional_papers/2010/RAND_OP292.pdf

"Obama's Covert War in Yemen," *New American Foundation*, http://yemendrones.newamerica.net/

"Operation Enduring Freedom," *iCasualties.org*. http://icasualties.org/oef/

"Operation Iraqi Freedom," *iCasualies.org*. http://icasualties.org/iraq/index.aspx

"SIPRI (Stockholm International Peace Research Institute) Military Expenditure Database." http://milexdata.sipri.org/

"Statistics," *B'Tselem*. http://www.btselem.org/statistics

Sutton, Malcom, "An Index of Deaths from the Conflict in Ireland," *CAIN*. http://cain.ulst.ac.uk/sutton/tables/Status_Summary.html

"Terrorism Against Israel: Comprehensive Listing of Fatalities," *Jewish Virtual Library*. http://www.jewishvirtuallibrary.org/jsource/Terrorism/victims.html#1993

"Terrorism deaths in Israel-1920-1999," *Israel Ministry of Foreign Affairs*. http://www.mfa.gov.il/MFA/MFA-Archive/2000/Pages/Terrorism%20deaths%20in%20Israel%20-%201920-1999.aspx

"UCDP Conflict Encyclopedia," *UCDP Database*. http://www.ucdp.uu.se/gpdatabase/search.php

Wayner, Pete "American Approval Rating (Percent) of War in Afghanistan," http://www-958.ibm.com/software/data/cognos/manyeyes/datasets/american-approval-rating-percent-o/versions/1

"The Year of the Drone: An Analysis of U.S. Drone Strikes in Pakistan, 2004-2012," *New America Foundation*, http://counterterrorism.newamerica.net/drones

Encyclopedias and Encyclopedic Entries

"Britain's Small Wars." http://www.britains-smallwars.com/

Clodfelter, Michael, *Warfare and Armed Conflicts: A Statistical Encyclopedia of Casualty and Other Figures, 1494-2007* 3rd *ed*. London: McFarland & Company, Inc., 1946, 2008.

"Chechen Terrorism," *Council on Foreign Relations*, http://www.cfr.org/terrorism/chechen-terrorism-russia-chechnya-separatist/p9181#p5

"Dillon, Robert," *U.S. Diplomacy.* http://www.usdiplomacy.org/history/service/robertdillon.php

"France/Corsica (1967-Present)," *University of Central Arkansas.* http://uca.edu/politicalscience/dadm-project/europerussiacentral-asia-region/francecorsica-1967-present/

Philips, R. Cody, "Operation Just Cause." http://www.history.army.mil/brochures/Just%20Cause/JustCause.htm

"Soviet Aggression: 1969 Border Conflict," *iBiblio*. http://www.ibiblio.org/chinesehistory/contents/03pol/c04s05.html#1969%20Border%20Conflict

"Terrorism Havens: Iraq," *Council on Foreign Relations*, December 2005. http://www.cfr.org/iraq/terrorism-havens-iraq/p9513

"The Warsaw Ghetto Uprising," The United States Holocaust Museum, http://www.ushmm.org/outreach/wgupris.htm

Governments, International Agencies, NGOs and Related Organizations

"2010 Annual Summary: Data and Trends in Terrorism," *Israeli Security Agency*. http://www.shabak.gov.il/SiteCollectionImages/english/TerrorInfo/reports/2010summary2-en.pdf

"The 9/11 Commission Report," *National Commission on Terrorist Attacks upon the United States*, New York, New York: W.W. Norton & Company, 2006.

"Afghanistan: Annual Report 2012 Protection of Civilians in Armed Combat," *United Nations Assistance Mission in Afghanistan and UN Office of the High Commissioner for Human Rights*, February, 2013. http://unama.unmissions.org/LinkClick.aspx?fileticket=K0B5RL2XYcU%3d&tabid=12254&language=en-US

"The Al-Qaida Papers – Drones," *Associated Press*, June 17, 2011.

"Al-Qaida Sanctions List," *Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities*, July 11, 2013.

"Analysis of the Fiscal Year 2012 Pentagon Spending Request," *CostofWar.com*, February 15, 2011. http://costofwar.com/en/publications/2011/analysis-fiscal-year-2012-pentagon-spending-request/
http://www.un.org/sc/committees/1267/AQList.htm#alqaedaent

Annual Threat Assessment of the US Intelligence Community, February 2, 2010, http://www.dni.gov/testimonies/20100202_testimony.pdf

"Armed Robots March into Battle," *United States Department of Defense*, December 6, 2004. http://www.defense.gov/transformation/articles/2004-12/ta120604c.html

Cacace, Gary, "Affidavit of Special Agent Gary S. Cacace: 11-mj-4270-tsh" published by *intelwire*. http://intelwire.egoplex.com/Ferdaus-Affidavit.pdf

"Camera Restrictions in New York," *411 New York*. http://411newyork.org/guide/2008/09/11/camera-restrictions-in-new-york/

"The Chola Incident," *Bharat-Rakshak*. http://www.bharat-rakshak.com/LAND-

FORCES/History/1962-71/270-Chola-Incident.html

Cole, Ronald H., “Operation Urgent Fury: The Planning and Execution of Joint Operations in Grenada,” *Office of the Chairman of the Joint Chiefs of Staff*, 1997. http://www.dtic.mil/doctrine/doctrine/history/urgfury.pdf

“Counterinsurgency Field Manual,” *U.S. Army and Marine Corps*, Chicago, Illinois: University of Chicago Press, 2007.

“Defense Budget Priorities and Choices,” *U.S. Department of Defense*, January 2012. www.defense.gov/news/Defense_Budget_Priorities.pdf

“Designated Foreign Terrorist Organizations,” *U.S. Department of State*, September 28, 2012. http://www.state.gov/j/ct/rls/other/des/123085.htm

“Enduring Strategic Partnership Agreement between the Islamic Republic of Afghanistan and the United States of America,” May 2, 2012. http://www.scribd.com/doc/92057506/Afghan-US-Strategic-Pact-Full-Text

“Field Update on Gaza from the Humanitarian Coordinator,” *United Nations Office for the Coordination of Humanitarian Affairs*, January 24-26, 2009. http://www.ochaopt.org/documents/ocha_opt_gaza_humanitarian_situation_report_2009_01_26_english.pdf

“First Strike: Global Terror in America,” *FBI*, February 26, 2008. http://www.fbi.gov/news/stories/2008/february/tradebom_022608

“Hamas' Weapons Arsenal Continues to Grow,” *IDF Blog*, February 14, 2012. http://www.idfblog.com/hamas/2012/02/14/hamas-weapons-arsenal-continues-grow/

“HM announces measures to enhance security,” *Press Information Bureau, Government of India*, December 11, 2008. http://pib.nic.in/newsite/erelease.aspx?relid=45446

“The Implementation of Network-Centric Warfare,” *The Office of Force Transformation*, 2005. http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf.

“Joint Doctrine for Information Operations” (Joint Pub 3-13), October 1998. http://www.c4i.org/jp3_13.pdf

“Miniature surveillance helicopters help protect front line troops,” *gov.uk*, February 4, 2013. https://www.gov.uk/government/news/miniature-surveillance-helicopters-help-protect-front-line-troops

“National Security Strategy of the United States of America,” September 2002. http://www.state.gov/documents/organization/63562.pdf

“National Strategy for Combating Terrorism,” February 2003. https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf

“Operation Cast Lead: Israel strikes back against Hamas terror in Gaza,” *Israel Ministry of Foreign Affairs*, January 21, 2009. http://www.mfa.gov.il/mfa/foreignpolicy/terrorism/pages/israel_strikes_back_against_hamas_terror_infrastructure_gaza_27-dec-2008.aspx

“Operation Pillar of Defense: Summary of Events,” *IDF Blog*, November 22, 2012. http://www.idfblog.com/2012/11/22/operation-pillar-of-defense-summary-of-events/

"Operation TELIC: British Casualties and Fatalities," *National Archives UK*. http://webarchive.nationalarchives.gov.uk/+/http://www.operations.mod.uk/telic/casualties.htm

"Palestinians launch rockets at Israel," *Israel Ministry of Foreign Affairs*, February 10, 2002. http://www.mfa.gov.il/mfa/pressroom/2002/pages/palestinians%20launch%20rockets%20at%20israel%20-%2010-feb-200.aspx

"Part 8 — Casualty Handling," *Report of the DoD Commission on Beirut International Airport Terrorist Act*, October 23, 1983. http://www.ibiblio.org/hyperwar/AMH/XX/MidEast/Lebanon-1982-1984/DOD-Report/Beirut-8.html.

Petraeus, David H., "Report to Congress on the Situation in Iraq," September 10, 2007. http://www.defense.gov/pubs/pdfs/Petraeus-Testimony20070910.pdf

"'Reaper' moniker given to MQ-9 unmanned aerial vehicle," *U.S. Air Force*, September 9, 2006. http://www.af.mil/news/story.asp?storyID=123027012

"The Road to Abu Ghraib," *Human Rights Watch*, June 2004, http://www.hrw.org/reports/2004/usa0604/usa0604.pdf

"Security Council Calls on Israel to Stop Demolition of Palestinian Homes," press release accompanying UNSC Resolution 1544, May 5, 2004, http://www.un.org/News/Press/docs/2004/sc8098.doc.htm

Sharp, Jeremy, "U.S. Foreign Aid to Israel," *Congressional Research Service*, April 11, 2013. http://www.fas.org/sgp/crs/mideast/RL33222.pdf

"Substitution for Testimony of Khalid Sheikh Mohammed," *United States District Court for the Eastern District of Virginia*, United States Department of Justice, 2006. http://www.vaed.uscourts.gov/notablecases/moussaoui/exhibits/defense/941.pdf

"TEXT: Cease-fire agreement between Israel and Hamas," *Haaretz*, November 21, 2012. http://www.haaretz.com/news/diplomacy-defense/text-cease-fire-agreement-between-israel-and-hamas.premium-1.479653

"Text of U.S.--Israel agreement to end Gaza arms smuggling," *Haaretz*, January 16, 2009. http://www.haaretz.com/news/text-of-u-s-israel-agreement-to-end-gaza-arms-smuggling-1.268308

"UK forces: operations in Afghanistan," *gov.uk*, June 18, 2013. https://www.gov.uk/uk-forces-operations-in-afghanistan

"United Nations Security Council Resolution 1701," August 11, 2006. http://www.un.org/News/Press/docs/2006/sc8808.doc.htm

"What is the FATF?," *Financial Action Task Force*. http://www.fatf-gafi.org/pages/aboutus/

"Winograd Committee submits final report," *Israel Ministry of Foreign Affairs*, January 30, 2008. http://www.mfa.gov.il/mfa/mfa-archive/2008/pages/winograd%20committee%20submits%20final%20report%2030-jan-2008.aspx

Letters, Addresses and Proclamations

Al Fahd, Nasir, "The Legal Status of Using Weapons of Mass Destruction against Infidels," May 2003. http://archive.org/stream/NasirAlFahd/NasirAl-fahd-TheRulingOnUsingWeaponsOfMassDestructionAgainstTheInfidels_djvu.txt

Azzam, Abdullah, "Defense of the Muslim Lands," translation by *Religioscope*. http://www.religioscope.com/info/doc/jihad/azzam_defence_1_table.htm

Ban Ki-Moon, "Secretary-General's remarks to the Security Council," *United Nations Office of the Secretary General*, November 21, 2012. http://www.un.org/sg/statements/index.asp?nid=6452

Bin Laden, Osama, "Declaration of War against the Americans Occupying the Land of the Two Holy Places," Originally published in Arabic in *Al Quds Al Arabi*, London, August, 1996. PBS News: http://www.pbs.org/newshour/terrorism/international/fatwa_1996.html.

"Bin Laden: 'Your security is in your own hands,'" *CNN*, October 29, 2004. http://www.cnn.com/2004/WORLD/meast/10/29/bin.laden.transcript/

Bush, George W., "Bush addresses nation" September 12, 2001. http://news.bbc.co.uk/2/hi/americas/1539328.stm

Bush, George W., "President Discusses Freedom and Democracy in Iraq," March 13, 2006. http://www.whitehouse.gov/news/releases/2006/03/20060313-3.html.

Bush George W., "Remarks at the United Nations General Assembly," September 12, 2002. http://www.guardian.co.uk/world/2002/sep/12/iraq.usa3

Bush, George W., "State of the Union Address," January 29, 2002. http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/sou012902.htm

"Letter from al-Zawahiri to al-Zarqawi," *globalsecurity.org*, July 9, 2005. http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm

Obama, Barack, "A New Beginning," June 4, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09/

News Media

"Airport Incident 'Was Terrorism,'" *BBC News*, July 1, 2007. http://news.bbc.co.uk/2/hi/uk_news/scotland/6257846.stm

"Al-Aqsa Intifada timeline," *BBC News*. http://news.bbc.co.uk/2/hi/middle_east/3677206.stm

Allen, Nick, "WikiLeaks: Yemen Covered Up US Drone Strikes," *The Telegraph*, November 28, 2010. http://www.telegraph.co.uk/news/worldnews/middleeast/yemen/8166610/WikiLeaks-Yemen-covered-up-US-drone-strikes.html

Al Mughrabi, Nidal, "Israel plans ceasefire, Hamas vows to fight on," *Reuters*, January 17, 2009. http://www.reuters.com/article/2009/01/17/idUSLG514136._CH_.2400

"Al-Qaeda claims Tunisia attack," *BBC News*, June 23, 2002. http://news.bbc.co.uk/2/hi/middle_east/2061071.stm

"Al-Shabaab joining al Qaeda, monitor group says," *CNN*, February 10, 2012. http://www.cnn.com/2012/02/09/world/africa/somalia-shabaab-qaeda/

"Ambush in Mogadishu," *PBS Frontline*, http://www.pbs.org/wgbh/pages/frontline/shows/ambush.

"As nation mourns, investigators try to figure out what led to tragedy in Newton, Conn.," *Fox News*, December 16, 2012. http://www.foxnews.com/us/2012/12/16/at-least-26-dead-in-shooting-at-connecticut-school/

Atkinson, Rick, “Left of Boom: The Struggle to Defeat Roadside Bombs,” *The Washington Post*, October 2007, http://www.washingtonpost.com/wp-srv/world/specials/leftofboom/index.html.

Atkinson, Rick, “Night of a Thousand Casualties; Battle Triggered U.S. Decision to Withdraw From Somalia Series,” *The Washington Post*, January 1994.

“At least 15 killed in Israeli air strikes on Gaza,” *The Guardian*, March 10, 2012. http://www.guardian.co.uk/world/2012/mar/10/israeli-air-strikes-gaza-strip

Axe, David, “Predator Drones Once Shot Back at Jets... But Sucked At It,” *Wired*, November 9, 2012. http://www.wired.com/dangerroom/2012/11/predator-defenseless/

Barnett, David, “Hezbollah takes responsibility for last week's drone over Israel,” *Long War Journal*, October 11, 2012. http://www.longwarjournal.org/archives/2012/10/netanyahu_hezbollah.php.

Barnett, David, “Pillar of Defense versus Cast Lead, 6 months after,” *Long War Journal*, June 4, 2013. http://www.longwarjournal.org/threat-matrix/archives/2013/06/pillar_of_defense_versus_cast.php

Barzak, Ibrahim, “After attack on jeep, Israeli army kills 4 in Gaza,” *Associated Press*, November 10, 2012. http://news.yahoo.com/attack-jeep-israeli-army-kills-4-gaza-175914332.html

Barzak, Ibrahim, and Karin Laub, “Hamas claims victory as ceasefire starts,” *Associated Press*, November 22, 2012. http://thechronicleherald.ca/world/188333-hamas-claims-victory-as-ceasefire-starts

Beirut Barracks Attack Remembered,” *CBS News*, October 23, 2003, http://www.cbsnews.com/stories/2003/10/23/world/main579638.shtml.

Beizer, Doug, “BAE to Develop Surveillance System,” *The Washington Post*, November 12, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/11/11/AR2007111101348.html

Belfiore, Michael, “Carnegie Takes First in DARPA's Urban Challenge,” *Wired*, November 4, 2007. http://www.wired.com/dangerroom/2007/11/darpa-names-win/

Benn, Aluf, “Israel declares victory in Gaza, but at what cost?,” *Haaretz*, January 18, 2009. http://www.haaretz.com/news/analysis-israel-declares-victory-in-gaza-but-at-what-cost-1.268327

Bergen, Peter L. and Jennifer Rowland, “Obama Ramps Up Covert War in Yemen,” *New America Foundation*, June 11, 2012. http://www.newamerica.net/publications/articles/2012/obama_ramps_up_covert_war_in_yemen_68427

Bergman, Ronen, “Hezbollah boosting drone unit,” *Ynet News*, April 27, 2012. http://www.ynetnews.com/articles/0,7340,L-4221414,00.html

Bidgood, Jess, “Massachusetts Man Gets 17 Years for Terrorist Plot,” *The New York Times*, November 2, 2012. http://www.nytimes.com/2012/11/02/us/rezwan-ferdaus-of-massachusetts-gets-17-years-in-terrorist-plot.html?_r=0

“Binalshibh to go to third country for questioning,” *CNN*, September 17, 2002. http://edition.cnn.com/2002/WORLD/asiapcf/south/09/16/alqaeda.pakistan/

Bittel, Jason, “Studying Hurricanes With Swarms of Smart Drones,” *Slate*, June 7, 2013.

http://www.slate.com/blogs/future_tense/2013/06/07/hurricane_research_drones_small_autonomous_submarine_and_plane_are_future.html

Bronner, Ethan, “As Battlefield Changes, Israel Takes Tougher Approach,” *The New York Times*, November 16, 2012. http://www.nytimes.com/2012/11/17/world/middleeast/israel-sticks-to-tough-approach-in-conflict-with-hamas.html?_r=0

Bronner, Ethan, “Israel Lets Reporters See Devastated Gaza Site and Image of a Confident Military,” *The New York Times*, January 16, 2009. http://www.nytimes.com/2009/01/16/world/middleeast/16gaza.html?_r=0

Butcher, Tim, “Israeli soldiers shocked by tunnel network,” *The Telegraph*, January 13, 2009. http://www.telegraph.co.uk/news/worldnews/middleeast/israel/4229042/Israeli-soldiers-shocked-by-tunnel-network.html

Carle, Glenn L., “Overstating Our Fears,” *The Washington Post*, July 13, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/11/AR2008071102710.html

“CIA 'killed al Qaeda suspects' in Yemen,” *BBC News*, November 5, 2002. http://news.bbc.co.uk/2/hi/2402479.stm

“CIA's final report: No WMD found in Iraq,” *Associated Press*, April 25, 2005. http://www.nbcnews.com/id/7634313/ns/world_news-mideast_n_africa/t/cias-final-report-no-wmd-found-iraq/#.UddRG_nVCSo

Clancy, Jim, “Petraeus: ‘Show Me’ if Iran has Stopped Supplying Iraqi Insurgents,” *CNN*, October 7, 2007, http://www.cnn.com/2007/WORLD/meast/10/07/petraeus.iran/index.html.

“Cheney Reasserts Al Qaeda Links to Saddam Hussein's Iraq,” *Fox News*, April 6, 2007. http://www.foxnews.com/story/0,2933,264542,00.html

Curiel, Ilana, “Rockets reach Beersheba, cause damage,” *Ynet News*, December 30, 2008. http://www.ynetnews.com/articles/0,7340,L-3647569,00.html

Dalmia, Shikha, “What Islamist Terrorist Threat?” *Reason*, February 15, 2011. http://reason.com/archives/2011/02/15/what-islamist-terrorist-threat

Danigelis, Alyssa, “Tiny Dragonfly UAV Flies and Hovers to Spy,” *Discovery News*, November 8, 2012. http://news.discovery.com/tech/dragonfly-uav-121108.htm

“Death toll passes 225 in Israeli offensive in Gaza,” *CBC News*, December 27, 2008. http://www.cbc.ca/news/world/story/2008/12/27/gaza.html

Dehghan, Saeed Kamali, “Iran supplied Hamas with Fajr-5 missile technology,” *The Guardian*, November 21, 2012. http://www.guardian.co.uk/world/2012/nov/21/iran-supplied-hamas-missile-technology

Deitch, Ian, “Israel apologizes to Turkey over flotilla deaths,” *Associated Press*, March 22, 2013. http://news.yahoo.com/israel-apologizes-turkey-over-flotilla-deaths-150703441.html

Dewey, Caitlin, “The obscure Russian jihadist whom Tamerlan Tsarnaev followed online,” *The Washington Post*, April 24, 2013. http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/24/the-obscure-russian-jihadist-whom-tamerlan-tsarnaev-followed-online/

“Dogfight between MQ-1 Predator drone and MiG-25 Foxbat,” *CBS News*.

http://www.youtube.com/watch?v=wWUR3sgKUV8

Dunlap, Charles, “We Still Need the Big Guns,” *The New York Times*, January 9, 2008.

Dreazen, Yochi J. and Evan Perez, “Suspect Cites Radical Imam's Writings,” *The Wall Street Journal*, May 6, 2010. http://online.wsj.com/article/SB10001424052748704370704575228150116907566.html

“Drone Shot Down Over Iran 'Lost' Over Afghanistan Last Week,” *The Telegraph*, December 4, 2001. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8934451/Drone-shot-down-over-Iran-lost-over-Afghanistan-last-week.html

Egerton, Brooks, “Imam's e-mails to Fort Hood suspect Hasan tame compared to online rhetoric,” *Dallas Morning News*, November 29, 2009. http://www.dallasnews.com/news/state/headlines/20091129-Imam-s-e-mails-to-Fort-7150.ece

Ephron, Dan, “Hizbullah's Worrisome Weapon,” *Newsweek*, September 11, 2006.

“FACTBOX-Al Qaeda's Yemen-based wing,” *Reuters*, November 8, 2010. http://uk.reuters.com/article/2010/11/08/yemen-qaeda-aqap-idUKLDE6A70TK20101108

Filut, Adrian, and Hadas Magen, “Manufacturers claim Cast Lead cost industry nearly NIS 90m,” *Globes*, January 18, 2009. http://www.globes.co.il/serveen/globes/docview.asp?did=1000417729

Fishman, Alex, “Uncovering the missiles,” *Ynet News*, March 16, 2011. http://www.ynetnews.com/articles/0,7340,L-4043392,00.html

“Gabon President Resumes Office,” *The New York Times*, February 21, 1964. http://select.nytimes.com/gst/abstract.html?res=F40A1EF73E5415738DDDA80A94DA405B848AF1D3

Gallagher, Ryan, “Could the Pentagon's 1.8 Gigapixel Drone Camera By Used for Domestic Surveillance?,” *Slate*, February 6, 2013. http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html

Gardner, Frank, “The growth of 'online Jihadism,'” *BBC News*, October 25, 2006. http://news.bbc.co.uk/2/hi/uk_news/6086042.stm

“Gaza-Israel truce in jeopardy,” *Al Jazeera*, December 15, 2008. http://www.aljazeera.com/news/middleeast/2008/12/2008121414433365449.html

“Gaza mortar shell wounds two men at Israeli farm,” *Reuters*, January 8, 2011. http://www.reuters.com/article/2011/01/08/us-palestinians-israel-gaza-idUSTRE7070YZ20110108

“Gaza: Palestinians killed and Israeli soldiers injured,” *BBC News*, November 11, 2012. http://www.bbc.co.uk/news/world-middle-east-20282793

Geoghegan, Tom, “Innocent photographer or terrorist?,” *BBC News*, April 17, 2008. http://news.bbc.co.uk/2/hi/technology/7351252.stm

Gorman, Siobhan and Yochi J. Dreazen and August Cole, “Insurgents Hack U.S. Drones,” *The Wall Street Journal*, December 17, 2009. http://online.wsj.com/article/SB126102247889095011.html

Graham, Bradley and Josh White, “Abizaid Credited With Popularizing the Term 'Long War,'” *The Washington Post*, February 3, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/02/02/AR2006020202242.html

Greenberg, Andy, “Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones,” *Forbes*, July 28, 2011. http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/

“Growing Terrorism in Pakistan,” *Peace Kashmir*, December 12, 2012. http://www.peacekashmir.org/views-articles/2012/1216-growing-terrorism-in-pakistan.htm

“Guide: Gaza under blockade,” *BBC News*, November 11, 2008. http://news.bbc.co.uk/2/hi/middle_east/7545636.stm

“Hamas: All Gaza militant groups agree to halt rocket attacks,” *Haaretz*, November 21, 2009. http://www.haaretz.com/news/hamas-all-gaza-militant-groups-agree-to-halt-rocket-attacks-1.3719

“Hamas announces ceasefire in Gaza,” *BBC News*, January 18, 2009. http://news.bbc.co.uk/2/hi/middle_east/7836205.stm

Harel, Amos, “Air Force: Hezbollah drone flew over Israel for five minutes,” *Haaretz*, November 9, 2004. http://www.haaretz.com/print-edition/news/air-force-hezbollah-drone-flew-over-israel-for-five-minutes-1.139744

Harel, Amos et. al., “Hezbollah drone brought down over Galilee held 30 kg of explosives,” *Haaretz*, August 14, 2006. http://www.haaretz.com/news/hezbollah-drone-brought-down-over-galilee-held-30-kg-of-explosives-1.195115

Harel, Amos, “Senior Shin Bet official: Hamas completely lost Gaza war,” *Haaretz*, October 21, 2009. http://www.haaretz.com/print-edition/news/senior-shin-bet-official-hamas-completely-lost-gaza-war-1.5743

Harris, Shane, and Stuart Taylor, “Homeland Security chief looks back, and forward.” *Govexec*, March 17, 2008. http://www.govexec.com/defense/2008/03/homeland-security-chief-looks-back-and-forward/26507/

Hashim, Asad, “The Bin Laden's life on the run,” *Al Jazeera*, July 8, 2013. http://www.aljazeera.com/indepth/features/2013/07/2013781444498188.html

Hauser, Christine, and Anahad O'Connor, “Virginia Tech Shooting Leaves 33 Dead,” *The New York Times*, April 16, 2007. http://www.nytimes.com/2007/04/16/us/16cnd-shooting.html?pagewanted=all

Hennigan, W.J., “Pentagon to soon deploy pint-sized but lethal Switchblade drones,” *Los Angeles Times*, June 11, 2012. http://articles.latimes.com/2012/jun/11/business/la-fi-kamikaze-drone-20120611

Hennigan, W.J., “United Arab Emirates set to buy U.S. Predator drones,” *Los Angeles Times*, February 22, 2013. http://articles.latimes.com/2013/feb/22/business/la-fi-predator-drone-sale-20130223

Herbert, Keith, “Boston Marathon timeline: from attack to capture,” *Newsday*, April 20, 2013. http://www.newsday.com/news/nation/boston-marathon-timeline-from-attack-to-capture-1.5112336

“Hezbollah's Rocket Force,” *BBC News*, July 18, 2006. http://news.bbc.co.uk/2/hi/middle_east/5187974.stm

“Hospital staff stunned as doctors are questioned,” *The Guardian*, July 2, 2007.

“IAEA: Syria tried to build nuclear reactor,” *Associated Press*, April 28, 2011. http://www.ynetnews.com/articles/0,7340,L-4062001,00.html

“Iranian Hostage Crisis,” *PBS*. http://www.pbs.org/wgbh/americanexperience/features/general-article/carter-hostage-crisis/

“Israel deploys 'Iron Dome' rocket shield,” *Al Jazeera*, March 27, 2011. http://www.aljazeera.com/news/middleeast/2011/03/201132718224159699.html

“Israeli gunfire kills Palestinian boy in Gaza clash: medics,” *Reuters*, November 8, 2012. http://www.reuters.com/article/2012/11/08/us-palestinians-israel-violence-idUSBRE8A711O20121108

“Israeli leaders 'to topple Hamas,'” *BBC News*, December 22, 2008. http://news.bbc.co.uk/2/hi/middle_east/7794577.stm

“Israel-OPT: Ashkelon empties, trauma teams struggle,” *IRIN*, January 13, 2009. http://www.irinnews.org/report/82338/israel-opt-ashkelon-empties-trauma-teams-struggle

“Israel reopens third Gaza Crossing,” *Al Jazeera*, Jun 29, 2008. http://www.aljazeera.com/news/middleeast/2008/06/200862974925963887.html

“Israel steps up offensive on Gaza,” *BBC News*, January 3, 2009. http://news.bbc.co.uk/2/hi/middle_east/7809699.stm

“Israel strikes Gaza after Hamas retaliation,” *Al Jazeera*, October 8, 2012. http://www.aljazeera.com/news/middleeast/2012/10/2012107232838573238.html

Janik, Rachel and Mitchell Armentrout, “Industry looks to use drones for commercial purposes,” *Miami Herald*, April 29, 2013. http://www.miamiherald.com/2013/04/29/3371170/industry-looks-to-use-drones-for.html

Jefferson, Cord, “Here's the Jihadist Magazine that Taught the Boston Bombers to Kill,” *Gawker*, April 23, 2013. http://gawker.com/heres-the-jihadist-magazine-that-taught-the-boston-bom-478605581

Johnson, Kevin, “Man accused of plotting drone attacks on Pentagon, Capital,” *USA Today*, September 29, 2011. http://usatoday30.usatoday.com/news/washington/story/2011-09-28/DC-terrorist-plot-drone/50593792/1

Katz, Yaakov, “IAF deploys third Iron Dome battery outside Ashdod,” *The Jerusalem Post*, August 31, 2011. http://www.jpost.com/Defense/IAF-deploys-third-Iron-Dome-battery-outside-Ashdod

Katz, Yaakov and Yaakov Lappin, “Iron Dome ups its interception rate to over 90%,” *The Jerusalem Post*, March 10, 2012. http://www.jpost.com/Defense/Iron-Dome-ups-its-interception-rate-to-over-90-percent

Kershner, Isabel, “Along Gaza, a Quiet (but Still Tense) Life,” *The New York Times*, October 8, 2009. http://www.nytimes.com/2009/10/09/world/middleeast/09israel.html

Kershner, Isabel, “Deadly Israeli Raid Draws Condemnation,” *The New York Times*, May 31, 2010. http://www.nytimes.com/2010/06/01/world/middleeast/01flotilla.html?_r=0

Khan, Behroz, “Pakistan Taliban: US Drone Strikes Forcing Militants Underground,” *Christian Science Monitor*, March 15, 2010. http://www.csmonitor.com/World/Asia-South-Central/2010/0315/Pakistan-Taliban-US-drone-strikes-forcing-militants-underground

Khoury, Hala, “Last French peacekeepers ready to leave Beirut,” *United Press International*, March 31, 1984.

Koebler, Jason, “Burrito Bomber Attacks Hunger with Drone-Delivered Mexican Food,” *U.S. News and World Report*, December 21, 2012. http://www.usnews.com/news/articles/2012/12/21/burrito-bomber-starts-the-drone-delivered-mexican-food

Kotz, Deborah, “Injury toll from Marathon bombs reduced to 264,” *The Boston Globe*, April 24, 2013. http://www.bostonglobe.com/lifestyle/health-wellness/2013/04/23/number-injured-marathon-bombing-revised-downward/NRpaz5mmvGquP7KMA6XsIK/story.html

Lappin, Yaakov, “Fifth Iron Dome battery deployed in Gush Dan,” *The Jerusalem Post*, November 16, 2012. http://www.jpost.com/Defense/Fifth-Iron-Dome-battery-deployed-in-Gush-Dan

Lappin, Yaakov, “IDF releases Cast Lead casualty numbers,” *The Jerusalem Post*, March 26, 2009. http://www.jpost.com/Israel/IDF-releases-Cast-Lead-casualty-numbers

“Leak reveals official story of London bombings,” *The Guardian*, April 8, 2006. http://www.guardian.co.uk/uk/2006/apr/09/july7.uksecurity

Loeb, Vernon, “Planned Jan. 2000 Attacks Failed or Were Thwarted; Plot Targeted U.S., Jordan, American Warship, Official Says,” *The Washington Post*, December 24, 2000. http://pqasb.pqarchiver.com/washingtonpost/access/65601030.html?dids=65601030:65601030&FMT=ABS&FMTS=ABS:FT&date=Dec+24%2C+2000&author=Vernon+Loeb&pub=The+Washington+Post&edition=&startpage=A.02&desc=Planned+Jan.+2000+Attacks+Failed+or+Were+Thwarted%3B+Plot+Targeted+U.S.%2C+Jordan%2C+American+Warship%2C+Official+Says

“Look, no hands,” *The Economist*, April 20, 2013.http://www.economist.com/news/special-report/21576224-one-day-every-car-may-come-invisible-chauffeur-look-no-hands

“Los Angeles Airport Shooting Kills 3,” *CNN.com*, July 4, 2002. http://articles.cnn.com/2002-07-04/us/la.airport.shooting_1_el-al-gunman-yakov-aminov?_s=PM:US

Mackenzie, Craig and Mark Duell, “'We hacked U.S. drone': Iran claims it electronically hijacked spy aircraft's GPS and tricked aircraft into landing on its soil,” *The Daily Mail*, December 19, 2001. http://www.dailymail.co.uk/news/article-2075157/Iran-claims-hacked-US-spy-planes-GPS-guided-aircraft-ground.html

Madhani, Aamer, “Cleric al-Awlaki dubbed 'bin Laden of the Internet,” *USA Today*, September 30, 2011. http://usatoday30.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm

“Man, 26, charged in model airplane plot to bomb Pentagon,” *DIY Drones*, September 28, 2011. http://diydrones.com/forum/topics/man-26-charged-in-model-airplane-plot-to-bomb-pentagon

McCarthy, Rory, “Gaza truce broken as Israeli raid kills six Hamas gunmen,” *The Guardian*, November 5, 2008. http://www.guardian.co.uk/world/2008/nov/05/israelandthepalestinians

McLeary, Paul, “Marines extend Afghan deployment of cargo UAV,” *Marine Times*, May 9, 2012. http://www.marinecorpstimes.com/news/2012/05/defense-marines-extend-kmax-afghan-deployment-050912/

“Middle East Crisis: Facts and Figures,” *BBC News*, August 31, 2006. http://news.bbc.co.uk/2/hi/middle_east/5257128.stm

Miller, Claire Cain, “With a Push from Google, California Legalizes Driverless Cars,” *The New York Times*, September 25, 2012. http://bits.blogs.nytimes.com/2012/09/25/with-a-push-from-google-california-legalizes-driverless-cars/

“The Military's New Weapon: Mini Spy Robots You Throw Like Grenades,” *The Week*, March 23, 2012. http://theweek.com/article/index/226011/the-militarys-new-weapon-mini-spy-robots-you-throw-like-grenades

Mueller, John, and Mark G. Stewart, “Hapless, Disorganized, and Irrational,” *Slate*, April 22, 2013. http://www.slate.com/articles/news_and_politics/politics/2013/04/tsarnaevs_and_boston_bombings_like_most_terrorists_they_were_hapless_and.html

“Mumbai Attacks: Terrorists Monitored British Websites Using BlackBerry Phones,” *The Telegraph*, December 1, 2008, http://www.telegraph.co.uk/news/worldnews/asia/india/3534599/Mumbai-attacks-Terrorists-monitored-coverage-on-UK-websites-using-BlackBerry-phones-bombay-india.html

Murphy, Dan, “How many rockets were fired from Gaza at Israel this year?,” *Christian Science Monitor*, November 15, 2012. http://www.csmonitor.com/World/Backchannels/2012/1115/How-many-rockets-were-fired-from-Gaza-at-Israel-this-year

Musharbash, Yassin, “A New Path for Al-Qaida: Zawahiri Confirmed as Bin Laden's Successor,” *Der Spiegel*, June 16, 2001. http://www.spiegel.de/international/world/a-new-path-for-al-qaida-zawahiri-confirmed-as-bin-laden-s-successor-a-768849.html

“Muslims Believe US Seeks to Undermine Islam,” *World Public Opinion*, April 24, 2007. http://www.worldpublicopinion.org/pipa/articles/brmiddleeastnafricara/346.php

Nakashima, Ellen and Craig Whitlock, “With Air Force's Gorgon Drone 'we can see everything,'” *The Washington Post*. January 2, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html

Nash, Elizabeth, “Madrid bombers 'were inspired by Bin Laden address,” *The Independent*, November 7, 2006. http://www.independent.co.uk/news/world/europe/madrid-bombers-were-inspired-by-bin-laden-address-423266.html

“Nasrallah Hits Out at Government,” *Al Jazeera*, May 8, 2008, http://english.aljazeera.net/NR/exeres/EB1FBB50-7FF6-4F98-B646-B2C795657F02.htm.

“Nasrallah Wins the War,” *The Economist*, August 17, 2006, http://www.economist.com/opinion/displaystory.cfm?story_id=7796790.

Nelson, Bryn, “Checkers computer becomes invincible,” *NBC News*, July 19, 2007. http://www.nbcnews.com/id/19839044/ns/technology_and_science-innovation/t/checkers-computer-becomes-invincible/#.Uc86KvnVCSo

“No Military Solution to Iraq, U.S. General Says,” CNN, March 9, 2007, http://www.cnn.com/2007/WORLD/meast/03/08/iraq.petraeus/index.html

“North Caucasus saw over 230 Interior Ministry deaths in 2009,” *RIA Novosti*, January 16, 2010. http://en.rian.ru/russia/20100116/157570882.html

“Officials release complete list of injured victims in Aurora massacre,” *Fox News*, January 10, 2013. http://www.foxnews.com/us/2013/01/10/officials-release-complete-list-injured-victims-in-aurora-massacre/

Page, Lewis, “Hurlable 360 cam-grenades used by IDF in Gaza,” *The Register*, February 23, 2009. http://www.theregister.co.uk/2009/02/23/i_ball_bull_island_industrial_subsidies/

"Pakistan Admits India Attack Link," *BBC News*, February 12, 2009, http://news.bbc.co.uk/2/hi/south_asia/7885261.stm

"Parcel bomb plotters 'used dry run,' say US officials," *BBC News*, November 2, 2010. http://www.bbc.co.uk/news/world-us-canada-11671377

Pfeffer Anshel, and Yanir Yagna, "Iron Dome successfully intercepts Gaza rocket for first time," *Haaretz*, April 7, 2011. http://www.haaretz.com/news/diplomacy-defense/iron-dome-successfully-intercepts-gaza-rocket-for-first-time-1.354696

Pfeiffer, Eric, "DARPA Unveils Robotic Mule," *Yahoo! News*, September 10, 2012. http://news.yahoo.com/darpa-unveils-robotic-mule.html

Pincus, Walter, "Air Force to Train More Remote than Actual Pilots," *The Washington Post*, August 11, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/08/10/AR2009081002712.html

Pitzke, Marc, "How Drone Pilots Wage War," *Der Spiegel*, March 12, 2010. http://www.spiegel.de/international/world/0,1518,682420,00.html

Porter, Gareth, "MIDEAST: Israel Rejected Hamas Ceasefire Offer in December," *IPS Inter Press Service*, January 9, 2009. http://www.ipsnews.net/2009/01/mideast-israel-rejected-hamas-ceasefire-offer-in-december/

Priest, Dana and William M. Arkin, "A Hidden World, Growing Beyond Control," *The Washington Post*, July 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/

"Profile: Al-Qaeda in Iraq (a.k.a. al-Qaeda in Mesopotamia)," *The Washington Post*, November 19, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/19/AR2007111900721.html

"Putin meets angry Beslan mothers," *BBC News*, September 2, 2005. http://news.bbc.co.uk/2/hi/europe/4207112.stm

Ramadan, Saud Abu and Jonathan Ferziger, "Gaza Tunnel Owners Renew Smuggling Under Egypt Border," *Bloomberg*, January 21, 2009. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aqps7qdeyKE0&refer=home

Ravid, Barak and Amos Harel and Avi Issacharoff, "Hamas declares end to cease-fire, Israeli gov't sources fear violence is unavoidable," *Haaretz*, December 19, 2008. http://www.haaretz.com/print-edition/news/hamas-declares-end-to-cease-fire-israeli-gov-t-sources-fear-violence-is-unavoidable-1.259846

Rawnsley, Adam, "Darpa's Cheetah-Bot Designed to Chase Human Prey," *Wired*, February 25, 2011. http://www.wired.com/dangerroom/2011/02/darpas-cheetah-bot-designed-to-chase-human-prey/

Rawnsley, Adam, "It's a Drone's World. We Just Live in it," *Wired*, November 28, 2011. http://www.wired.com/dangerroom/2011/11/drone-world/?pid=858

"Researchers use spoofing to 'hack' a drone." *BBC News*, June 29, 2012. http://www.bbc.com/news/technology-18643134

"Robocopter arrives," *The Economist*, September 15-21, 2012, pp. 74-75.

"Rockets hit homes in south as fire continues for second day," *The Times of Israel*, November 11,

2012. http://www.timesofisrael.com/air-force-strikes-multiple-terror-targets-in-gaza/

"Robodiptera," *The Economist*, May 4, 2013, p. 77.

Ronen, Gil, "Second Iron Dome Battery Deployed – to Protect Ashkelon," *Israel National News*, April 4, 2011. http://www.israelnationalnews.com/News/News.aspx/143343#.Uak3mkDVCSo

"Russia Lost 64 Troops in Georgia War," *Reuters*, February 21, 2009. http://uk.reuters.com/article/2009/02/21/us-russia-georgia-deaths-idUKTRE51K1B820090221

Saletan, William, "Technology Lessons from the Iraq War," *Slate*, October 12, 2007, http://www.slate.com/id/2175723.

Sasso, Brendan, "Hollywood wants drones for filmmaking," *The Hill*, January 25, 2013.

Schmitt, Eric and Thom Shanker, "Washington recasts terror war as 'struggle,'" *The Washington Post*, July 27, 2005. http://www.nytimes.com/2005/07/26/world/americas/26iht-terror.html?_r=0

Schneider, Howard, "Hezbollah rearms away from border," *The Washington Post*, January 23, 2010. http://articles.washingtonpost.com/2010-01-23/world/36923442_1_hezbollah-litani-river-judith-palmer-harik

"Scores Killed in Mumbai Attacks," *Al Jazeera*, November 27, 2008, http://english.aljazeera.net/news/asia/2008/11/2008112617472965818.html

Shachtman, Noah, "Flying Spy Surge: Surveillance Missions Over Afghanistan Quadruple," *Wired*, October 19, 2011. http://www.wired.com/dangerroom/2011/10/flying-spy-surge/

Shachtman, Noah, "Hamas Fires Long-Range Chinese Rockets at Israel," *Wired*, December 31, 2008. http://www.wired.com/dangerroom/2008/12/hamas-chinese-a/

Shachtman, Noah, "The Secret History of Iraq's Invisible War," *Wired*, June 14, 2011. http://www.wired.com/dangerroom/2011/06/iraqs-invisible-war/all/1

Sherwood, Harriet, "Flotilla raid: Turkish jihadis bent on violence attacked troops, Israel claims," *The Guardian*, June 2, 2010. http://www.guardian.co.uk/world/2010/jun/02/flotilla-raid-turkish-jihadis-troops-israel-claims

"Shootings at Fort Hood: Attack on U.S. Military Post in Texas Kills 13," *The Washington Post*, http://www.washingtonpost.com/wp-srv/special/nation/fort-hood.html

Sofer, Roni, "Israel in favor of extending Gaza lull," *Ynet News*, December 13, 2008. http://www.ynetnews.com/articles/0,7340,L-3637877,00.html

Sofer, Roni, "Israel in favor of extending Gaza lull," *Ynet News*, November 5, 2011. http://www.maannews.net/eng/ViewDetails.aspx?ID=533909

"Suspect Arrested in Arkansas Recruiting Center Shooting," *CNN.com*, June 1, 2009. http://articles.cnn.com/2009-06-01/justice/arkansas.recruiter.shooting_1_abdulhakim-mujahid-muhammad-soldier-recruiting?_s=PM:CRIME

"Taliban confirms death of Osama bin Laden's military chief in U.S. strike," *Associated Press*, November 17, 2001. http://www.chron.com/news/article/Taliban-confirms-death-of-Osama-bin-Laden-s-2035185.php

Taubman, Philip, "Soviet Lists Afghan War Toll," *The New York Times*, May 26, 1988.

http://www.nytimes.com/1988/05/26/world/soviet-lists-afghan-war-toll-13310-dead-35478-wounded.html

Teinowitz, Ira, "Hollywood to the FAA: Let Us Use Drones!," *The Wrap*, February 5, 2013. http://www.thewrap.com/movies/column-post/hollywood-faa-let-us-use-drones-76011

Terdiman, Daniel, "Drone dogfights by 2015? U.S. Navy preps futuristic combat," *CNET*, June 21, 2012. http://news.cnet.com/8301-13576_3-57457501-315/drone-dogfights-by-2015-u.s-navy-preps-for-futuristic-combat/

Thompson, Mark, "Iron Dome: A Missile Shield That Works," *Time*, November 19, 2012. http://nation.time.com/2012/11/19/iron-dome-a-missile-shield-that-works/

"TIMELINE – Israeli-Hamas violence since truce ended," *Reuters*, January 5, 2009. http://uk.reuters.com/article/2009/01/05/uk-palestinians-israel-gaza-timeline-idUKTRE50423320090105

"Tiny airplanes and subs from University of Florida laboratory could be next hurricane hunters," *University of Florida News*, June 4, 2013. http://news.ufl.edu/2013/06/04/hurricane-drones/

"Two died in Apache crash," *BBC News*, May 5, 1999, http://news.bbc.co.uk/2/hi/335709.stm

"Two Grad rockets hit Be'er Sheva; IAF strikes Gaza launching squad," *Haaretz*, March 23, 2011. http://www.haaretz.com/news/diplomacy-defense/two-grad-rockets-hit-be-er-sheva-iaf-strikes-gaza-launching-squad-1.351301

"UK combat operations end in Iraq," *BBC News*, April 30, 2009. http://news.bbc.co.uk/2/hi/8026136.stm

Vardi, Nathan, "Is al Qaeda Bankrupt?," *Forbes*, February 11, 2010. http://www.forbes.com/forbes/2010/0301/terrorism-funds-finance-osama-al-qaeda-bankrupt.html

Verini, James, "The Tunnels of Gaza," *National Geographic*, December 2012. http://ngm.nationalgeographic.com/2012/12/gaza-tunnels/verini-text

Vick, Karl, "Spy Fail: Why Iran Is Losing Its Covert War with Israel," *Time*, February 13, 2013. http://world.time.com/2013/02/13/spy-fail-why-iran-is-losing-its-covert-war-with-israel/

Wander, Andrew, "A history of terror: Al-Qaeda 1998-2008," *The Observer*, July 12, 2008. http://www.guardian.co.uk/world/2008/jul/13/history.alqaida

"Washington Post-ABC New Poll," *The Washington Post*, February 4, 2012. http://www.washingtonpost.com/wp-srv/politics/polls/postabcpoll_020412.html

Webb, Sam, "Last French soldiers leaves Afghanistan as country fulfills its bid to withdraw troops faster than any other," *Daily Mail*, November 20, 2012. http://www.dailymail.co.uk/news/article-2235900/Last-French-soldiers-leaves-Afghanistan-country-fulfils-bid-withdraw-troops-faster-other.html

"Why Soldiers Hate the Raven UAV," *Military.com*, May 29, 2012. http://www.military.com/video/aircraft/pilotless-aircraft/why-soldiers-hate-the-raven-uav/1661802396001/

Wilson, Chris, "Jeopardy, Schmeopardy," *Slate*, February 15, 2011. http://www.slate.com/articles/health_and_science/science/2011/02/jeopardy_schmeopardy.html

Wilson, Scott and Al Kamen, “'Global War on Terror' Is Given New Name,” *The Washington Post*, March 29, 2009. http://articles.washingtonpost.com/2009-03-25/politics/36918330_1_congressional-testimony-obama-administration-memo

Windrem, Robert, “Why Hezbollah is sitting on 40,000 rockets and missiles and sitting out the Gaza conflict,” *NBC News*, November 20, 2012. http://worldnews.nbcnews.com/_news/2012/11/20/15315678-why-hezbollah-is-sitting-on-40000-rockets-and-missiles-and-sitting-out-the-gaza-conflict?lite

Wingfield, Nick and Somini Sengupta, “Drones Set Sights on U.S. Skies,” *The New York Times*, February 17, 2012. http://www.nytimes.com/2012/02/18/technology/drones-with-an-eye-on-the-public-cleared-to-fly.html?pagewanted=all

“Woolwich machete attack leaves man dead” *BBC News*, May 22, 2013. http://www.bbc.co.uk/news/uk-22630303

“World's Biggest Country Becomes a Little Bit Smaller,” *RT*, October 14, 2008. http://rt.com/news/worlds-biggest-country-becomes-a-little-bit-smaller/

Wright, Lawrence, “The Rebellion Within,” *The New Yorker*, June 2, 2008. http://www.newyorker.com/reporting/2008/06/02/080602fa_fact_wright

Wright, Robin, “Strikes Are Called Part of Broad Strategy,” *The Washington Post*, July 16, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/07/15/AR2006071500957_pf.html

Yellin, Jessica, “Obama strongly considers withdrawing all troops from Afghanistan in 2014,” *CNN*, July 11, 2013. http://www.cnn.com/2013/07/08/politics/afghanistan-troop-withdrawal/index.html

Zernike Kate and Michael T. Kaufman, “The Most Wanted Face of Terrorism,” *The New York Times*, May 2, 2011. http://www.nytimes.com/2011/05/02/world/02osama-bin-laden-obituary.html?pagewanted=all&_r=0

Trade Journal and Magazine Articles

“Aircraft that Changed the World,” *Smithsonian Air and Space Magazine*, July 2008. http://www.airspacemag.com/history-of-flight/Aircraft_That_Changed_the_World.html?c=y&page=5#

“A Laser Phalanx?,” *Defense Industry Daily*, April 23, 2009. http://www.defenseindustrydaily.com/a-laser-phalanx-03783/

Anderson, Chris, “A newbie's guide to UAVs,” *DIY Drones*, March 28, 2009. http://diydrones.com/profiles/blogs/a-newbies-guide-to-uavs

Anderson, Chris, “The DIY Drones Mission (aka The Five Rules), *DIY Drones*, January 4, 2008. http://diydrones.com/profiles/blog/show?id=705844:BlogPost:17789

“Armed, Aware and Dangerous: the Top Five Military Robots,” *Army-Technology.com*, February 27, 2012. http://www.army-technology.com/features/featurearmed-aware-and-dangerous-the-top-five-military-robots/

Atwood, Tom, and Jonathan Klein, “Vecna's Battlefield Extraction-Assist Robot BEAR,” *Robot*, April 25, 2007. http://www.botmag.com/articles/04-25-07_vecna_bear.shtml

Bowman, Zach, “Learn how to turn an R/C car into an autonomous vehicle,” *Autoblog*, April 10, 2012.

http://www.autoblog.com/2012/04/10/learn-how-to-turn-an-r-c-car-into-an-autonomous-vehicle/

Clark, Colin, “Gorgon Stare Blinks A Lot; Testers Say Don't Field Til Fixed,” *DoDBuzz.com*, January 24, 2011. http://www.dodbuzz.com/2011/01/24/gordon-stare-blinks-a-lot-testers-say-dont-field-til-fixed/

Crane, David, “Anti-Sniper/Sniper Detection/Gunfire Detection Systems at a Glance,” *Defense Review*, July 19, 2006. http://www.defensereview.com/anti-snipersniper-detectiongunfire-detection-systems-at-a-glance/

Dogaru, Traian, and Calvin Le, “Validation of Xpatch Computer Models for Human Body Radar Signature,” *Army Research Laboratory*, March 2008, http://www.arl.army.mil/arlreports/2008/ARL-TR-4403.pdf

Dsouza, Larkins, “RQ-170 Sentinel 'Beast of Kandahar,'” *Defense Aviation*, December 26, 2009. http://www.defenceaviation.com/2009/12/rq-170-sentinel-beast-of-kandahar-confirmed-by-us-airforce.html

Dunnigan, James, “Switchblade Enters Service,” *Strategy Page*, September 24, 2011. http://www.strategypage.com/dls/articles/Switchblade-Enters-Service-9-24-2011.asp

“Elbit Systems Unveils VIPeR a Portable Combat Robots,” *Defense Update*, 2007. http://www.defense-update.com/newscast/0307/news/080307_viper.htm

Eshel, David, “David's Sling Makes Direct Hit in Intercept Test,” *Aviation Week*, January 28, 2013. http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_01_28_2013_p10-535569.xml

Eshel, Tamir, “Israel Navy Intercepts Missiles Loaded Cargo Vessel Bound for Gaza,” *Defense Update*, March 15, 2011. http://defense-update.com/20110315_victoria_arms_ship.html

Fingas, Jon, “Google lands patent for automatic object recognition in videos, leaves no stone untagged,” *Engadget*, August 28, 2012. http://www.engadget.com/2012/08/28/google-lands-patent-for-automatic-object-recognition-in-videos/

Finkelstein, Robert, “Military Robotics: Malignant Machines or the Path to Peace?,” *Robotic Technology Inc.*, January 2010. http://www.robotictechnologyinc.com/images/upload/file/Presentation%20Military%20Robotics%20Overview%20Jan%2010.pdf

Green, Ollie, “Dragonfly Robotic Insect UAV is Freaking Cool,” *Mobile*, November 7, 2012. http://www.mobilemag.com/2012/11/07/dragonfly-robotic-insect-uav-is-freaking-cool/

Hill, David J., “Toy-Size Helicopter Drones Now on Surveillance Duty in Afghanistan,” *SingularityHUB*, February 11, 2013. http://singularityhub.com/2013/02/11/toy-size-helicopter-drones-now-on-surveillance-duty-in-afghanistan/

Hoffman, Mike, “British soldiers flying nano helicopters in Afghanistan,” *Defensetech*, February 5, 2013. http://defensetech.org/2013/02/05/british-soldiers-flying-nano-helicopters-in-afghanistan/

Hoffman, Mike, “PBS Features DARPA's ARGUS-IS,” *Defensetech*, January 29, 2013. http://defensetech.org/2013/01/29/pbs-features-darpas-argus-is/

Humphries, Matthew, “WASP: The Linux-powered flying spy drone that cracks Wi-Fi & GSM networks,” *Geek.com*, July 29, 2011. http://www.geek.com/articles/geek-pick/wasp-the-linux-powered-flying-spy-drone-that-cracks-wi-fi-gsm-netwokrs-20110729/

Kopp, Carlo, "The Electromagnetic Bomb – a Weapon of Electrical Mass Destruction," *Air & Space Power Journal*, October 1996. http://www.airpower.maxwell.af.mil/airchronicles/cc/apjemp.html

Koren, Marina, "3 Robots That Braved Fukushima," *Popular Mechanics.* http://www.popularmechanics.com/technology/engineering/robots/3-robots-that-braved-fukushima-7223185#slide-1

Labella, Thomas H., Marco Dorigo, and Jean-Louis Deneubourg, "Division of Labor in a Group of Robots Inspired by Ants' Foraging Behavior," *ACM Transactions on Autonomous and Adaptive Systems 1 (1)*, pp. 4-25, 2006. http://www.swarm-bots.org/dllink.php?id=751&type=documents

Lassa, Todd, "The Beginning of the End of Driving: The Autonomous Car Continues to Progress," *Motor Trend*, January 2013. http://www.motortrend.com/features/auto_news/2012/1301_the_beginning_of_the_end_of_driving/

Lum, Zachary, "The Measure of MASINT," *Journal of Electronic Defense*, August 1, 1998. http://www.globalsecurity.org/intell/library/news/1998/08/MASINT.htm

McLeary, Paul, "K-MAX Chugging Along in Afghanistan," *Aviation Week*, February 3, 2012. http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%253a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%253a32270b95-e2c6-4d57-8ebd-a9ed007f342c&plckScript=blogScript&plckElementId=blogDest

Pardesi, Manjeet Singh, "Unmanned Aerial Vehicles/Unmanned Aerial Combat Vehicles: Likely Missions and Challenges for the Policy-Relevant Future," *Air & Space Power Journal*, Fall 2005. http://www.airpower.au.af.mil/airchronicles/apj/apj05/fal05/pardesi.html

"Rise of the Machines," *Army-Technology.com*, May 21, 2008. http://www.army-technology.com/features/feature1951/

Ruppert, Barb, "The Battlefield-Extraction-Assist Robot to Rescue Wounded on Battlefield," *MilitaryInfo.com*, November 22, 2010. http://www.militaryinfo.com/news_story.cfm?textnewsid=6556

Sahin, Erol and Nigel R. Franks, "Measurement of Space: From Ants to Robots," *Proceedings of WGW 2002: EPSCRBBSRC International Workshop Biologically-Inspired Robotics*, pp. 241-247, Bristol, UK, August 14-16, 2002. http://www.swarm-bots.org/dllink.php?id=161&type=documents

Sanborn, James K., "Beacon improves UAV cargo-delivery accuracy," *Marine Times*, July 8, 2012. http://www.marinecorpstimes.com/news/2012/07/marine-kmax-beacon-improves-uav-cargo-delivery-accuracy-070812w/

Sofge, Erik, "5 Robots We Should Deploy Right Now," *Popular Mechanics*, April 13, 2010. http://www.popularmechanics.com/technology/engineering/robots/robots-to-deploy-now

Stirling, Timothy, James Robert, Jean-Christophe Zufferey and Dario Floreano, "Indoor Navigation with a Swarm of Flying Robots," *Proceedings of the 2012 IEEE International Conference on Robotics and Automation*, 2012. http://www.swarmanoid.org/upload/pdf/StirlingEtAl2012.pdf

"Swarmanoid: Towards Humanoid Robotic Swarms," *Swarmanoid.org.* http://www.swarmanoid.org/index.php

"Swarm-bots: Swarms of self-assembling artifacts," *Swarm-bots.org*. http://www.swarm-bots.org/

Trianni, Vito and Marco Dorigo, “Emergent Collective Decisions in a Swarm of Robots,” *2005 IEEE Swarm Intelligence Symposium (SIS 2005)*, pp. 241-248, June 8-10, 2005. http://www.swarm-bots.org/dllink.php?id=692&type=documents

Trimble, Stephen, “Lockheed Martin to Build the Mother of All Airborne Radars,” *The DEW Line*, April 27, 20009. http://www.flightglobal.com/blogs/the-dewline/2009/04/lockheed-martin-to-build-the-m.html

Ungerleider, Neal, “The Science Behind the Drone Terrorism Attack,” *Fast Company*, September 29, 2011. http://www.fastcompany.com/1783721/science-behind-drone-terrorism-attack

“Unmanned Aircraft Systems Flight Plan,” *United States Air Force*, May 18, 2009. http://www.scribd.com/doc/17312080/United-States-Air-Force-Unmanned-Aircraft-Systems-Flight-Plan-20092047-Unclassified

Urmson, Chris, “The self-driving car logs more miles on new wheels,” *Google Official Blog*, August 7, 2012. http://googleblog.blogspot.hu/2012/08/the-self-driving-car-logs-more-miles-on.html

“U.S. Army Awards AeroVironment $5.1 Million Order for Switchblade Loitering Munitions System and Services,” *AeroVironment*, May 23, 2012. http://www.avinc.com/resources/press_release/u.s._army_awards_aerovironment_5.1_million_order_for_switchblade_loitering_

“US Military Bringing a Switchblade to A Gun Fight,” *Defense Industry Daily*, September 13, 2012. http://www.defenseindustrydaily.com/us-army-brings-a-switchblade-to-a-gun-fight-07071/

Yirka, Bob, “Makers of infamous BigDog robot unveil human version – PETMAN,” *Phys.org*, November 1, 2011. http://phys.org/news/2011-11-makers-infamous-bigdog-robot-unveil.html

Technical Specifications, Manufacturer Information, and Demonstration Videos

“Ababil (Swallow) Unmanned Aerial Vehicle,” *Globalsecurity.org*. http://www.globalsecurity.org/military/world/iran/ababil.htm

“About Us,” *The Rabbit-Hole*, https://rabbit-hole.org/about/

“ArduCopter User Group,” *DIY Drones*. http://diydrones.com/group/arducopterusergroup

“ArduPilot,” *code.google.com*. https://code.google.com/p/ardupilot/

“Army Orders 1,100 Recon Scout XT Robots from ReconRobotics,” *Business Wire*, February 15, 2012. http://www.businesswire.com/news/home/20120215005395/en/Army-Orders-1100-Recon-Scout-XT-Robots

“ARPAnet,” *PCMAG.com*. http://www.pcmag.com/encyclopedia/term/37989/arpanet

“AutoCAD Map 3D,” *Autodesk*. http://www.autodesk.com/products/autodesk-autocad-map-3d/overview

“Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System (ARGUS-IS),” *DARPA*, http://www.darpa.mil/Our_Work/I2O/Programs/Autonomous_Real-time_Ground_Ubiquitous_Surveillance-Imaging_System_(ARGUS-IS).aspx

“BigDog Overview (video),” *Boston Dynamics*, http://www.youtube.com/watch?v=cNZPRsrwumQ

“BigDog – The Most Advanced Rough-Terrain Robot on Earth,” *Boston Dynamics*, http://www.bostondynamics.com/robot_bigdog.html

“Cheetah Robot runs 28.3 mph; a bit faster than Usain Bolt,” *Boston Dynamics*, September 5, 2012. http://www.youtube.com/watch?v=chPanW0QWhA&list=UU7vVhkEfw4nOGp8TyDk7RcQ&index=3

“Counter Rocket, Artillery, and Mortar (C-RAM),” *globalsecurity.org*. http://www.globalsecurity.org/military/systems/ground/cram.htm

“Decibel Levels of Everyday Sounds,” *informationxchange*. http://www.stuartxchange.com/Decibels.html

“Download the Arduino Software,” *Arduino.cc*. http://arduino.cc/en/Main/Software

“Dynamic Robot Manipulation,” *Boston Dynamics*, March 1, 2013. http://www.youtube.com/user/BostonDynamics?feature=watch

“E-Flite F-86 Sabre 15 Ducted Fan Jet ARF,” *A Main Hobbies*. http://www.amainhobbies.com/product_info.php/cPath/3_516_2077_693/products_id/173356/n/E-Flite-F-86-Sabre-15-Ducted-Fan-Jet-ARF?utm_source=Google-Base&utm_medium=cpc&utm_campaign=Product-Feeds&source=google_ext&gclid=CPirx5Chp7cCFYyZ4AodLS4AYA

“Flying-Cam and Bond 007 'Skyfall,'” *Flying-Cam*, April 24, 2012. http://flying-cam.com/en/news.php

“Gorgon Stare,” *Globalsecurity.org*. http://www.globalsecurity.org/intell/systems/gorgon-stare.htm

“Ground Robots – 510 PackBot,” *iRobot*. http://www.irobot.com/gi/ground/510_PackBot

“Hezbollah Displays Iranian Fajr-5 Missile,” posted on *YouTube* April 2, 2013: http://www.youtube.com/watch?v=CoacPETi26k and April 6, 2013: http://www.youtube.com/watch?v=c9Ad6NYxQ60.

“High Performance Hydraulics for Industrial Applications,” *Vecna*, http://www.vecna.com/robotics/multimedia/downloads/high_performance_hydraulics_for_industrial_applications.pdf

“IED Jammer,” *Bomb Jammer*. http://www.bombjammer.com/ecom-catshow/ied_jammer.html

“Integrated Sensor Is Structure (ISIS),” *DARPA Strategic Technology Office*, http://www.darpa.mil/Our_Work/STO/Programs/Integrated_Sensor_is_Structure_%28ISIS%29.aspx

“iRobot PackBot 510 with Engineer Kit,” *iRobot*, http://www.ulkem.com.tr/html/urunler/robotlar/PackBot510engineer/ppdf.pdf

“Iron Dome,” *Rafael Advanced Defense Systems*. http://www.rafael.co.il/Marketing/186-1530-en/Marketing.aspx

“Lockheed Martin RQ-170 Sentinel Unmanned Aerial Vehicle,” *Miltaryfactory.com*, December 12, 2011. http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=896

“MK 15 – Phalanx Close-In Weapons System (CIWS),” *United States Navy Fact File*. http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2

"Mohajer (UAV)," *Globalsecurity.org*. http://www.globalsecurity.org/military/world/iran/mohajer.htm

"NBS MANTIS Air Defense Protection System, Germany," *Army-technology.com*. http://www.army-technology.com/projects/mantis/

"PackBot Tactical Robot," *Defense Update*, http://defense-update.com/products/p/pacbot.htm

"Packet Switching," *PCMAG.com*. http://www.pcmag.com/encyclopedia/term/48751/packet-switching

"PD-100 PRS – Your Personal Reconnaissance System," *Prox Dynamics*. http://www.proxdynamics.com/products/pd_100_prs/

"Personal Computer," *PGMAG.com*. http://www.pcmag.com/encyclopedia/term/49133/personal-computer

"PETMAN – BigDog Gets a Big Brother," *Boston Dynamics*, http://www.bostondynamics.com/robot_petman.html

"Phantom," *DJI Innovations*. http://www.dji-innovations.com/product/phantom/

"Predator RQ-1/MQ-1/MQ-9 Reaper – United States of America," *Airforce-technology.com* http://www.airforce-technology.com/Projects/predator-uav/

"Predator B UAS," *General Atomics*, http://www.ga-asi.com/products/aircraft/predator_b.php

"Predator C Avenger," *General Atomics*, http://www.ga-asi.com/products/aircraft/predator_c.php

"Predator UAS," *General Atomics*, http://www.ga-asi.com/products/aircraft/predator.php

"Raytheon's Mobile Land-Based Phalanx Weapon System Completes Live-Fire Demonstration," *Raytheon*, December 2, 2010. http://raytheon.mediaroom.com/index.php?s=43&item=1715

"RC Car to Robot," *Instructables.* http://www.instructables.com/id/RC-Car-to-Robot/

"Recon Scout Throwbot LE," *Recon Robotics*. http://www.reconrobotics.com/products/recon-scout_throwbot_LE.cfm

"RQ-4 Global Hawk: High-Altitude, Long-Endurance Unmanned Aerial Reconnaissance System," *Northrup Grumman*, http://www.as.northropgrumman.com/products/ghrq4a/assets/HALE_Factsheet.pdf

"RQ-11 Raven Unmanned Aerial Vehicle," *Army-technology.com*. http://www.army-technology.com/projects/rq11-raven/

"SkyGrabber," *Sky Software*, http://www.skygrabber.com/en/skygrabber.php

"Switchblade – Miniature Loitering Weapon," *Defense Update*, 2011. http://defense-update.com/products/s/switchblade_31122010.html

"Talon Specifications," *Robotinfo.wordpress.com*, http://roboinfo.wordpress.com/2010/04/09/talon-specifications/

"TCP/IP," *PCMAG.com*. http://www.pcmag.com/encyclopedia/term/52614/tcp-ip

"The Throwbot XT with Audio Capabilities," *Recon Robotics*. http://www.reconrobotics.com/products/Throwbot_XT_audio.cfm

"The Totally New SARAH Unmanned Aerial System," *Flying-Cam*, February 7, 2011. http://www.flying-cam.com/en/news.php?id=108&PHPSESSID=9baa6b326c5ae8c672eb2328a62d198c

"UAS Advanced Development: Raven RQ-11A," *AeroVironment*. http://www.avinc.com/uas/adc/raven/

"UAS Advanced Development: Switchblade," *AeroVironment*. http://www.avinc.com/uas/adc/switchblade/

"UAS: RQ-11B Raven," *AeroVironment*. http://www.avinc.com/uas/small_uas/raven/

"UAS: Wasp AE," *AeroVironment*. http://www.avinc.com/uas/small_uas/waspAE/

"Unmanned Aerial Vehicles," *GlobalSecurity.org*, http://www.globalsecurity.org/intell/systems/uav.htm

US Patent 7339516, "Method to Provide Graphical Representation of Sense Through the Wall (STTW) Targets," issued March 4, 2008, http://www.patentstorm.us/patents/7339516.html

"Wasp III," *U. S. Air Force*, January 1, 2013. http://www.af.mil/information/factsheets/factsheet.asp?id=10469

"What is Synthetic-Aperture Radar?," *Sandia National Laboratories.* http://www.sandia.gov/radar/whatis.html

"World Wide Web," *PCMAG.com*. http://www.pcmag.com/encyclopedia/term/54867/world-wide-web